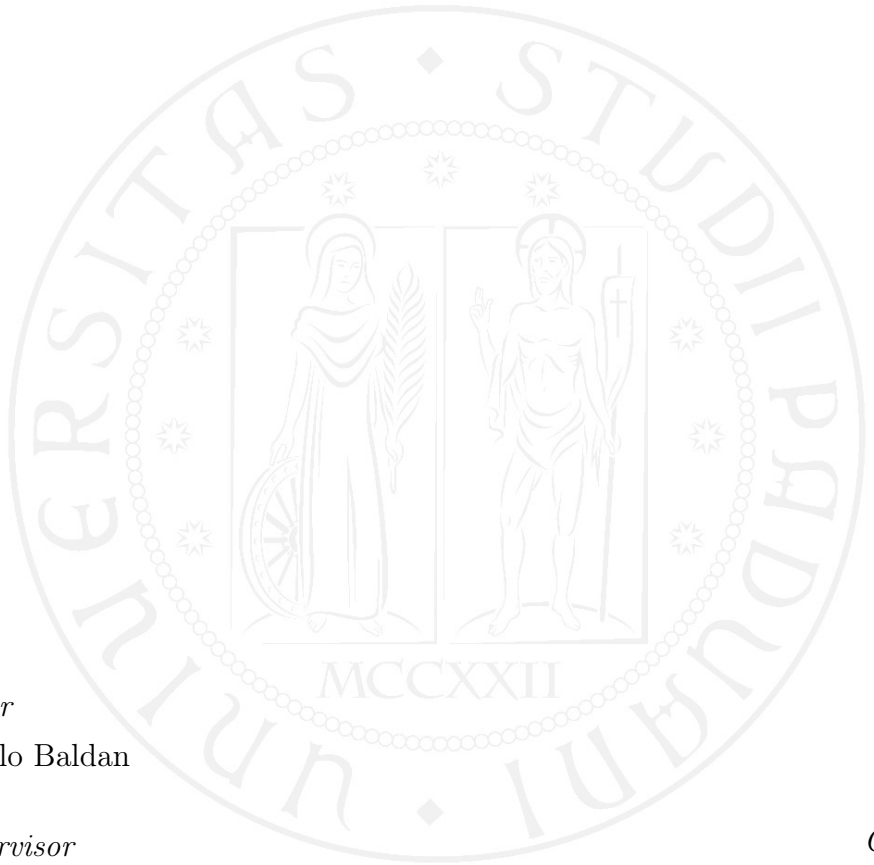
University of Padova

Department of Mathematics "Tullio Levi-Civita"

Master degree in Computer Science

Some decidability questions in abstract program semantics



Supervisor

Prof. Paolo Baldan

Co. Supervisor

Prof. Francesco Ranzato

Candidate

Luca Zaninotto

Academic Year 2023-2024

Abstract

This thesis explores program verification trough abstract interpretation in the context of computability theory. Abstract Interpretation is a program analysis technique, based on approximating the semantics of programs over so-called *abstract domains*, usually represented as complete lattices, whose elements represent program properties. These approximations rely on some abstract operators, which usually include fixpoint iterations. Traditionally, to ensure convergence of such iterations, and therefore ensuring the termination of the analyzer, the literature relied on two important operators: the *widening* and the *narrowing* operators, first defined in [CC77]: the first one to compute an upper bound on some chain in the complete lattice, and the second one to recover some additional information from the program and refine the upper bound provided by the widening. This thesis focuses on a special abstract domain, called the *intervals* domain, where each variable of program is assigned to an interval over the integer numbers. The thesis argues that in such a context widening and narrowing operators can be replaced by another method, that relies on deciding program divergence by looking at the behavior of variables in the context of the program.

Acknowledgments

To my family.

Contents

Introduction

Because of its widespread adoption software has become a crucial aspect of everyone's life for all sorts of tasks, from the more mundane ones – like sending text messages or view online content – to the most crucial ones. Banking, aviation, space industry, car controls are only a small example of important everyday tasks that software runs in the modern era. Such tasks demand requirements of safety and reliability which are difficult to pair with the growing complexity and size of contemporary software. Errors can be exphensive both in monetary and in human lives terms, hence preventing them becomes more and more valuable as well as detecting them early.

Notable examples of such bugs are Meltdown and Spectre [Lip+18; Koc+19]. Those vulnerabilities exploted an hardware related bug in floating-point division to access data outside the bounds imposed to a program y the operating system, resulting in the theft of arbitrary data, meaning a malicius actor could access – for example – passwords stored locally or – more realistically – data of other customers in a cloud environment. Another notable example is the first internet worm, which allowed the deployer to run arbitrary code on a significant portion of the computers on the internet at the time [Spa89; See89; Orm03; Eis+89]. The last example is set on 4 June 1996, when the Ariane 501 satellite launch failed catastrophically 40 seconds after initiation of the flight sequence, incurring a direct cost of approximately 370 million US dollars [Dow97]. To asses the causes of the incident, the automated analysis of the Ariane code [Lac+98] was done using a static analyzer based on Abstract Interpretation [Le 97].

Software verification is therefore a crucial task, which cannot be accomplished using testing practices alone: testing in fact can be used to show the *presence* of bugs (if a test fails the bug occur), but they do not offer any *mathematical guarantee* of their absence. The latter can be obtained trough *formal methods*, i.e., by mathematical proving the correctness of a program with respect to some *specification*.

Formal methods. Despite the progress done to bring the usefulness of formal methods to everyone (e.g. with [OHe19; Dis+19] or with the Grand Challenge of software verification [JOW06; HM08; Woo06]) their use is still restricted to specific niches of developers. This is due to some prblems with the technique itself. Firstly, the problem is intrinsic in the theory of computation. Consider the following program in a pseudo-C language

```
1  int* p = NULL;
2  arbitrary_function();
3  *p = 0;
```

If control reaches Line 3 the program will crash (as we are trying to access address 0x0). Hence we have to prove that `arbitrary_function()` does not halt. Unfortunately Turing [Tur21] shows that this problem is undecidable. Moreover, Rice's Theorem [Ric53] expands on this stating that *all non-trivial semantics properties* of programs are undecidable. The consequence is that we cannot have an *universal verifier*, i.e., a verification tool that proves or disproves the correctness of every program with respect to some specification. However we do not need to solve such a general problem. We as humans tend to use patterns and structures, even to write our logic. The outcome is that we work with just a small subset of all possible programs, and therefore to work in practice our analyzers have to trace the correctness of just that small subset of programs.

Moreover the result of our analysis does not have to be the most precise description of the outcome of the program we are analyzing. We need a tool that can state that our program satisfies

a property (an *invariant*) which is *sound* to the real property of the program, i.e., a property which is *less precise* than the real one. Notable example of such analyzers are well known and available today on the internet. For example Astreè [Cou+05] and Mopsa [MOM23] are two sound analyzers of C and python code, which can infer program properties and catch bugs ahead of time. They both use a technique called *abstract interpretation* which (roughly) involves interpreting a given program by mapping variables to an abstract rapresentation of some properties we are interested in.

Abstract interpretation. Since universal program verification is a fundamentally undecidable problem, the best we can do is to consider non-universal verification, at the cost of getting non-conclusive answers. In this work we focus on one of the major technique for software analysis that can be used to implement a sound verifier: abstract interpretation. To best introduce the technique we start from an example. Consider the following fragment of pseudo-C code:

```
1  int x = 0;
2  for(int i = 0; i < 5; i++){
3    int val = rand();
4    if (val > 0.5) x += 2;
5    else x -= 2;
6  }
7  printf("%d", x);
```

Code 1: Incrementing or decrementing randomly

Each execution of the snippet could result in a different value of `x` being printed on screen. From a mathematical point of view, before entering the loop the value of `x` is fixed, it can only be 0. Abstracting the execution means *abstracting* the values the variables can assume. For this example variables can assume *interval* values, e.g., $\texttt{x} \in [0, 0]$ at the beginning of the interval. Assuming `rand()` returns a `float` value in $[0, 1]$, at each iteration either `x` is incremented or decremented by 2. Hence, after the first iteration $\texttt{x} \in [-2, +2]$, after the second $\texttt{x} \in [-4, +4]$, and so on. The loop could carry on forever, however, because of the `for` guard $\texttt{i} < 5$ we reach a stall at $\texttt{x} \in [-10, +10]$. Therefore at the end of the loop, what our analysis can infer is that $\texttt{x} \in [-10, +10]$.

The analysis is sound: the most precise property of the value of `x` would be being in the set $S = \{-10, -8, -6, -4, -2, 0, +2, +4, +6, +8, +10\}$, as for each iteration the value of `x` can increment or decrement by 2, and our result $[-10, +10]$ is a *superset* of S.

Abstract interpretation, introduced by Radhia and Patrick Cousot in [CC77; CC79] is therefore a framework that generalizes this idea by providing tools to compute efficently general abstractions. As a result, a sound verifier can be obtained by comparing the resulting abstraction with the program specification: if the latter satisfies the former (i.e. it is a *superset*) then also the pregram does and therefore it is correct, otherwise noting can be said about the program, as the abstraction is an *over-approximation*.

With the example we already introduced the idea of the framework of abstract interpretation:

- We start from a *concrete semantics*, describing the meaning of program commands in a *computational domain*;
- We define an *abstract domain*, which models some properties of interest of the concrete computation and leaves out the details (in our example, the *interval* domain);
- We induce an *abstract semantics*, based on the concrete semantics and our abstract domain, which allows to *abstractly execute* our program on the abstract domain in order to compute the program properties modeled by the abstract domain;
- The result of our abstract execution is the final property of the program.

Generally the abstract execution of our program (i.e. the abstract interpretation) involves *fixpoint computations* on algebraic structures called *lattices*. Lattices are sets equipped with a notion of *order* between elements, while fixpoint computaitons usually involve computing a minimal element

in a *chain* of lattice elements such that the computaiton does not proceed further. In other words, at which point the guard of a loop is not satisfied anymore and which guarantees can we infer for the program *after* the loop? Consider the snipped of Code 1. We argued that our computation of the abstract value of the variable `x` could start from $[0, 0]$ and proceed with $[-2, +2], [-4, +4], \ldots$ In this case we find a fixpoint with $[-8, +8]$, since the guard of the loop is not respected anymore (because of the variable `i`) and therefore "executing" the loop again would result in the same initial value $[-8, +8]$, hence a *fixpoint* is reached.

However this is not always the case. Consider instead the following snippet

```
1  int x = 0;
2  while(true) {
3    x += 1;
4  }
```

Obviously the concrete computaion does not halt, but looking at the chain of iterands for our program for the variable `x` we could infer the chain

$$[0, 0], [+1, +1], \ldots, [+k, +k], \ldots$$

and therefore (intuitively) at the end of the loop we might want to say that our variable has a value in the range $[0, +\infty]$, which is sound to the *real* property of non-termination (i.e., $\texttt{x} \in \varnothing$, `x` has *no* final value).

To infer properties while dealing with infinite chains the standard approach is to use *widening* operators (from [CC92], usually denoted as $\triangledown$) to infer the *divergence* of a variable after some round of increments. Such technique however, while still providing a sound analysis and ensuring termination, limits a lot the precision of the analysis itself. For example, we could widen our analysis after the second step with a naive widening $[-2, +2] \triangledown [-4, +4] = [-\infty, +\infty]$ and infer that our variable after the end of the loop has a value between $+\infty$ and $-\infty$. This is certanly true, but is however very imprecise.

To recover some information loss with the widening we can use narrowing operators, but these work only when the information to refine our anaysis is explicit. In our example a narrowing would be sufficent to infer that the variable is between -10 and $+10$, but in general it is not.

This opens a question, is it possible to have a precise analysis of abstract properties, while ensuring the termination of the analyzer?

Precise interval analysis Because the presence of infinite ascending chains in the domain of intervals, the analysis over that domain was considered an algorithmic challenge: ordinary fixpoint iteration (trough kleene iteration) will not result in terminating analysis algoritm, while widening and narrowing do not compute the least solution of a system of equations, but only a safe over approximation of it, while ensuring termination. Initially in [SW05] Su and Wagner identify a class of interval equations for which the least solution can be computed precisely in polinomial time. Later [Gaw+09] expands on the latter article by providing an algorithm to compute least solutions that also deals with the arbitrary multiplication of intervals.

Outline The following document consists of 5 chapters. Chapter 1 provides the necessary background and fixes the necessary notation that will later be used in the following chapters: from recursion and order theory to talk about program termination and undecidability to abstract interpretation to prove some properties of our analysis. Chapter 2 Introduces the framework of the thesis: the Imp language (and its constraints), its *concrete* semantics and its properties (namely undecidability of some properties of the programs written in the language). Chapter 3 introduces and shows the properties of interval and non-relational collecting analysis on the Imp language, while Chapter 4 proves that, similarly to previous work, it is possible to bound the domains we previously introduced to remove infinite ascending chains, hence ensuring analysis termination. Some contraits will emerge and the results will later be exposed in Chapter 5.

Chapter 1

Background

The following chapter aims to provide context, notation and the important external references for the work that will follow on. We start with Section 1.1 where we introduce some notation and the important aspect of recursion theory needed to understand the following chapters. Later, in Section 1.2 we explore order theory and set the notation that we will use in the rest of the thesis to talk about this topic. Finally Section 1.3 introduces the notation and concepts we need to properly talk about abstract interpretation in later chapters.

1.1 Recursion theory

This first section aims to provide background and terminology for the parts in recursion theory that will follow. More in detail, we will take some notation from [Cut80] and introduce some notation based on the same book. We start with functions: total and partial functions are essential to recursion theory:

Definition 1.1 (Total and partial functions)**.** Let X, Y be two sets. We denote by

$$X \to Y$$

the set of all total functions from X to Y. And by

$$X \hookrightarrow Y$$

the set of all partial functions from X to Y.

Partial functions are actually functions from a subset $S \subseteq X$ which is called the *natural domain* of f.

Definition 1.2 (Domain of partial functions)**.** Let $f : X \hookrightarrow Y$. We write $f(x)\downarrow$ to indicate that f is defined on x, and $f(x)\uparrow$ to indicate that f is undefined on x. The domain of f is

$$dom(f) = \{x \in X \mid f(x)\downarrow\}$$

We then need (mostly in Section 2.4) to talk about partial recursive functions and their properties. We therefore define partial recursive and total recursive functions as follows:

Notation 1.3 (partial and total recursive functions)**.** By $\mathbb{N}^k \overset{r}{\hookrightarrow} \mathbb{N}$ we denote the set of partial recursive functions on natural numbers, while by $\mathbb{N} \overset{r}{\to} \mathbb{N}$ we denote the set of partial recursive functions on natural numbers.

We also need to talk about decidable properties and decidable sets. We therefore introduce the notion of recursive and recursively enumerable sets.

Definition 1.4 (Recursively enumerable and recursive sets)**.** A set $A \subseteq \mathbb{N}^k$ is *recursively enumerable* (r.e. or semi-decidable) if $A = dom(f)$ for some $f \in \mathbb{N}^k \overset{r}{\hookrightarrow} \mathbb{N}$.

A set $A \subseteq \mathbb{N}$ is a recursive set if both A and its complement $\overline{A} = \mathbb{N} \setminus A$ are semi-decidable, i.e., there exists some $f \in \mathbb{N} \overset{r}{\to} \mathbb{N}$ s.t.

$$f = \lambda n.(n \in A)?1 : 0$$

1.2 Order theory

Within Theoretical Computer Science, especially in the field of semantics, partial orders hold significant importance. They are extensively employed in Abstract Interpretation, as highlighted in [Min18], serving different levels of the theory to model core notions. These notions include the idea of approximation, where certain analysis results may be less precise than others, creating a partial order where some results are incomparable. Moreover, partial orders are fundamental in conveying the concept of soundness: an analysis is deemed sound if its result is an over-approximation of the actual behavior. These mathematical notions, essential for discussions surrounding the Abstract Interpretation formalism, primarily involve order and lattice theory.

Definition 1.5 (Partiall ordered set)**.** Let X be a non-empty set, $\sqsubseteq \subseteq X \times X$ be a reflexive, anti-symmetric and transitive relation on that set, i.e., $\forall x, y, z \in X$:

1. $x \sqsubseteq x$ (reflexivity)
2. $x \sqsubseteq y \wedge y \sqsubseteq x \implies x = y$ (antisymmetry)
3. $x \sqsubseteq y \wedge y \sqsubseteq z \implies x \sqsubseteq z$ (transitivity)

Then the tuple $\langle X, \sqsubseteq \rangle$ is a *partially ordered set* (POSet).

Definition 1.6 (Least upper bound)**.** Let $\langle X, \sqsubseteq \rangle$ be a POSet and let $Z \subseteq X$. We say that $\overline{z} \in Z$ is an *upper bound* of Z if $\forall z \in Z \; z \sqsubseteq \overline{z}$. It is the *least upper bound* of Z if $\forall z'$ upper bounds of Z, $\overline{z} \sqsubseteq z'$.

Definition 1.7 (Greatest lower bound)**.** Let $\langle X, \sqsubseteq \rangle$ be a POSet and let $Z \subseteq X$. We say that $\overline{z} \in Z$ is a *lower bound* of Z if $\forall z \in Z \; \overline{z} \sqsubseteq z$. It is the *greatest lower bound* of Z if $\forall z'$ upper bounds of Z, $z' \sqsubseteq \overline{z}$.

Usually then we are talking about least and greatest lower bound the host set is often implicit, and we therefore simply write $\text{lub}(Z)$ and $\text{glb}(Z)$. In abstract interpretation we often rely on special kinds of POSets, where the existence of the greatest lower bound and the least upper bound is ensured for each subset of the original POSet. These sets are called complete lattices

Definition 1.8 (Complete lattice)**.** A POSet $\langle X, \sqsubseteq \rangle$ is called a *complete lattice* if

$$\forall Y \subseteq X \quad \exists \cup Y \wedge \exists \cap Y$$

Complete lattices are a subset of the class of chain complete partial ordered sets. These kinds of partial orders are defined using the concept of chains:

Definition 1.9 (Chain)**.** Let $\langle D, \sqsubseteq \rangle$ be a partially ordered set. Then $Y \subseteq D$ is a chain if for any $y_1, y_2 \in Y$ it holds that

$$y_1 \sqsubseteq y_2 \vee y_2 \sqsubseteq y_1$$

Definition 1.10 (**CCPOs**)**.** A chain complete partially ordered set (ccpo) is a poset $\langle D, \sqsubseteq \rangle$ such that every chain of D has a least upper bound.

The last building block we will use in the following chapters is the Kleene-Knaster-Tarski theorem. This theorem is a fundamental result in order theory and provides a powerful tool for analyzing and establishing the existence of fixed points in complete lattices. To state it we need to first link functions and order theory with some definitions

Definition 1.11 (Monotone functions)**.** Let $\langle D, \sqsubseteq \rangle$ and $\langle D', \sqsubseteq' \rangle$ be complete lattices. The total function $f : D \to D'$ is *monotone* if

$$d_1 \sqsubseteq d_2 \implies f(d_1) \sqsubseteq' f(d_2)$$

Monotonicity however does not preserve upper bounds, just orders. In particular if we take a chain $Y \subseteq D$ of some ccpo $\langle D, \subseteq \rangle$ and some monotone function $f : D \to D$, in general $\sqcup\{f(d) \mid d \in Y\} \sqsubseteq f(\sqcup Y)$, but not $\sqcup\{f(d) \mid d \in Y\} = f(\sqcup Y)$. Therefore we introduce the concept of continuity, functions that preserve both order and upper bounds

Definition 1.12 (Continuous functions)**.** Let $\langle X, \sqsubseteq \rangle$ and $\langle X', \sqsubseteq' \rangle$ be ccpos. The total function $f : D \to D'$ is *continuous* if

- f is monotone;
- $\sqcup'\{f(d) \mid d \in D\} = f(\sqcup X)$

Continuous functions over ccpos are important for the Kleene fixed-point theorem, usually attributed to Tarski from [Tar55], which is also called Kleene iteration. It gives us an iteration strategy to find the least fixpoint of a function over a ccpo, provided that the function is continuous.

Theorem 1.13 (Kleene fixed-point)**.** *Let $f : D \to D$ be a continuous function over a chain complete partial order $\langle D, \sqsubseteq \rangle$ with the lest element $\bot$. Then*

$$\mathit{lfp}(f) = \bigsqcup\{f^n(\bot) \mid n \in \mathbb{N}\}$$

where

- $f^0 = id$
- $f^{n+1} = f \circ f^n \quad \forall n \in \mathbb{N}$

is the least fix point of f.

1.3 Abstract Interpretation

Abstract interpretation is among the most well known methods of static analysis of programs. First introduced by Patrick and Radhia Cousot in [CC77; CC79], it consists in a sound-by-construction method to infer program properties given a model of their behavior. The general idea is that we can approximate the semantics of a program with monotonic functions over ordered sets (usually *complete lattices*). To do so we usually first introduce *Abstract Domains* that capture some essential aspects of program execution while ignoring the details of the computation, which would make the analysis computationally infeasible. This analysis however carries the issue of completeness, which is closely related to the issue of choosing the best abstract domain to decide program correctness without raising false alarms. Achieving completeness in analysis is often desirable, but it can lead to the problem of undecidability. This means that even though we strive for the most accurate analysis of a program, such as through its interpreter, we can't guarantee that the process will always terminate. The technique per-se is a concept which is around since the '70s, hence an extensive amount of literature has been produced. For a brief history of the technique, see [GR22].

The main source of this chapter comes from the notes on abstract interpretation in [Min18].

1.3.1 General concepts

Abstract interpretation heavily relies on order theory, which we introduced in Section 1.2, and builds on top of it. The core idea is that we use an *abstract domain* as an approximation of the *concrete domain*, in such a way that abstract computations are *sound* with respect to the concrete ones. The minimal structure that we will require both in the abstract and the concrete domains is a partial order that models the amount of information each instruction carries with respect to the program execution. Thus, the concrete domain is a partially ordered set $\langle C, \leqslant \rangle$ (e.g. integers powersets) and the abstract domain is another partially ordered set $\langle A, \sqsubseteq \rangle$ (e.g. intervals). The minimal amount of connection between these two worlds is a *concretization* functions

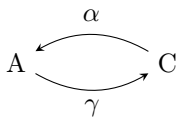


Figure 1.1: Galois connection between an abstract domain A and a concrete domain C

Definition 1.14 (Concretization)**.** A concretization function $\gamma : \langle A, \sqsubseteq\rangle \to \langle C, \leqslant\rangle$ is a *monotonic* function from an *abstract* partially ordered set $\langle A, \sqsubseteq\rangle$ to a *concrete* partially ordered set $\langle C, \leqslant\rangle$

Trough concretization we have a first notion of *soundness*

Definition 1.15 (Soundness)**.** Given an *abstract* domain A and a *concrete* domain C, we call $a \in A$ a *sound* abstraction of $c \in C$ iff $c \leqslant \gamma(a)$.

While monotonic concretizations are sufficient to reason about soundness, more structure is useful to design a sound and *accurate* analyzer. The standard abstract interpretation framework from [CC77] also assumes the existence of some monotonic *abstraction function* $\alpha : \langle C, \leqslant\rangle \to \langle A, \sqsubseteq\rangle$, such that $\langle \alpha, C, A, \gamma\rangle$ forms a Galois connection:

Definition 1.16 (Galois connection)**.** Given two partially ordered sets $\langle C, \leqslant\rangle, \langle A, \sqsubseteq\rangle$, the tuple $\langle \alpha, C, A, \gamma\rangle$ is a Galois connection if

- A, C are complete lattices;
- $\alpha : \langle C, \leqslant\rangle \to \langle A, \sqsubseteq\rangle$ and $\gamma : \langle A, \sqsubseteq\rangle \to \langle C, \leqslant\rangle$ are monotonic;
- for all $a \in A, c \in C$,
$$c \leqslant \gamma(a) \iff \alpha(c) \sqsubseteq a. \tag{1.1}$$

We denote $\langle \alpha, C, A, \gamma\rangle$ as $\langle C, \leqslant\rangle \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} \langle A, \sqsubseteq\rangle$.

Usually though we use an alternative characterization of Galois Connections:

Theorem 1.17. *$\langle C, \leqslant\rangle \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} \langle A, \sqsubseteq\rangle$ is a Galois connection iff the function pair $\langle \alpha, \gamma\rangle$ satisfies all the following properties:*

(1) α, γ are monotonic;

(2) $\forall c \in C \quad c \leqslant \gamma(\alpha(c))$ i.e., $\gamma \circ \alpha$ is extensive;

(3) $\forall a \in A \quad \alpha(\gamma(a)) \sqsubseteq a$, i.e., $\alpha \circ \gamma$ is reductive.

Proof. Assume that $\langle \alpha, \gamma\rangle$ satisfies (1.1), then we want to prove that the properties of Theorem 1.17 hold.

(1) Applying (1.1) with $a \triangleq \alpha(c)$ we get
$$c \leqslant \gamma(\alpha(c)) \tag{1.2}$$
i.e., $\gamma \circ \alpha$ is extensive, which is our first thesis.

(2) Applying (1.1) with $c \triangleq \gamma(a)$ we get
$$\alpha(\gamma(a)) \sqsubseteq a \tag{1.3}$$
i.e., $\alpha \circ \gamma$ is reductive, which is our second thesis.

(3) By (1) $\forall c, c' \in C$ it holds that $c \leqslant c' \implies c \leqslant \gamma(\alpha(c'))$. Hence, we can apply again (1.1) with $a \triangleq \alpha(c')$ and get that $\alpha(c) \sqsubseteq \alpha(c')$, i.e., α is monotonic.

(4) By (2) $\forall a, a' \in C$ it holds that $a \sqsubseteq a' \implies \alpha(\gamma(a)) \sqsubseteq a$. Hence, we can apply (1.1) with $c \triangleq \gamma(a)$ and get that $\gamma(a) \leqslant \gamma(a')$, i.e., γ is monotonic.

Assume conversely that the four properties hold. Then we want to prove that (1.1) holds.

($\implies$) First assume that $c \leqslant \gamma(a)$. Then $\alpha(c) \sqsubseteq \alpha(\gamma(a))$ by monotonicity of α and $\alpha(\gamma(a)) \sqsubseteq a$ by reductivity, hence $\alpha(c) \sqsubseteq a$.

($\impliedby$) Likewise, assume that $\alpha(c) \sqsubseteq a$. Then $\gamma(\alpha(c)) \leqslant \gamma(a)$ by monotonicity of γ and $c \leqslant \gamma(\alpha(c))$ by extensivity, hence $c \leqslant \gamma(a)$.

□

Galois connections carry with them some well known properties, that are useful to state best correct approximations (bca) and to prove the soundness by construction of the analyzer:

Theorem 1.18 (Galois connection properties)**.** *Given a Galois connection* $\langle C, \leqslant\rangle \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} \langle A, \sqsubseteq\rangle$ *we have:*

1. $\gamma \circ \alpha \circ \gamma = \gamma$ *and* $\alpha \circ \gamma \circ \alpha = \alpha$*;*
2. $\alpha \circ \gamma$ *and* $\gamma \circ \alpha$ *are idempotent;*
3. $\forall c \in C\ \alpha(c) = \sqcap\{a \mid c \leqslant \gamma(a)\}$*;*
4. $\forall a \in A\ \gamma(a) = \vee\{c \mid \alpha(c) \sqsubseteq a\}$*;*
5. α *maps concrete lubs to abstract lubs:*
$$\forall X \subseteq C \quad \exists \vee X \implies \alpha(\vee X) = \sqcup\{\alpha(x) \mid x \in X\}$$
6. γ *maps abstract glbs to concrete glbs:*
$$\forall X \subseteq A \quad \exists \sqcap X \implies \gamma(\sqcap X) = \wedge\{\gamma(x) \mid x \in X\}$$

Theorem 1.18 states two important properties of Galois connections: *soundness* and *optimality*. Recall that $c \leqslant \gamma(a)$ means by Definition 1.15 that a is a *sound* approximation of c. Then, given $c \in C$ recall that $c \leqslant \gamma(\alpha(c))$, which means that $\alpha(c)$ is a sound abstraction of c. Finally, Property 3 states that $\alpha(c)$ is the best (i.e., smallest) sound abstraction of c, i.e., the *optimal* abstraction.

Additionally, from the theorem we can derive the following corollary:

Corollary 1.19 (Best abstraction)**.** *If we have a Galois connection* $\langle \alpha, C, A, \gamma\rangle$*, then* $\forall c \in C, \alpha(c)$ *is the* best abstraction *of* c*, i.e., the smallest abstract element which is a sound abstraction of* c*.*

In general we saw that for a Galois connection $\gamma \circ \alpha$ is idempotent, and generally not the identity function, as abstracting looses precision. Concretizing however, should not loose precision, so we could expect $\alpha \circ \gamma$ to be the identity function. When this is the case, we have a *Galois insertion*:

Definition 1.20 (Galois Insertion)**.** A Galois connection $\langle C, \leqslant\rangle \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} \langle A, \sqsubseteq\rangle$ is a *Galois insertion* if one of the following, equivalent properties hold:

1. α is surjective: $\forall a \in A\ \exists c \in C \mid \alpha(c) = a$;
2. γ is injective: $\forall a, a' \in A\ \gamma(a) = \gamma(a') \implies a = a'$;
3. $\alpha \circ \gamma$ is the identity function.

We denote Galois insertions as $\langle C, \leqslant\rangle \underset{\alpha}{\overset{\gamma}{\leftrightarrows\!\!\!\!\rightarrow}} \langle A, \sqsubseteq\rangle$.

Next, we can show that given a Galois connection and by doing a *point-wise lifting* of the values in the concrete and abstract domain, we get another Galois connection. This will later be useful in Chapter **??** to lift proofs from a domain to its point-wise lifting.

Theorem 1.21. *Given a Galois connection* $\langle C, \leqslant\rangle \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} \langle A, \sqsubseteq\rangle$ *we can derive a new Galois connection with the* point wise lifting, *i.e.* $\langle S \to C, \dot{\leqslant}\rangle \underset{\dot{\alpha}}{\overset{\dot{\gamma}}{\leftrightarrows}} \langle S \to A, \dot{\sqsubseteq}\rangle$ *where*

$$\begin{aligned} f \mathrel{\dot{\leqslant}} f' &\triangleq \forall s \in S \quad f(s) \leqslant f'(s) \\ f \mathrel{\dot{\sqsubseteq}} f' &\triangleq \forall s \in S \quad f(s) \sqsubseteq f'(s) \\ \dot{\alpha}(f) &\triangleq \lambda s \in S.\alpha(f(s)) \\ \dot{\gamma}(f) &\triangleq \lambda s \in S.\gamma(f(s)) \end{aligned}$$

and S is an arbitrary set.

Proof.

$$\begin{aligned} \dot{\alpha}(c) \mathrel{\dot{\sqsubseteq}} a &\iff \forall x \in S \quad \alpha(c)(x) \sqsubseteq a(x) && \text{by definition} \\ &\iff \forall x \in S \quad c(x) \leqslant a(x) && \text{by (1.1)} \\ &\iff c \mathrel{\dot{\leqslant}} \dot{\gamma}(a) && \text{by definition} \end{aligned}$$

□

from this, we can derive the following

Theorem 1.22. *if* $\langle C, \leqslant\rangle \underset{\alpha}{\overset{\gamma}{\leftrightarrows\!\!\!\!\!\twoheadrightarrow}} \langle A, \sqsubseteq\rangle$ *is a Galois insertion, then its point-wise lifting is again a Galois insertion:*

$$\langle S \to C, \dot{\leqslant}\rangle \underset{\dot{\alpha}}{\overset{\dot{\gamma}}{\leftrightarrows\!\!\!\!\!\twoheadrightarrow}} \langle S \to A, \dot{\sqsubseteq}\rangle$$

Proof. By Th. 1.21 it holds that $\langle S \to C, \dot{\leqslant}\rangle \underset{\dot{\alpha}}{\overset{\dot{\gamma}}{\leftrightarrows}} \langle S \to A, \dot{\sqsubseteq}\rangle$. What we have to prove is that $\dot{\alpha} \circ \dot{\gamma} = \mathsf{id}$ knowing that $\alpha \circ \gamma = \mathsf{id}$.

$$\begin{aligned} (\dot{\alpha} \circ \dot{\gamma})(f) &= \dot{\alpha}(\lambda s \in S.\gamma(f(s))) && \text{by definition} \\ &= \lambda s \in S.(\alpha \circ \gamma)(f(s)) && \text{by definition} \\ &= \lambda s \in S.\mathsf{id}(f(s)) && \text{by hypothesis} \\ &= f && \text{by definition} \end{aligned}$$

hence $\dot{\alpha} \circ \dot{\gamma} = \mathsf{id}$, which means $\langle S \to C, \dot{\leqslant}\rangle \underset{\dot{\alpha}}{\overset{\dot{\gamma}}{\leftrightarrows\!\!\!\!\!\twoheadrightarrow}} \langle S \to A, \dot{\sqsubseteq}\rangle$. □

In this context we also need a way of ensuring abstract operations are sound (and occasionally) exact. Even by only using the concretization map and no Galois connection, the notion of sound and exact abstraction carries naturally from domain elements to domain operators:

Definition 1.23 (Sound and exact operator abstraction)**.** Let $\gamma : \langle A \sqsubseteq\rangle \to \langle C, \leqslant\rangle$ be a concretization map from an abstract domain $\langle A, \sqsubseteq\rangle$ to a concrete domain $\langle C, \leqslant\rangle$, $f : C \to C$ be a concrete operator and $g : A \to A$ an abstract operator.

1. g is a *sound abstraction* of f if $\forall a \in A \quad f(\gamma(a)) \leqslant \gamma(g(a))$;
2. g is an *exact abstraction* of f if $f \circ \gamma = \gamma \circ g$.

Notice that an exact abstraction is always sound. Another remarkable thing of Galois connections, is that along with this notion we can introduce the notion of *Best correct approximation*:

Definition 1.24 (Best correct approximation (bca))**.** Given a Galois connection $\langle \alpha, C, A, \gamma\rangle$ and a concrete operator $f : C \to C$, the *best abstraction* of f is given by $\alpha \circ f \circ \gamma$.

It is imperative to prioritize the modular and composable nature of our abstractions. As elaborated in subsequent chapters, the semantics of a program typically emerge from the composition of atomic semantic functions drawn from a finite library representing fundamental language operations. This framework lends itself well to a modular abstraction scheme, where abstract operators are designed exclusively for this foundational set of operations. By adhering to the same principles governing concrete semantics, these abstract operators can be composed effectively. This is facilitated by the inherent composability and accuracy of sound abstractions:

Theorem 1.25 (Operator composition)**.** *Let $f, f' : C \to C$ be concrete operators and $g, g' A \to A$ abstract operators. The following properties hold:*

(1) if g, g' are sound abstractions *of f and f' respectively and f is monotonic, then $g \circ g'$ is a sound abstraction of $f \circ f'$;*

(2) if g, g' are exact abstractions of f and f' respectively then $g \circ g'$ is an exact abstraction of $f \circ f'$.

Proof. We proceed to prove the two properties in order:

(1) g' is a sound abstraction of f', hence

$$\begin{aligned} \forall a \in A \quad & (f' \circ \gamma)(a) \leqslant (\gamma \circ g')(a) \\ & (f \circ f' \circ \gamma)(a) \leqslant (f \circ \gamma \circ g')(a) && \text{by monotonicity of } f \\ & (f \circ f' \circ \gamma)(a) \leqslant (f \circ \gamma \circ g')(a) \leqslant (\gamma \circ g \circ g')(a) && \text{by monotonicity of } g \end{aligned}$$

(2) since both $f \circ \gamma = \gamma \circ g$ and $f' \circ \gamma = \gamma \circ g'$ it holds that

$$f \circ f' \circ \gamma = f \circ \gamma \circ g' = \gamma \circ g \circ g'$$

□

1.3.2 Fixpoint approximations

Critical parts of program semantics are defined trough the idea of least fixpoints $\mathrm{lfp} f$ of some monotonic function or continuous operator $f : C \to C$ over the concrete domain $\langle C, \leqslant \rangle$. In order to abstract the computation of $\mathrm{lfp} f$ in the abstract domain $\langle A, \sqsubseteq \rangle$ the natural idea is to start with a sound abstraction $g : A \to A$ of f. Then there are many ways of approximate the fixpoint computation trough the use of g. We mention two, in order to see what its main problems are.

Kleene fixpoint. A first idea is to mimic the fixpoint computation with g instead of f. For instance by relying on the constructive definition of $\mathrm{lfp} f$ as the limit of an iteration sequence from Kleene's Theorem 1.13:

$$\mathrm{lfp}(f) = \sqcup\{f^i(\bot) \mid i \in \mathbb{N}\} \sqsubseteq \sqcup\{g^i(\bot) \mid i \in \mathbb{N}\} = \mathrm{lfp}(g)$$

Tarski fixpoint. Tarski fixpoint is instead based on the Tarski characterization of the fixpoint:

$$\mathrm{lfp}(f) = \sqcap\{x \in C \mid f(x) \sqsubseteq x\} \tag{1.4}$$

i.e., the least fixpoint of a monotonic function f over a complete lattice f is the greatest lower bound of the post-fixpoints. The observation is that any abstract post-fixpoint of a sound abstract represents, trough γ, a concrete fixpoint (by Theorem 1.18). The theorem however does not state how to compute a post-fixpoint of g in the abstract, but is nonetheless useful as it allows us to provide a sound answer (a post-fixpoint) even with abstract fixpoints are difficult to compute (as for infinite ascending chains) or non-existent at all.

As mentioned before, in order to solve the convergence problem in abstract domains in [CC77] the authors proposed to use Tarski's characterization to provide post fixpoint of infinite ascending chains, introducing a binary operator: the *widening* operator $\triangledown$.

Definition 1.26 (Widening operator)**.** A binary operator $\triangledown : A \times X \to A$ is a *widening operator* in an abstract domain $\langle A, \sqsubseteq \rangle$ if

1. it computes upper bounds:

$$\forall x, y \in A \quad x \sqsubseteq x \triangledown y \ \wedge \ y \sqsubseteq x \triangledown y;$$

2. it enforces convergence: for any sequence $\{y^i\}_{i \in \mathbb{N}}$ in A, the sequence $\{z^i\}_{i \in \mathbb{N}}$ computed as

$$\begin{aligned} z^0 &\triangleq y^0 \\ z^{i+1} &\triangleq z^i \mathbin{\triangle} y^{i+1} \end{aligned}$$

stabilizes in finite time: $\exists k \geqslant 0 \mid x^{k+1} = x^k$.

With the widening operator we enforce the termination of a sound abstract analyzer for the computation of upper bounds:

Theorem 1.27. *Let f be a monotonic operator in a complete concrete lattice and g a sound abstraction of f. Then the following iteration*

$$\begin{aligned} x^0 &\triangleq \bot \\ x^{i+1} &\triangleq x^i \triangledown g(x^i) \end{aligned}$$

converges in finite time, and its limit x is a sound abstraction of the least fixpoint lfp(f), i.e., lfp$(f) \leqslant \gamma(x)$.

Proof. Convergence is ensured by Property 2 of Definition 1.26, while the soundness is because of Equation (1.4) given that, when encountering a stable value $x^{i+1} = x^i$, then $f(x^i) \sqsubseteq x^i \triangledown f(x^i) = x^{i+1}$, i.e., x^i is an abstract post-fixpoint. □

Where the first point states that $\triangle$ refines its left argument while bringing a sound approximation, and the second point enforces termination.

Chapter 2

Framework

In order to talk about program properties we need a language to express such programs. We define the Imp language, made of regular commands and based on Kozen's Kleene algebra with tests, described in [Koz97].

2.1 The Imp language

We denote by $\mathbb{Z}$ the set of integers with the usual order, extended with the least and greatest elements $-\infty$ and $+\infty$, s.t. $-\infty \leqslant z \leqslant +\infty$ for all $z \in \mathbb{Z}$. We also extend addition and subtraction by letting, for all $z \in \mathbb{Z}$ it holds that $+\infty + z = +\infty - z = +\infty$ and $-\infty + z = -\infty + z = -\infty$. We focus on the following non-deterministic language.

$$\begin{aligned} \mathsf{Exp} \ni \mathsf{e} &::= \mathtt{x} \in I \mid \mathtt{x} := k \mid \mathtt{x} := \mathtt{y} + k \\ \mathsf{Imp}_s \ni \mathsf{D} &::= \mathsf{e} \mid \mathsf{D} + \mathsf{D} \mid \mathsf{D}; \mathsf{D} \\ \mathsf{Imp} \ni \mathsf{C} &::= \mathsf{D} \mid \mathsf{C} + \mathsf{C} \mid \mathsf{C}; \mathsf{C} \mid \mathsf{C}^* \mid \mathsf{fix}(\mathsf{C}) \end{aligned}$$

where $\mathtt{x}, \mathtt{y} \in \mathit{Var}$ a finite set of variables of interest, i.e., the variables appearing in the considered program, $I \in \mathbb{I}$ an *interval* (as defined in Definition 3.5), $a \in \mathbb{Z} \cup \{-\infty\}, b \in \mathbb{Z} \cup \{+\infty\}, a \leqslant b$ and $k \in \mathbb{Z}$ is any finite integer constant.

2.2 Semantics

In order to talk about program properties in our language, we first need to define its *semantics*. In the following section we introduce both a collecting semantics in order to reason about program *invariants* and a small step semantics, in order to reason about program *execution*.

Definition 2.1 (Semantics of Basic Expressions)**.** Let *environments* be the maps from the set of variables to their numerical value: $\mathsf{Env} \triangleq \{\rho \mid \rho : \mathit{Var} \to \mathbb{Z}\}$. For basic expressions $e \in \mathsf{Exp}$ the *concrete semantics* $(\!|\cdot|\!) : \mathsf{Exp} \to \mathsf{Env} \to \mathsf{Env}_\bot$ is inductively defined by:

$$(\!|\mathtt{x} \in I|\!)\rho \triangleq \begin{cases} \rho & \rho(\mathtt{x}) \in I \\ \bot & \text{otherwise} \end{cases}$$

$$(\!|\mathtt{x} := k|\!)\rho \triangleq \rho[\mathtt{x} \mapsto k]$$

$$(\!|\mathtt{x} := \mathtt{y} + k|\!)\rho \triangleq \begin{cases} \rho[\mathtt{x} \mapsto \rho(\mathtt{y}) + k] & \rho \neq \bot \\ \bot & \text{otherwise} \end{cases}$$

$$(\!|\mathtt{x} := \mathtt{y} - k|\!)\rho \triangleq \begin{cases} \rho[\mathtt{x} \mapsto \rho(\mathtt{y}) - k] & \rho \neq \bot \\ \bot & \text{otherwise} \end{cases}$$

where with $\mathsf{Env}_\bot$ we mean $\mathsf{Env} \cup \{\bot\}$.

The next building block is the concrete collecting semantics for the language, it associates each program in Imp to a function which, given a set of initial environments X "collects" the set of final states produced by executing the program from X.

Definition 2.2 (Concrete collecting semantics)**.** Let $\mathcal{C} \triangleq \langle \wp(\mathsf{Env}), \subseteq \rangle$ be a complete lattice called *concrete collecting domain*. The *concrete collecting semantics* for Imp is given by the total function $\langle\cdot\rangle : \mathsf{Imp} \to \mathcal{C} \to \mathcal{C}$ which maps each program $\mathsf{C} \in \mathsf{Imp}$ to a total function over the complete lattice $\mathcal{C}$, inductively defined as follows: given $X \in \mathcal{C}$

$$\begin{aligned}
\langle \mathsf{e} \rangle X &\triangleq \{ (\!|\mathsf{e}|\!)\rho \mid \rho \in X, (\!|\mathsf{e}|\!)\rho \neq \bot \} \\
\langle \mathsf{C}_1 + \mathsf{C}_2 \rangle X &\triangleq \langle \mathsf{C}_1 \rangle X \cup \langle \mathsf{C}_2 \rangle X \\
\langle \mathsf{C}_1 ; \mathsf{C}_2 \rangle X &\triangleq \langle \mathsf{C}_2 \rangle (\langle \mathsf{C}_1 \rangle X) \\
\langle \mathsf{C}^* \rangle X &\triangleq \bigcup_{i \in \mathbb{N}} \langle \mathsf{C} \rangle^i X \\
\langle \mathsf{fix}(\mathsf{C}) \rangle X &\triangleq \mathrm{lfp}(\lambda Y \in \wp(\mathsf{Env}).(X \cup \langle \mathsf{C} \rangle Y))
\end{aligned}$$

We observe that the semantics we described is additive:

Observation 2.3 (Additivity)**.** Given $\mathsf{C} \in \mathsf{Imp}$, $X, Y \in \mathcal{C}$,

$$\langle \mathsf{C} \rangle (X \cup Y) = \langle \mathsf{C} \rangle X \cup \langle \mathsf{C} \rangle Y$$

Proof. We will prove it by induction on the program C. Let's first explore the base cases.

Case (e). Therefore

$$\begin{aligned}
\langle \mathsf{e} \rangle (X \cup Y) &= \{ (\!|\mathsf{e}|\!)\rho \mid \rho \in X \cup Y, (\!|\mathsf{e}|\!)\rho \neq \bot \} \\
&= \{ (\!|\mathsf{e}|\!)\rho \mid \rho \in X \vee \rho \in Y, (\!|\mathsf{e}|\!)\rho \neq \bot \} \\
&= \{ (\!|\mathsf{e}|\!)\rho \mid \rho \in X, (\!|\mathsf{e}|\!)\rho \neq \bot \} \cup \{ (\!|\mathsf{e}|\!)\rho \mid \rho \in Y, (\!|\mathsf{e}|\!)\rho \neq \bot \} \\
&= \langle \mathsf{e} \rangle X \cup \langle \mathsf{e} \rangle Y
\end{aligned}$$

Next we can explore the inductive cases.

Case ($\mathsf{C}_1 + \mathsf{C}_2$). Therefore

$$\begin{aligned}
\langle \mathsf{C}_1 + \mathsf{C}_2 \rangle (X \cup Y) &= \langle \mathsf{C}_1 \rangle (X \cup Y) \cup \langle \mathsf{C}_2 \rangle (X \cup Y) && \text{by definition} \\
&= \langle \mathsf{C}_1 \rangle X \cup \langle \mathsf{C}_1 \rangle Y \cup \langle \mathsf{C}_2 \rangle X \cup \langle \mathsf{C}_2 \rangle Y && \text{by inductive hypothesis} \\
&= \langle \mathsf{C}_1 + \mathsf{C}_2 \rangle X \cup \langle \mathsf{C}_1 + \mathsf{C}_2 \rangle Y
\end{aligned}$$

Case ($\mathsf{C}_1 ; \mathsf{C}_2$). Therefore

$$\begin{aligned}
\langle \mathsf{C}_1 ; \mathsf{C}_2 \rangle (X \cup Y) &= \langle \mathsf{C}_2 \rangle (\langle \mathsf{C}_1 \rangle (X \cup Y)) && \text{by definition} \\
&= \langle \mathsf{C}_2 \rangle (\langle \mathsf{C}_1 \rangle X \cup \langle \mathsf{C}_1 \rangle Y) && \text{by inductive hypothesis} \\
&= \langle \mathsf{C}_2 \rangle (\langle \mathsf{C}_1 \rangle X) \cup \langle \mathsf{C}_2 \rangle (\langle \mathsf{C}_1 \rangle Y) && \text{by inductive hypothesis}
\end{aligned}$$

Case (C^*). Therefore

$$\langle \mathsf{C}^* \rangle (X \cup Y) = \bigcup_{i \in \mathbb{N}} \langle \mathsf{C} \rangle^i (X \cup Y)$$

in order to use the inductive hypothesis we have to show that

$$\forall i \in \mathbb{N} \quad \langle \mathsf{C} \rangle^i (X \cup Y) = \langle \mathsf{C} \rangle^i X \cup \langle \mathsf{C} \rangle^i Y$$

to do that, we work again by induction on i:

- the base case is $i = 0$ then $X \cup Y = X \cup Y$.
- For the inductive case we need to show that $i \implies i+1$:

$$\begin{aligned}
\langle \mathsf{C} \rangle^{i+1} (X \cup Y) &= \langle \mathsf{C} \rangle \left(\langle \mathsf{C} \rangle^{i} (X \cup Y) \right) \\
&= \langle \mathsf{C} \rangle \left(\langle \mathsf{C} \rangle^{i} X \cup \langle \mathsf{C} \rangle^{i} Y \right) && \text{by induction hypothesis on } i \\
&= \langle \mathsf{C} \rangle \left(\langle \mathsf{C} \rangle^{i} X \right) \cup \langle \mathsf{C} \rangle \left(\langle \mathsf{C} \rangle^{i} Y \right) && \text{by induction hypothesis on } \mathsf{C} \\
&= \langle \mathsf{C} \rangle^{i+1} X \cup \langle \mathsf{C} \rangle^{i+1} Y
\end{aligned}$$

Therefore we can use the inductive hypothesis internally and say

$$\begin{aligned}
\langle \mathsf{C}^* \rangle (X \cup Y) &= \bigcup_{i \in \mathbb{N}} \langle \mathsf{C} \rangle^{i} (X \cup Y) \\
&= \bigcup_{i \in \mathbb{N}} \left(\langle \mathsf{C} \rangle^{i} X \cup \langle \mathsf{C} \rangle^{i} Y \right) && \text{for the later statement} \\
&= \left(\bigcup_{i \in \mathbb{N}} \langle \mathsf{C} \rangle^{i} X \right) \cup \left(\bigcup_{i \in \mathbb{N}} \langle \mathsf{C} \rangle^{i} Y \right) \\
&= \langle \mathsf{C}^* \rangle X \cup \langle \mathsf{C}^* \rangle Y && \square
\end{aligned}$$

We can also observe that a program induces a monotone function in the concrete domain $\mathcal{C}$:

Lemma 2.4. *Given a program $\mathsf{C} \in \mathsf{Imp}$, the semantic function $\langle \mathsf{C} \rangle : \mathcal{C} \to \mathcal{C}$ is monotone.*

Proof. We can prove this by induction on the program $\mathsf{C} \in \mathsf{Imp}$. Let $X, Y \in \mathcal{C}, X \subseteq Y$. We want to prove that $\langle \mathsf{C} \rangle X \subseteq \langle \mathsf{C} \rangle Y$.

Case (e). In this case

$$\begin{aligned}
\langle \mathsf{e} \rangle X &= \{ (\!| \mathsf{e} |\!) \rho \mid \rho \in X, (\!| \mathsf{e} |\!) \rho \neq \bot \} \\
\langle \mathsf{e} \rangle Y &= \{ (\!| \mathsf{e} |\!) \rho \mid \rho \in Y, (\!| \mathsf{e} |\!) \rho \neq \bot \}
\end{aligned}$$

$X \subseteq Y$ therefore $\rho \in X \implies \rho \in Y$ which also means that $\rho' \in \langle \mathsf{e} \rangle X \implies \rho' \in \langle \mathsf{e} \rangle Y$, therefore $\langle \mathsf{e} \rangle X \subseteq \langle \mathsf{e} \rangle Y$

Case ($\mathsf{C}_1 + \mathsf{C}_2$). In this case we need to show that $\langle \mathsf{C}_1 + \mathsf{C}_2 \rangle X \subseteq \langle \mathsf{C}_1 + \mathsf{C}_2 \rangle Y$

$$\begin{aligned}
\langle \mathsf{C}_1 + \mathsf{C}_2 \rangle X &= \langle \mathsf{C}_1 \rangle X \cup \langle \mathsf{C}_2 \rangle X \\
\langle \mathsf{C}_1 + \mathsf{C}_2 \rangle Y &= \langle \mathsf{C}_1 \rangle Y \cup \langle \mathsf{C}_2 \rangle Y
\end{aligned}$$

by inductive hypothesis both $\langle \mathsf{C}_1 \rangle X \subseteq \langle \mathsf{C}_1 \rangle Y$ and $\langle \mathsf{C}_2 \rangle X \subseteq \langle \mathsf{C}_2 \rangle Y$ and therefore $\langle \mathsf{C}_1 + \mathsf{C}_2 \rangle X \subseteq \langle \mathsf{C}_1 + \mathsf{C}_2 \rangle Y$.

Case ($\mathsf{C}_1; \mathsf{C}_2$). Therefore we need to show that $\langle \mathsf{C}_1; \mathsf{C}_2 \rangle X \subseteq \langle \mathsf{C}_1; \mathsf{C}_2 \rangle Y$

$$\begin{aligned}
\langle \mathsf{C}_1; \mathsf{C}_2 \rangle X &= \langle \mathsf{C}_2 \rangle (\langle \mathsf{C}_1 \rangle X) \\
\langle \mathsf{C}_1; \mathsf{C}_2 \rangle Y &= \langle \mathsf{C}_2 \rangle (\langle \mathsf{C}_1 \rangle Y)
\end{aligned}$$

By induction hypothesis $\langle \mathsf{C}_1 \rangle X \subseteq \langle \mathsf{C}_1 \rangle Y$, and by induction hypothesis again $\langle \mathsf{C}_2 \rangle (\langle \mathsf{C}_1 \rangle X) \subseteq \langle \mathsf{C}_2 \rangle (\langle \mathsf{C}_1 \rangle Y)$ which means $\langle \mathsf{C}_1; \mathsf{C}_2 \rangle X \subseteq \langle \mathsf{C}_1; \mathsf{C}_2 \rangle Y$.

Case (C^*). Therefore we need to show that $\langle \mathsf{C}^* \rangle X \subseteq \langle \mathsf{C}^* \rangle Y$.

$$\begin{aligned}
\langle \mathsf{C}^* \rangle X &= \bigcup_{i \in \mathbb{N}} \langle \mathsf{C} \rangle^{i} X \\
\langle \mathsf{C}^* \rangle Y &= \bigcup_{i \in \mathbb{N}} \langle \mathsf{C} \rangle^{i} Y
\end{aligned}$$

what we need to prove is that

$$\forall j \in \mathbb{N} \quad \bigcup_{i=0}^{j} \langle \mathsf{C} \rangle^i X \subseteq \bigcup_{i=0}^{j} \langle \mathsf{C} \rangle^i Y$$

we can do this by induction on j:

- $j = 0$ therefore $X \subseteq Y$ which is true by hypothesis.
- Now we need to work on the inductive case $j \implies j+1$. Notice that it holds that

$$\begin{aligned} \bigcup_{i=0}^{k+1} \langle \mathsf{C} \rangle^i X &= X \cup \bigcup_{i=1}^{k+1} \langle \mathsf{C} \rangle^i X && \text{by definition} \\ &= X \cup \langle \mathsf{C} \rangle \left(\bigcup_{i=0}^{k} \langle \mathsf{C} \rangle^i X \right) && \text{by additivity} \end{aligned}$$

  and also for Y

$$\bigcup_{i=0}^{k+1} \langle \mathsf{C} \rangle^i Y = Y \cup \langle \mathsf{C} \rangle \left(\bigcup_{i=0}^{k} \langle \mathsf{C} \rangle^i Y \right)$$

  Also notice that

  (i) $X \subseteq Y$ by hypothesis;
  (ii) $\bigcup_{i=0}^{k} \langle \mathsf{C} \rangle^i X \subseteq \bigcup_{i=0}^{k} \langle \mathsf{C} \rangle^i Y$ by inductive hypothesis;
  (iii) $\langle \mathsf{C} \rangle \left(\bigcup_{i=0}^{k} \langle \mathsf{C} \rangle^i X \right) \subseteq \langle \mathsf{C} \rangle \left(\bigcup_{i=0}^{k} \langle \mathsf{C} \rangle^i Y \right)$ by additivity.

  Therefore

$$\bigcup_{i=0}^{k+1} \langle \mathsf{C} \rangle^i X = X \cup \langle \mathsf{C} \rangle \left(\bigcup_{i=0}^{k} \langle \mathsf{C} \rangle^i X \right) \subseteq Y \cup \langle \mathsf{C} \rangle \left(\bigcup_{i=0}^{k} \langle \mathsf{C} \rangle^i Y \right) = \bigcup_{i=0}^{k+1} \langle \mathsf{C} \rangle^i Y$$

□

Proposition 2.5. *Kleene star (C^*) and the fixpoint ($\mathsf{fix}(\mathsf{C})$) share the same concrete semantics:*

$$\langle \mathsf{C}^* \rangle = \langle \mathsf{fix}(\mathsf{C}) \rangle$$

Proof. To start, let $X \in \mathcal{C}, f = \lambda Y \in \mathcal{C}.\, (X \cup \langle \mathsf{C} \rangle Y)$ and recall that $f^0 X = X$ and $f^{n+1} X = X \cup \langle \mathsf{C} \rangle (f^n X)$.

$$\begin{aligned} \langle \mathsf{fix}(\mathsf{C}) \rangle X = \mathrm{lfp}(f) &= \bigcup \{ f^n \perp \mid n \in \mathbb{N} \} && \text{by fixpoint theorem (1.13)} \\ &= \bigcup_{i \in \mathbb{N}} \left(X \cup \langle \mathsf{C} \rangle^i X \right) && \text{by definition} \\ &= \bigcup_{i \in \mathbb{N}} \langle \mathsf{C} \rangle^i X \\ &= \langle \mathsf{C}^* \rangle X \end{aligned}$$

□

This will not be the case for the abstract semantics (cf. Example 3.12), where the Kleene star can be more precise than the fixpoint semantics, but harder to compute and, as such, less suited for analysis. For the concrete semantics, however, since they are the same in the next proofs we only explore the case C^* since it captures also $\mathsf{fix}(\mathsf{C})$. Since for a given program C and a set of initial states $X \in \mathcal{C}$ the collecting semantics $\langle \mathsf{C} \rangle X$ expresses properties that hold at the end of the execution of C we will in the following chapters usually refer to $\langle \mathsf{C} \rangle X$ as program *invariant*.

Notation 2.6 (Singleton shorthand)**.** Sometimes we need to consider the semantics over the singleton set $\{\rho\}$. In these cases we will write $\langle \mathsf{C} \rangle \rho$ instead of $\langle \mathsf{C} \rangle \{\rho\}$.

2.2.1 Syntactic sugar

We define some syntactic sugar for the language. In the next chapters we will often use the syntactic sugar instead of its real equivalent for the sake of simplicity.

$$\begin{aligned}
\mathtt{x} \in [a,b] &= \mathtt{x} \in I && \text{with } I = [a,b] \\
\mathtt{x} \leqslant k &= \mathtt{x} \in (-\infty, k] \\
\mathtt{x} > k &= \mathtt{x} \in [k+1, +\infty) \\
\mathsf{true} &= \mathtt{x} \in \mathbb{Z} \\
\mathsf{false} &= \mathtt{x} \in \varnothing \\
\mathtt{x} \in I_1 \vee \mathtt{x} \in I_2 &= (\mathtt{x} \in I_1) + (\mathtt{x} \in I_2) \\
\mathtt{x} \in I_1 \wedge \mathtt{x} \in I_2 &= (\mathtt{x} \in I_1); (\mathtt{x} \in I_2) \\
\mathsf{if}\ b\ \mathsf{then}\ C_1\ \mathsf{else}\ C_2 &= (\mathsf{e}; \mathsf{C}_1) + (\neg \mathsf{e}; \mathsf{C}_2) \\
\mathsf{while}\ b\ \mathsf{do}\ C &= \mathsf{fix}(b; \mathsf{C}); \neg b \\
\mathtt{x}\mathtt{+}\mathtt{+} &= \mathtt{x} := \mathtt{x} + 1
\end{aligned}$$

2.2.2 Small step semantics

Now that we have defined the collecting semantics to express program properties, we need the small step semantics to talk about program execution. We start by defining *program states*: $\mathsf{State} \triangleq \mathsf{Imp} \times \mathsf{Env}$ tuples of programs and program environments. With states we can define our small step semantics:

Definition 2.7 (Small step semantics)**.** The small step transition relation for the language Imp $\rightarrow$: $\mathsf{State} \times (\mathsf{State} \cup \mathsf{Env})$ is defined by the following rules:

$$\frac{(\!|e|\!)\rho \neq \bot}{\langle \mathsf{e}, \rho \rangle \rightarrow (\!|e|\!)\rho}\ \text{expr}$$

$$\frac{}{\langle \mathsf{C}_1 + \mathsf{C}_2, \rho \rangle \rightarrow \langle \mathsf{C}_1, \rho \rangle}\ \text{sum}_1 \qquad \frac{}{\langle \mathsf{C}_1 + \mathsf{C}_2, \rho \rangle \rightarrow \langle \mathsf{C}_2, \rho \rangle}\ \text{sum}_2$$

$$\frac{\langle \mathsf{C}_1, \rho \rangle \rightarrow \langle \mathsf{C}_1', \rho' \rangle}{\langle \mathsf{C}_1; \mathsf{C}_2, \rho \rangle \rightarrow \langle \mathsf{C}_1'; \mathsf{C}_2, \rho' \rangle}\ \text{comp}_1 \qquad \frac{\langle \mathsf{C}_1, \rho \rangle \rightarrow \rho'}{\langle \mathsf{C}_1; \mathsf{C}_2, \rho \rangle \rightarrow \langle \mathsf{C}_2, \rho' \rangle}\ \text{comp}_2$$

$$\frac{}{\langle \mathsf{C}^*, \rho \rangle \rightarrow \langle \mathsf{C}; \mathsf{C}^*, \rho \rangle}\ \text{star} \qquad \frac{}{\langle \mathsf{C}^*, \rho \rangle \rightarrow \rho}\ \text{star}_{\text{fix}}$$

In the following chapters we will usually use the following notation to talk about program execution:

- $\rightarrow^+$ is the transitive closure of the relation $\rightarrow$;
- $\rightarrow^*$ is the reflexive and transitive closure of the relation $\rightarrow$.

With the following lemma we introduce a link between the small step semantics and the concrete collecting semantics: the invariant of a program is the collection of all the environments the program halts on when executing.

Lemma 2.8. *For any* $\mathsf{C} \in \mathsf{Imp}, X \in \wp(\mathsf{Env})$

$$\langle \mathsf{C} \rangle X = \{\rho' \in \mathsf{Env} \mid \rho \in X, \langle \mathsf{C}, \rho \rangle \rightarrow^* \rho'\}$$

where $\rightarrow^*$ is the reflexive and transitive closure of the $\rightarrow$ relation.

Proof. by induction on C:

Case (e). In this case it holds that $\langle \mathsf{e} \rangle X = \{(\!|e|\!)\rho \mid \rho \in X \wedge (\!|e|\!)\rho \neq \bot\}$, $\forall \rho \in X. \langle \mathsf{e}, \rho \rangle \to (\!|e|\!)\rho$ if $(\!|e|\!)\rho \neq \bot$, and because of the expr rule

$$\langle \mathsf{e} \rangle X = \{(\!|e|\!)\rho \mid \rho \in X \wedge (\!|e|\!)\rho \neq \bot\} = \{\rho' \in \mathsf{Env} \mid \rho \in X \langle \mathsf{e}, \rho \rangle \to \rho'\}$$

Case ($\mathsf{C}_1 + \mathsf{C}_2$). In this case $\langle \mathsf{C}_1 + \mathsf{C}_2 \rangle X = \langle \mathsf{C}_1 \rangle X \cup \langle \mathsf{C}_2 \rangle X$, $\forall \rho \in X. \langle \mathsf{C}_1 + \mathsf{C}_2, \rho \rangle \to \langle \mathsf{C}_1, \rho \rangle \vee \langle \mathsf{C}_1 + \mathsf{C}_2, \rho \rangle \to \langle \mathsf{C}_2, \rho \rangle$ respectively according to rules sum_1 and sum_2. By inductive hypothesis

$$\langle \mathsf{C}_1 \rangle X = \{\rho' \in \mathsf{Env} \mid \rho \in X, \langle \mathsf{C}_1, \rho \rangle \to^* \rho'\} \quad \langle \mathsf{C}_2 \rangle X = \{\rho' \in \mathsf{Env} \mid \rho \in X, \langle \mathsf{C}_2, \rho \rangle \to^* \rho'\}$$

Therefore

$$\begin{aligned}
\langle \mathsf{C}_1 + \mathsf{C}_2 \rangle X &= \langle \mathsf{C}_1 \rangle X \cup \langle \mathsf{C}_2 \rangle X && \text{(by definition)} \\
&= \{\rho' \in \mathsf{Env} \mid \rho \in X. \langle \mathsf{C}_1, \rho \rangle \to^* \rho'\} \cup \{\rho' \in \mathsf{Env} \mid \rho \in X, \langle \mathsf{C}_2, \rho \rangle \to^* \rho'\} && \text{(by ind. hp)} \\
&= \{\rho' \in \mathsf{Env} \mid \rho \in X. \langle \mathsf{C}_1, \rho \rangle \to^* \rho' \vee \langle \mathsf{C}_2, \rho \rangle \to^* \rho'\} \\
&= \{\rho' \in \mathsf{Env} \mid \rho \in X. \langle \mathsf{C}_1 + \mathsf{C}_2, \rho \rangle \to^* \rho'\}
\end{aligned}$$

Case ($\mathsf{C}_1; \mathsf{C}_2$). In this case $\langle \mathsf{C}_1; \mathsf{C}_2 \rangle X = \langle \mathsf{C}_2 \rangle (\langle \mathsf{C}_1 \rangle X)$. By inductive hp $\langle \mathsf{C}_1 \rangle X = \{\rho' \in \mathsf{Env} \mid \rho \in X, \langle \mathsf{C}_1, \rho \rangle \to^* \rho'\} = Y$, by inductive hp again $\langle \mathsf{C}_2 \rangle Y = \{\rho' \in \mathsf{Env} \mid \rho \in Y, \langle \mathsf{C}_2, \rho \rangle \to^* \rho'\}$. Therefore

$$\begin{aligned}
\langle \mathsf{C}_1; \mathsf{C}_2 \rangle X &= \langle \mathsf{C}_2 \rangle (\langle \mathsf{C}_1 \rangle X) && \text{(by definition)} \\
&= \{\rho' \in \mathsf{Env} \mid \rho'' \in \{\rho''' \mid \rho \in X, \langle \mathsf{C}_1, \rho \rangle \to^* \rho'''\}, \langle \mathsf{C}_2, \rho'' \rangle \to^* \rho'\} && \text{(by ind. hp)} \\
&= \{\rho' \in \mathsf{Env} \mid \rho \in X. \langle \mathsf{C}_1, \rho \rangle \to^* \rho'' \wedge \langle \mathsf{C}_2, \rho'' \rangle \to^* \rho'\} && \text{(by composition lemma)} \\
&= \{\rho' \in \mathsf{Env} \mid \rho \in X. \langle \mathsf{C}_1; \mathsf{C}_2, \rho \rangle \to^* \rho'\}
\end{aligned}$$

Case (C^*). Then, in this case $\langle \mathsf{C}^* \rangle X = \cup_{i \in \mathbb{N}} \langle \mathsf{C} \rangle^i X$

$$\begin{aligned}
\langle \mathsf{C}^* \rangle X &= \bigcup_{i \in \mathbb{N}} \langle \mathsf{C} \rangle^i X \\
&= \bigcup_{i \in \mathbb{N}} \{\rho' \in \mathsf{Env} \mid \rho \in X. \langle \mathsf{C}^i, \rho \rangle \to^* \rho'\} && \text{by inductive hypothesis} \\
&= \{\rho' \in \mathsf{Env} \mid \rho \in X. \vee_{i \in \mathbb{N}} \langle \mathsf{C}^i, \rho \rangle \to^* \rho'\} \\
&= \{\rho' \in \mathsf{Env} \mid \rho \in X. \langle \mathsf{C}^*, \rho \rangle \to^* \rho'\}
\end{aligned}$$

□

Note that $\langle \mathsf{C} \rangle X = \varnothing \iff \nexists \rho' \in \mathsf{Env}, \rho \in X \mid \langle \mathsf{C}, \rho \rangle \to^* \rho'$, in other words the collecting semantics of some program C starting from some states $X \in \mathcal{C}$ is empty iff the program never halts on some state ρ'. Another observation is that due to non-determinism a program can halt on multiple final states, or have one branch of execution that halts on some final state, while the other never halts on any final state. Non-determinism implies that there are two different types of termination, intuitively a program can *always* halt or *partially* halt. We will better explore this concept in the next chapter.

2.3 Transition system

With the set of states State, the set of environments Env and the small step operational semantics $\to$ we define a transition system, this will be useful to define universal and partial termination and to reason about program properties in the next chapters.

Definition 2.9 (Transition system)**.** The transition system for the language Imp is

$$\mathsf{TS} \triangleq \langle \mathsf{State} \cup \mathsf{Env}, \mathsf{Env}, \to \rangle$$

where

- $\mathsf{State} \cup \mathsf{Env}$ is the set of configurations in the system;
- Env is the set of terminal states;
- $\to$ is the small step semantics defined in Definition 2.7, which describes the transition relations in the system.

With the concept of derivation sequences we can define what we mean for *partial* and *universal* termination.

Definition 2.10 (Partial termination)**.** Let $\mathsf{C} \in \mathsf{Imp}, \rho \in \mathsf{Env}$. We say C *partially halts* on ρ when there is at least one derivation sequence of finite length in the transition system starting with $\langle \mathsf{C}, \rho \rangle$ and ending in some state ρ':

$$\langle \mathsf{C}, \rho \rangle \downarrow \iff \exists k \in \mathbb{N} \mid \langle \mathsf{C}, \rho \rangle \to^k \rho'.$$

Dually

$$\langle \mathsf{C}, \rho \rangle \Uparrow \iff \neg \langle \mathsf{C}, \rho \rangle \downarrow$$

a program *always loops* if there is no finite derivation sequence in its transition system that leads to a final environment.

Definition 2.11 (Universal termination)**.** Let $\mathsf{C} \in \mathsf{Imp}, \rho \in \mathsf{Env}$. We say$\mathsf{C}$ *partially loops* on ρ when there is at least one derivation sequence of infinite length in the transition system starting from $\langle \mathsf{C}, \rho \rangle$:

$$\langle \mathsf{C}, \rho \rangle \uparrow \iff \forall k \in \mathbb{N}\ \langle \mathsf{C}, \rho \rangle \to^k \langle \mathsf{C}', \rho' \rangle \quad \text{for some } \mathsf{C}' \in \mathsf{Imp}, \rho' \in \mathsf{Env}.$$

Dually

$$\langle \mathsf{C}, \rho \rangle \Downarrow \iff \neg \langle \mathsf{C}, \rho \rangle \uparrow$$

a program *universally halts* on ρ iff there is no infinite derivation sequence starting from $\langle \mathsf{C}, \rho \rangle$ in the transition systems.

Example 2.14 shows a program that partially halts, while Example 2.13 shows a program that always loops. Notice that the absence of infinite derivation sequences implies that $\mathsf{TS}(\langle \mathsf{C}, \rho \rangle)$ is finite. Example 2.14 shows a program that partially loops, while example 2.12 shows a program that universally halts.

Example 2.12. Consider the program

$$\mathtt{x} := 0;$$

it universally halts, since $\forall \rho \in \mathsf{Env}, \rho \neq \bot$

$$\langle \mathtt{x} := 0, \rho \rangle \to \rho[\mathtt{x} \mapsto 0]$$

according to the expr rule in definition 2.7. Therefore $\langle (\mathtt{x} := 0), \rho \rangle \Downarrow \forall \rho \in \mathsf{Env} \setminus \{\bot\}$.

Example 2.13. Consider the program P

$$(\mathtt{x} \geqslant 0; \mathtt{x{+}{+}})^*; \mathtt{x} < 0$$

The program never halts on $\forall \rho \in \mathsf{Env}$ s.t. $\rho(\mathtt{x}) \geqslant 0$. In fact in these cases it builds the transition system in figure 2.1, where the infinite derivation sequence

$$\langle (\mathtt{x} \geqslant 0; \mathtt{x{+}{+}})^*; x < 0, \rho \rangle \to^* \langle (\mathtt{x} \geqslant 0; \mathtt{x{+}{+}})^*; x < 0, \rho[\mathtt{x} \mapsto \rho(\mathtt{x}) + 1] \rangle \to^* \dots$$

$$\dots \to^* \langle (\mathtt{x} \geqslant 0; \mathtt{x{+}{+}})^*; x < 0, \rho[\mathtt{x} \mapsto \rho(\mathtt{x}) + k] \rangle \to^* \dots$$

is always present.

$$\langle (\mathtt{x} \geqslant 0; \mathtt{x{+}{+}})^*; \mathtt{x} < 0, \rho\rangle \longrightarrow \langle \mathtt{x} < 0, \rho\rangle \not\to$$
$$\downarrow$$
$$\langle \mathtt{x} \geqslant; 0\mathtt{x{+}{+}}; (\mathtt{x} \geqslant 0; \mathtt{x{+}{+}})^*; \mathtt{x} < 0, \rho\rangle$$
$$\downarrow^*$$
$$\langle (\mathtt{x} \geqslant 0; \mathtt{x{+}{+}})^*; \mathtt{x} < 0, \rho[\mathtt{x} \mapsto \rho(\mathtt{x}) + 1]\rangle \longrightarrow \langle \mathtt{x} < 0, \rho[\mathtt{x} \mapsto \rho(\mathtt{x}) + 1]\rangle \not\to$$
$$\downarrow^*$$
$$\langle (\mathtt{x} \geqslant 0; \mathtt{x{+}{+}})^*; \mathtt{x} < 0, \rho[\mathtt{x} \mapsto \rho(\mathtt{x}) + k]\rangle \longrightarrow \langle \mathtt{x} < 0, \rho[\mathtt{x} \mapsto \rho(\mathtt{x}) + k]\rangle \not\to$$

Figure 2.1: Transition system of $(\mathtt{x} \geqslant 0; \mathtt{x{+}{+}})^*; \mathtt{x} < 0$

Example 2.14. Consider the program

$$(\mathtt{x{+}{+}})^*$$

it partially halts ($\langle (\mathtt{x{+}{+}})^*, \rho\rangle \downarrow$), as according to the transition rule star_{fix} $\exists \rho \in \mathsf{Env}$ s.t.

$$\frac{\rho \neq \bot}{\langle (\mathtt{x{+}{+}})^*, \rho\rangle \to \rho}\ \text{star}_{\text{fix}}$$

But it also partially loops ($\langle (\mathtt{x{+}{+}})^*, \rho\rangle \uparrow$). In fact we can build the infinite derivation sequence

$$\langle (\mathtt{x{+}{+}})^*, \rho[\mathtt{x} \mapsto 0]\rangle \to^* \langle (\mathtt{x{+}{+}})^*, \rho[\mathtt{x} \mapsto 1]\rangle \to^* \langle (\mathtt{x{+}{+}})^*, \rho[\mathtt{x} \mapsto 2]\rangle \to^* \dots$$

Other useful lemmas in the system are the composition and decomposition lemma.

Lemma 2.15 (Decomposition lemma)**.** *If $\langle \mathsf{C}_1; \mathsf{C}_2, \rho\rangle \to^k \rho''$, then there exists a state ρ' and a natural number k_1, k_2 s.t. $\langle \mathsf{C}_1, \rho\rangle \to^{k_1} \rho'$ and $\langle \mathsf{C}_2, \rho'\rangle \to^{k_2} \rho''$, where $k_1 + k_2 = k$*

Proof. The proof is on induction on $k \in \mathbb{N}$, i.e., by induction on the length of the derivation sequence.

Case ($k = 0$). Then

$$\langle \mathsf{C}_1; \mathsf{C}_2, \rho\rangle \to^0 \rho''$$

holds vacuously since $\langle \mathsf{C}_1; \mathsf{C}_2, \rho\rangle$ and ρ'' are different.

Case ($k \implies k + 1$). Then

$$\langle \mathsf{C}_1; \mathsf{C}_2, \rho\rangle \to^{k+1} \rho''$$

can be written as

$$\langle \mathsf{C}_1; \mathsf{C}_2, \rho\rangle \to \gamma \to^k \rho''$$

for some configuration γ. Now two cases apply, depending on the use of either comp_1 or comp_2 rules.

Case [comp_1]. Then $\gamma = \langle \mathsf{C}_1'; \mathsf{C}_2, \rho'\rangle$ and $\langle \mathsf{C}_1; \mathsf{C}_2, \rho\rangle \to \langle \mathsf{C}_1'; \mathsf{C}_2, \rho'\rangle$ because $\langle \mathsf{C}_1, \rho\rangle \to \langle \mathsf{C}_1', \rho'\rangle$. Therefore we have

$$\langle \mathsf{C}_1'; \mathsf{C}_2, \rho'\rangle \to^k \rho''$$

Here we can use the induction hypothesis since the derivation sequence is shorter than the one we started with. Hence $\exists \rho''' \in \mathsf{Env}$ and natural numbers k_1, k_2 s.t.

$$\langle \mathsf{C}_1'; \rho'\rangle \to^{k_1} \rho''' \quad \wedge \quad \langle \mathsf{C}_2, \rho'''\rangle \to^{k_2} \rho''$$

where $k_1 + k_2 = k$. Hence it holds that

$$\langle \mathsf{C}_1, \rho\rangle \to^{k_1+1} \rho'''$$

and since $(k_1 + 1) + k_2 = k + 1$ it holds that

$$\langle \mathsf{C}_1; \mathsf{C}_2, \rho\rangle \to^{k+1} \rho''$$

which is our thesis.

Case [$\mathsf{comp_2}$]. In this case $\gamma = \langle \mathsf{C}_2, \rho' \rangle$ because $\langle \mathsf{C}_1, \rho \rangle \to \rho'$ and it holds that

$$\langle \mathsf{C}_1; \mathsf{C}_2, \rho \rangle \to \langle \mathsf{C}_2, \rho' \rangle \to^k \rho''$$

Hence our thesis follows by using the inductive hypothesis on $\langle \mathsf{C}_2, \rho' \rangle$ and by choosing $k_1 = 1, k_2 = k$. □

From the latter theorem follows its corollary, which abstracts the value of k.

Corollary 2.16. *If* $\langle \mathsf{C}_1; \mathsf{C}_2, \rho \rangle \to^* \rho''$ *then* $\exists \rho'$ *s.t.* $\langle \mathsf{C}_1, \rho \rangle \to^* \rho'$ *and* $\langle \mathsf{C}_2, \rho' \rangle \to^* \rho''$.

The second lemma states a similar but inverted property:

Lemma 2.17 (Composition lemma)**.** *If* $\langle \mathsf{C}_1, \rho \rangle \to^k \rho'$ *then* $\langle \mathsf{C}_1; \mathsf{C}_2, \rho \rangle \to^k \langle \mathsf{C}_2, \rho' \rangle$

Proof. The proof works again by induction on the length k of the derivation sequence:

Case ($k = 0$). In this case the statement vacuously holds as $\langle \mathsf{C}_1, \rho \rangle$ and ρ' are different.

Case ($k \implies k+1$). In this case we have to prove that if $\langle \mathsf{C}_1, \rho \rangle \to^{k+1} \rho'$ then $\langle \mathsf{C}_1; \mathsf{C}_2, \rho \rangle \to^{k+1} \rho'$. To start we can notice that $\langle \mathsf{C}_1, \rho \rangle \to^{k+1} \rho'$ means that we have 2 cases:

(1) either $k = 0$, hence $\langle \mathsf{C}_1, \rho \rangle \to \rho'$. But in this case we can use [$\mathsf{comp_2}$] and deduce that

$$\frac{\langle \mathsf{C}_1, \rho \rangle \to \rho'}{\langle \mathsf{C}_1; \mathsf{C}_2, \rho \rangle \to \langle \mathsf{C}_2, \rho' \rangle}$$

(2) Or $k > 0$, which means

$$\langle \mathsf{C}_1, \rho \rangle \to \langle \mathsf{C}_1', \rho'' \rangle \to^k \rho'. \tag{2.1}$$

In this case we can use [$\mathsf{comp_1}$] and notice that

$$\frac{\langle \mathsf{C}_1, \rho \rangle \to \langle \mathsf{C}_1', \rho'' \rangle}{\langle \mathsf{C}_1; \mathsf{C}_2, \rho \rangle \to \langle \mathsf{C}_1'; \mathsf{C}_2, \rho'' \rangle}$$

Now, by induction on k in (2.1) we know that $\langle \mathsf{C}_1'; \mathsf{C}_2, \rho'' \rangle \to^k \rho'$, hence

$$\langle \mathsf{C}_1; \mathsf{C}_2, \rho \rangle \to \langle \mathsf{C}_1'; \mathsf{C}_2, \rho'' \rangle \to^k \rho'$$

which is our thesis.

□

Corollary 2.18. *If* $\langle \mathsf{C}_1, \rho \rangle \to^* \rho'$ *then* $\langle \mathsf{C}_1; \mathsf{C}_2, \rho \rangle \to^* \langle \mathsf{C}_2, \rho' \rangle$.

In order to better talk about the intermediate states in the execution of a program we also introduce the notion of reducts:

Definition 2.19 (Reducts)**.** Let Imp^* denotes the set whose elements are statements in Imp. The reduction function $\mathsf{red} : \mathsf{Imp} \to \mathsf{Imp}^*$ is recursively defined by the following clauses:

$$\begin{aligned}
\mathsf{red}(\mathsf{e}) &\triangleq \{\mathsf{e}\} \\
\mathsf{red}(\mathsf{C}_1 + \mathsf{C}_2) &\triangleq \{\mathsf{C}_1 + \mathsf{C}_2\} \cup \mathsf{red}(\mathsf{C}_1) \cup \mathsf{red}(\mathsf{C}_2) \\
\mathsf{red}(\mathsf{C}_1; \mathsf{C}_2) &\triangleq (\mathsf{red}(\mathsf{C}_1); \mathsf{C}_2) \cup \mathsf{red}(\mathsf{C}_2) \\
\mathsf{red}(\mathsf{C}^*) &\triangleq \{\mathsf{C}^*\} \cup (\mathsf{red}(\mathsf{C}); \mathsf{C}^*)
\end{aligned}$$

Where we overload the symbol ; with the operator $; : \mathsf{Imp}^* \times \mathsf{Imp} \to \mathsf{Imp}^*$ defined by

$$\begin{aligned}
\varnothing; \mathsf{C} &\triangleq \varnothing \\
\{\mathsf{C}_1, \ldots, \mathsf{C}_k\}; \mathsf{C} &\triangleq \{\mathsf{C}_1; \mathsf{C}, \ldots, \mathsf{C}_k; \mathsf{C}\}
\end{aligned}$$

Notice that the set of reduction of any finite program $\mathsf{C} \in \mathsf{Imp}$ is finite.

2.4 Functions in Imp

Last section defined the language we are working with (the Imp language), its semantics and its transition system. Building upon those elements, we now present the first properties of the language. More in detail, in the following section we argue that the set of functions is at least a superset of the partially recursive functions described in [Cut80]. This way we can derive some properties from well known computability results, without proving them from scratch. We can do this by encoding partial recursive functions into Imp programs. We therefore start by better describing what we mean by partially recursive functions:

Definition 2.20 (Partially recursive functions)**.** The class $\mathbb{N}^k \overset{r}{\hookrightarrow} \mathbb{N}$ of *partially recursive functions* is the least class of functions on the natural numbers which contains

(a) the zero function:

$$\begin{aligned} z : \mathbb{N}^k &\to \mathbb{N} \\ (x_1, \ldots, x_k) &\mapsto 0 \end{aligned}$$

(b) the successor function

$$\begin{aligned} s : \mathbb{N} &\to \mathbb{N} \\ x_1 &\mapsto x_1 + 1 \end{aligned}$$

(c) the projection function

$$\begin{aligned} U_i^k : \mathbb{N}^k &\to \mathbb{N} \\ (x_1, \ldots, x_k) &\mapsto x_i \end{aligned}$$

and is closed under

(1) composition: given a function $f : \mathbb{N}^k \overset{r}{\hookrightarrow} \mathbb{N}$ and functions $g_1, \ldots, g_k : \mathbb{N}^n \overset{r}{\hookrightarrow} \mathbb{N}$ the *composition* $h : \mathbb{N}^n \overset{r}{\hookrightarrow} \mathbb{N}$ is defined by

$$h(\vec{x}) = \begin{cases} f(g_1(\vec{x}), \ldots, g_k(\vec{x})) & \text{if } g_1(\vec{x}) \downarrow, \ldots, g_k(\vec{x}) \downarrow \text{ and } f(g_1(\vec{x}), \ldots, g_k(\vec{x})) \downarrow \\ \uparrow & \text{otherwise} \end{cases}$$

(2) primitive recursion: given $f : \mathbb{N}^k \overset{r}{\hookrightarrow} \mathbb{N}$ and $g : \mathbb{N}^{k+2} \overset{r}{\hookrightarrow} \mathbb{N}$ we define $h : \mathbb{N}^{k+1} \overset{r}{\hookrightarrow} \mathbb{N}$ by *primitive recursion* by

$$\begin{cases} h(\vec{x}, 0) & = f(\vec{x}) \\ h(\vec{x}, y+1) & = g(\vec{x}, y, h(\vec{x}, y)) \end{cases}$$

(3) minimalization: given $f : \mathbb{N}^{k+1} \overset{r}{\hookrightarrow} \mathbb{N}$, $h : \mathbb{N}^k \overset{r}{\hookrightarrow} \mathbb{N}$ defined trough *unbounded minimalization* is

$$h(\vec{x}) = \mu y.f(\vec{x}, y) = \begin{cases} \text{least } z \text{ s.t.} & \begin{cases} f(\vec{x}, z) = 0 \\ f(\vec{x}, z) \downarrow \quad f(\vec{x}, z') \neq 0 \quad \forall z < z' \end{cases} \\ \uparrow & \text{otherwise} \end{cases}$$

We also need to define what it means providing $(a_1, \ldots, a_k)$ as input for an Imp program. We do this by special input states and variables: we can consider initial states $\rho = [\mathtt{x}_1 \mapsto a_1, \ldots, \mathtt{x}_k \mapsto a_k]$ where each special variable $\mathtt{x}_k$ maps to its initial value a_k, this way we can encode partial functions input into initial states for a program C. Observe that since we are interested in finite programs, it makes sense to consider only finite collections of free variables.

We also need to define what we mean by program output.

Notation 2.21 (Program output)**.** Let $\mathsf{Env} \ni \rho = [\mathtt{x}_1 \mapsto a_1, \ldots, \mathtt{x}_n \mapsto a_n]$. We say

$$\langle \mathsf{C}, \rho \rangle \Downarrow b \iff \forall \rho' \mid \langle \mathsf{C}, \rho \rangle \to^* \rho' \quad \rho'(\mathtt{y}) = b$$
$$\langle \mathsf{C}, \rho \rangle \downarrow b \iff \exists \rho' \mid \langle \mathsf{C}, \rho \rangle \to^* \rho' \quad \rho'(\mathtt{y}) = b$$

C universally (partially) halts on b whenever for every (for some) final state ρ $\rho(\mathtt{y}) = b$. In other words we are using the special variable $\mathtt{y}$ as an output register.

Definition 2.22 (Imp computability)**.** Let $f : \mathbb{N}^k \to \mathbb{N}$ be a function. We say that f is Imp computable if

$$\exists \mathsf{C} \in \mathsf{Imp} \mid \forall (a_1, \ldots, a_k) \in \mathbb{N}^k \wedge b \in \mathbb{N}$$
$$\mathsf{TS}(\langle \mathsf{C}, \rho \rangle) \Downarrow b \iff (a_1, \ldots, a_k) \in dom(f) \wedge f(a_1, \ldots, a_k) = b$$

with $\rho = [\mathtt{x}_1 \mapsto a_1, \ldots, \mathtt{x}_k \mapsto a_k]$.

We argue that the class of function computed by Imp is the same as the set of partially recursive functions $\mathbb{N} \overset{r}{\hookrightarrow} \mathbb{N}$ (as defined in [Cut80]). To do that we have to prove that the class of functions computed by the Imp language is a *rich* , i.e.

Definition 2.23 (Rich class)**.** A class of functions $\mathcal{A}$ is said to be rich if it includes (a),(b) and (c) and it is closed under (1), (2) and (3) from Definition 2.20.

Lemma 2.24 (Imp functions richness)**.** *The class of Imp-computable function is rich.*

Proof. We proceed by proving that Imp has each and every one of the basic functions (zero, successor, projection).

- The zero function:

$$z : \mathbb{N}^k \to \mathbb{N}$$
$$(x_1, \ldots, x_k) \mapsto 0$$

  is Imp-computable:

$$z(a_1, \ldots, a_k) \triangleq y := 0$$

- The successor function

$$s : \mathbb{N} \to \mathbb{N}$$
$$x_1 \mapsto x_1 + 1$$

  is Imp-computable:

$$s(a_1) \triangleq y := x_1 + 1$$

- The projection function

$$U_i^k : \mathbb{N}^k \to \mathbb{N}$$
$$(x_1, \ldots, x_k) \mapsto x_i$$

  is Imp-computable:

$$U_i^k(a_1, \ldots, a_k) \triangleq y := x_i + 0$$

We then prove that it is closed under composition, primitive recursion and unbounded minimalization.

Lemma 2.25. *let $f : \mathbb{N}^k \to \mathbb{N}$, $g_1, \ldots, g_k : \mathbb{N}^n \to \mathbb{N}$ and consider the composition*

$$h : \mathbb{N}^k \to \mathbb{N}$$
$$\vec{x} \mapsto f(g_1(\vec{x}), \ldots, g_k(\vec{x}))$$

h is Imp-computable.

Proof. Since by hp $f, g_n \forall n \in [1,k]$ are computable, we consider their programs $F, G_n \forall n \in [1,k]$. Now consider the program

$$\begin{aligned}
&G_1(\vec{x});\\
&y_1 := y + 0;\\
&G_2(\vec{x});\\
&y_2 := y + 0;\\
&\ldots;\\
&G_k(\vec{x});\\
&y_k := y + 0;\\
&F(y_1, y_2, \ldots, y_k);
\end{aligned}$$

Which is exactly h. Therefore Imp is closed under generalized composition. □

Lemma 2.26. *Given $f : \mathbb{N}^k \to \mathbb{N}$ and $g : \mathbb{N}^{k+2} \to \mathbb{N}$ Imp computable, we argue that $h : \mathbb{N}^{k+1} \to \mathbb{N}$*

$$\begin{cases} h(\vec{x}, 0) = f(\vec{x}) \\ h(\vec{x}, y+1) = g(\vec{x}, y, h(\vec{x}, y)) \end{cases}$$

defined trough primitive recursion is Imp-computable.

Proof. We want a program to compute $h : \mathbb{N}^{k+1} \to \mathbb{N}$. By hypothesis we have programs F, G to compute respectively $f : \mathbb{N}^k \to \mathbb{N}$ and $g : \mathbb{N}^{k+2} \to \mathbb{N}$. Consider the program $H(\vec{x}, x_{k+1})$:

$$\begin{aligned}
&s := 0;\\
&F(\vec{x});\\
&(x_{k+1} \notin [0,0]; G(\vec{x}, s, y); s := s + 1; x_{k+1} := x_{k+1} - 1)^*;\\
&x_{k+1} \in [0,0];
\end{aligned}$$

which computes exactly h. Therefore Imp is closed under primitive recursion. □

Lemma 2.27. *Let $f : \mathbb{N}^{k+1} \to \mathbb{N}$ be a Imp-computable function. Then the function $h : \mathbb{N}^k \to \mathbb{N}$ defined trough unbounded minimalization*

$$h(\vec{x}) = \mu y. f(\vec{x}, y) = \begin{cases} \textit{least } z \textit{ s.t.} & \begin{cases} f(\vec{x}, z) = 0 \\ f(\vec{x}, z) \downarrow \quad f(\vec{x}, z') \neq 0 \quad \forall z < z' \end{cases} \\ \uparrow & \textit{otherwise} \end{cases} \tag{2.2}$$

is Imp-computable.

Proof. Let F be the program for the computable function f with arity $k+1$, $\vec{x} = (x_1, x_2, \ldots, x_k)$. Consider the program $H(\vec{x})$

$$\begin{aligned}
&z := 0;\\
&F(\vec{x}, z);\\
&(y \notin [0,0]; z := z + 1; F(\vec{x}, z))^*;\\
&y \in [0,0];\\
&y := z + 0;
\end{aligned}$$

Which outputs the least z s.t. $F(\vec{x}, z) \downarrow 0$, and loops forever otherwise. Imp is therefore closed under bounded minimalization. □

Since has the zero function, the successor function, the projections function and is closed under composition, primitive recursion and unbounded minimalization, the class of Imp-computable functions is rich. □

Since it is rich and $\mathbb{N} \overset{r}{\hookrightarrow} \mathbb{N}$ is the least class of rich functions, $\mathbb{N} \overset{r}{\hookrightarrow} \mathbb{N} \subseteq \mathsf{Imp}_f$ holds. Therefore we can say

$$f \in \mathbb{N}^k \overset{r}{\hookrightarrow} \mathbb{N} \implies \exists \mathsf{C} \in \mathsf{Imp} \mid \langle \mathsf{C}, \rho \rangle \Downarrow b \iff f(a_1, \ldots, a_k) \downarrow b$$

with $\rho = [\mathtt{x}_1 \mapsto a_1, \ldots, \mathtt{x}_k \mapsto a_k]$.

The final step is to recall the Rice theorem from [Ric53] and the definition of saturated sets:

Definition 2.28 (Saturated set)**.** $A \subseteq \mathbb{N}$ is *saturated* (or *extensional*) is for all $x, y \in \mathbb{N}$

$$x \in A \wedge \varphi_x = \varphi_y \implies y \in A$$

In other words a set is saturated if it contains all the numbers that encode for programs that compute functions with some properties. Rice's theorem links extensional sets and decidability:

Theorem 2.29 (Rice's theorem)**.** *Let $A \subseteq \mathbb{N}$, $A \neq \varnothing, A \neq \mathbb{N}$ be a saturated set. Then A is not recursive.*

Meaning that deciding weather a program is in some saturated set, i.e., the program has some extensional property, is impossible. From this we get a couple of facts that derive from well known computability results:

Corollary 2.30. *$\langle \mathsf{C}, \rho \rangle \Uparrow$ (i.e., $\langle \mathsf{C} \rangle \rho = \varnothing$) is undecidable.*

Proof. The set of functions $f \in \mathbb{N}^k \overset{r}{\hookrightarrow} \mathbb{N}$ s.t. $f(x) \uparrow \forall x \in \mathbb{N}^k$ is not trivial and saturated, therefore it is not recursive by Rice's theorem [Ric53]. □

Corollary 2.31. *$\langle \mathsf{C}, \rho \rangle \Downarrow$ is undecidable.*

Proof. The set of functions $f \in \mathbb{N}^k \overset{r}{\hookrightarrow} \mathbb{N}$ s.t. $f(x) \downarrow \forall x \in \mathbb{N}^k$ is not trivial and saturated, therefore it is not recursive by Rice's theorem [Ric53]. □

2.5 Deciding invariant finiteness

In this section we argue that even the finiteness of the semantics of some program on some initial states is undecidable. We show that if we were able to establish whether $\langle \mathsf{C} \rangle X$ is finite for some program $\mathsf{C} \in \mathsf{Imp}$ and some initial states $X \in \mathcal{C}$, we could decide whether $\langle \mathsf{C}, \rho \rangle \Downarrow$ for all $\rho \in X$, which instead is known to be undecidable. The first step is showing that if we have a program where the * operator does not appear, then the program can only produce a finite amount of finite derivation sequences.

Lemma 2.32. *If $\mathsf{D} \in \mathsf{Imp}_s$, and $X \in \wp(env)$ is finite, then*

(i). $\langle \mathsf{D} \rangle X$ *is finite;*

(ii). $\forall \rho \in X \ \langle \mathsf{D}, \rho \rangle \Downarrow$

(iii). $|\mathsf{TS}(\langle \mathsf{D}, \rho \rangle)| < \infty$ *for all* $\rho \in X$*.*

where by $\mathsf{TS}(\langle \mathsf{D}, \rho \rangle)$ we mean the set of all derivation sequences starting from $\langle \mathsf{D}, \rho \rangle$ in the transition system.

Proof. By induction on the program D:

Base case:
$\mathsf{D} \equiv e$, therefore

(i). $\langle \mathsf{e} \rangle X = \{ (\!| e |\!) \rho \mid \rho \in X, (\!| e |\!) \rho \neq \bot \}$, which is finite, since X is finite;

(ii). by expr rule $\forall \rho \in X$ either $\langle e, \rho \rangle \to (\!| e |\!) \rho$ or $\langle e, \rho \rangle \not\to$. In both cases there are no infinite derivation sequences, and therefore $\mathsf{TS}(\langle \mathsf{e}, \rho \rangle) \Downarrow$;

(iii). Notice that $\forall \rho \in X$ either by the expr rule $\langle \mathsf{e}, \rho \rangle \to (\!| \mathsf{e} |\!) \rho$ or $\langle \mathsf{e}, \rho \rangle \not\to$ therefore

$$|\mathsf{TS}(\langle \mathsf{e}, \rho \rangle)| \leqslant |X| < \infty$$

Inductive cases:

1. $\mathsf{D} \equiv \mathsf{D}_1 + \mathsf{D}_2$, therefore
   (i). $\langle \mathsf{D}_1 + \mathsf{D}_2 \rangle X = \langle \mathsf{D}_1 \rangle X \cup \langle \mathsf{D}_2 \rangle X$. By inductive hypothesis, both $\langle \mathsf{D}_1 \rangle X, \langle \mathsf{D}_2 \rangle X$ are finite, as they are sub expressions of D. Since the union of finite sets is finite, $\langle \mathsf{D}_1 + \mathsf{D}_2 \rangle X$ is finite;
   (ii). by inductive hypothesis again $\forall \rho \in X \ \langle \mathsf{D}_1, \rho \rangle \downdownarrows$ and $\langle \mathsf{D}_2, \rho \rangle \downdownarrows$. By sum_1 rule $\langle \mathsf{D}_1 + \mathsf{D}_2, \rho \rangle \to \langle \mathsf{D}_1, \rho \rangle$ and by sum_2 $\langle \mathsf{D}_1 + \mathsf{D}_2, \rho \rangle \to \langle \mathsf{D}_2, \rho \rangle$. Therefore $\langle \mathsf{D}_1 + \mathsf{D}_2 \rangle \rho \downdownarrows$.
   (iii). For the latter argument, since both $\langle \mathsf{D}_1 \rangle \rho$ and $\langle \mathsf{D}_2 \rangle \rho$ are finite and composed of finite derivation sequences $|\mathsf{TS}(\langle \mathsf{D}_1 + \mathsf{D}_2, \rho \rangle)| < \infty$.
2. $\mathsf{D} \equiv \mathsf{D}_1; \mathsf{D}_2$, therefore
   (i). $\langle \mathsf{D}_1; \mathsf{D}_2 \rangle X = \langle \mathsf{D}_2 \rangle (\langle \mathsf{D}_1 \rangle X)$. By inductive hypothesis $\langle \mathsf{D}_1 \rangle X = Y$. By inductive hypothesis again $\langle \mathsf{D}_2 \rangle Y$ is finite;
   (ii). by inductive hypothesis both $\forall \rho \in X \ \langle \mathsf{D}_1, \rho \rangle \downdownarrows$ and $\forall \rho' \in Y \ \langle \mathsf{D}_2, \rho' \rangle \downdownarrows$, therefore by composition lemma $\langle \mathsf{D}_1; \mathsf{D}_2, \rho \rangle \downdownarrows$
   (iii). by inductive hypothesis both $|\mathsf{TS}(\langle \mathsf{D}_1, \rho \rangle)| < \infty$ and $|\mathsf{TS}(\langle \mathsf{D}_2, \rho' \rangle)| < \infty \ \forall \rho \in X, \rho' \in \langle \mathsf{D}_1 \rangle X$. For all derivation sequences starting from $\langle \mathsf{D}_1, \rho \rangle$ where

$$\langle \mathsf{D}_1, \rho \rangle \to^* \rho'$$

   with $\rho' \in \langle \mathsf{D}_1 \rangle X$ we can apply the composition lemma and state that

$$\langle \mathsf{D}_1; \mathsf{D}_2, \rho \rangle \to^* \langle \mathsf{D}_2, \rho' \rangle \quad \forall \rho \in X$$

   from there we can notice that since $|\langle \mathsf{D}_2, \rho' \rangle| < \infty$ then $|\langle \mathsf{D}_1; \mathsf{D}_2, \rho' \rangle| < \infty$

□

In order to prove that finiteness is undecidable we need the following Lemma:

Lemma 2.33. *Let* $\mathsf{D} \in \mathsf{Imp}_s$ *and* $\rho \in \mathsf{Env}$. *If*

$$\langle \mathsf{D} \rangle^{k+1} \rho \subseteq \bigcup_{i=0}^{k} \langle \mathsf{D} \rangle^i \rho \quad \textit{for some } k \in \mathbb{N} \tag{2.3}$$

then

$$\forall j \in \mathbb{N} \quad \langle \mathsf{D} \rangle^{k+1+j} \rho \subseteq \bigcup_{i=0}^{k} \langle \mathsf{D} \rangle^i \rho \tag{2.4}$$

and therefore $\langle \mathsf{D}^* \rangle \rho \subseteq \cup_{i=0}^{k} \langle \mathsf{D} \rangle^i \rho$

Proof. We can show (2.4) by induction on j:

- if $j = 0$ then we want to show that $\langle \mathsf{D} \rangle^{k+1} \rho \subseteq \cup_{i=0}^{k} \langle \mathsf{D} \rangle^i \rho$, which is true by hypothesis (2.3);
- In the inductive case we have to show that if the statement holds for j, it also holds for $j+1$. We know that

$$\begin{aligned}
\bigcup_{i=0}^{k} \langle \mathsf{D} \rangle^i \rho &= \bigcup_{i=0}^{k+1} \langle \mathsf{D} \rangle^i \rho && \text{since by (2.3) } \langle \mathsf{D} \rangle^{k+1} \rho \subseteq \cup_{i=0}^{k} \langle \mathsf{D} \rangle^i \rho \\
&= \rho \cup \bigcup_{i=1}^{k+1} \langle \mathsf{D} \rangle^i \rho \\
&= \rho \cup \langle \mathsf{D} \rangle \left(\bigcup_{i=0}^{k} \langle \mathsf{D} \rangle^i \rho \right) && \text{by additivity of } \langle \mathsf{D} \rangle
\end{aligned}$$

By inductive hypothesis

$$\langle \mathsf{D} \rangle^{k+1+j} \rho \subseteq \bigcup_{i=0}^{k} \langle \mathsf{D} \rangle^{i} \rho$$

so, by monotonicity of $\langle \mathsf{D} \rangle$

$$\langle \mathsf{D} \rangle \left(\langle \mathsf{D} \rangle^{k+1+j} \rho \right) \subseteq \langle \mathsf{D} \rangle \left(\bigcup_{i=0}^{k} \langle \mathsf{D} \rangle^{i} \rho \right)$$

and therefore

$$\langle \mathsf{D} \rangle^{(k+1)+(j+1)} \rho \subseteq \left(\bigcup_{i=1}^{k+1} \langle \mathsf{D} \rangle^{i} \rho \right) \subseteq \rho \cup \left(\bigcup_{i=1}^{k+1} \langle \mathsf{D} \rangle^{i} \rho \right) = \bigcup_{i=0}^{k+1} \langle \mathsf{D} \rangle^{i} \rho = \bigcup_{i=0}^{k} \langle \mathsf{D} \rangle^{i} \rho$$

□

We also need to recall König's Lemma from [Kön26]:

Lemma 2.34 (König's Lemma)**.** *Let T be a rooted tree with an infinite number of nodes, each with a finite number of children. Then T has a branch of infinite length.*

With Lemma 2.33 and Lemma 2.34 we can prove the following.

Lemma 2.35. *Given $\mathsf{D} \in \mathsf{Imp}_s$, and $\rho \in \mathsf{Env}$, the predicate "$\langle \mathsf{D}^* \rangle \rho$ is finite" is undecidable.*

Proof. We work by contradiction, showing that if we know whether $\langle \mathsf{C} \rangle \rho$ is finite or infinite we can decide $\langle \mathsf{C}, \rho \rangle \downdownarrows$.

- Suppose that $\langle \mathsf{D}^* \rangle \rho$ is infinite, then we can observe that because Lemma 2.33

$$\forall k \in \mathbb{N} \quad \langle \mathsf{D} \rangle^{k+1} \rho \not\subseteq \bigcup_{i=0}^{k} \langle \mathsf{D} \rangle^{i} \rho \tag{2.5}$$

Otherwise $\langle \mathsf{D}^* \rangle \rho \subseteq \bigcup_{i \in \mathbb{N}} \langle \mathsf{D} \rangle^{i} \rho$ and we would contradict the hypothesis of $\langle \mathsf{D}^* \rangle \rho$ being infinite. Therefore $\forall k \in \mathbb{N}\ \langle \mathsf{D} \rangle^{k+1} \rho \not\subseteq \bigcup_{i=0}^{k} \langle \mathsf{D} \rangle^{i} \rho$, otherwise $\langle \mathsf{D}^* \rangle \rho \subseteq \bigcup_{i=0}^{k} \langle \mathsf{D} \rangle \rho$ which is impossible since the right term is a finite quantity. With this observation we build the tree $\langle \mathsf{Env}, \rightarrow^{D} \rangle$, where $\rightarrow^{D} \subseteq \mathsf{Env} \times \mathsf{Env}$ and $\rho' \rightarrow^{D} \rho''$ if $\langle \mathsf{D}, \rho' \rangle \rightarrow^{*} \rho''$. We define by the following rule the levels of the tree:

$$\begin{aligned} Y_0 &= \{\rho\} \\ Y_{k+1} &= \left(\langle \mathsf{D} \rangle^{k+1} \rho \right) \setminus \left(\bigcup_{i=0}^{k} \langle \mathsf{D} \rangle \rho \right) \end{aligned}$$

Where Y_0 is the singleton set containing the root ρ and the k-th level is made of the environments in the Y_k set. Figure 2.2 shows a tree of $\rightarrow^{D}$ relations and visualizes the levels Y_k. We can therefore make the following observations:

(i) The tree is rooted in $\rho \in Y_0$. In fact $\forall \rho' \in Y_1\ \rho \rightarrow^{D} \rho'$ by definition and $\forall \rho''' \in Y_{k+1} \exists \rho'' \in Y_k \mid \rho'' \rightarrow^{D} \rho'''$;

(ii) since $\forall k \in \mathbb{N}\ \langle \mathsf{D} \rangle^{k+1} \rho \not\subseteq \cup_{i=0}^{k} \langle \mathsf{D} \rangle^{i} \rho$ by (2.5), each level Y_k is non empty. Each level is also finite because of Lemma 2.32.(i). Therefore there is an infinite quantity of levels, where each node has a finite quantity of children.

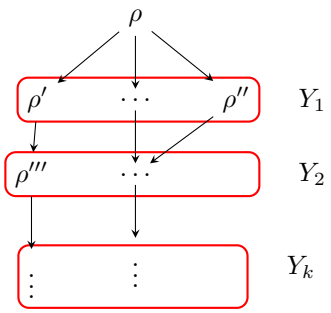


Figure 2.2: Example of $\to^D$ relations between elements of Env.

what is left to do is show that there is a derivation sequence from $\langle \mathsf{D}^*, \rho \rangle$ of infinite length. We can do this by using König's Lemma 2.34 and deduce that there exists an infinite derivation sequence from ρ of $\to^D$ relations

$$\rho \to^D \rho' \to^D \rho'' \to^D \dots$$

Where each element belongs to a different level Y_k, and therefore is different from every other environment appearing in the sequence. Observe that for all $\rho', \rho'' \in \mathsf{Env}$ s.t. $\rho' \to^D \rho''$ since $\langle \mathsf{D}, \rho' \rangle \to^* \rho''$ we can apply Corollary 2.18 of Lemma 2.17 and derive that $\langle \mathsf{D}; \mathsf{D}^*, \rho' \rangle \to^* \langle \mathsf{D}^*, \rho'' \rangle$ and because of the star rule $\langle \mathsf{D}^*, \rho' \rangle \to \langle \mathsf{D}; \mathsf{D}^*, \rho' \rangle$. We can therefore say that

$$\langle \mathsf{D}^*, \rho' \rangle \to^* \langle \mathsf{D}^*, \rho'' \rangle$$

Therefore, there exists an infinite derivation sequence

$$\langle \mathsf{D}^*, \rho \rangle \to^* \langle \mathsf{D}^*, \rho' \rangle \to^* \langle \mathsf{D}^*, \rho'' \rangle \to^* \dots$$

which means $\langle \mathsf{D}^*, \rho \rangle \uparrow$ and therefore $\langle \mathsf{D}^*, \rho \rangle \Downarrow$ is false.

- if instead $\langle \mathsf{D}^* \rangle \rho$ is finite, then we can reduce total termination to the presence of some cycle in one of the derivation sequences starting from $\langle \mathsf{D}^*, \rho \rangle$. The statement we want to prove is the following:

  if $\langle \mathsf{D}^* \rangle \rho$ is finite, then $\langle \mathsf{D}^*, \rho \rangle \Downarrow \iff$ no derivation sequence starting from $\langle \mathsf{D}^*, \rho \rangle$ has cycles

($\implies$) In this case we want to prove that if $\langle \mathsf{D}^* \rangle$ is finite and $\langle \mathsf{D}, \rho \rangle \Downarrow$ then there are no cycles in any derivation sequence starting from $\langle \mathsf{D}, \rho \rangle$. To do so we work by contradiction. Suppose there is some derivation sequence starting from $\langle \mathsf{D}^*, \rho \rangle$ with some cycle

$$\langle \mathsf{D}^*, \rho \rangle \to^* \langle \mathsf{D}^*, \rho' \rangle \to^+ \langle \mathsf{D}^*, \rho' \rangle \to^* \rho''$$

with $\rho'' \neq \rho, \rho'$, then we can notice that also the infinite derivation sequence

$$\langle \mathsf{D}^*, \rho \rangle \to^* \langle \mathsf{D}^*, \rho' \rangle \to^+ \langle \mathsf{D}^*, \rho' \rangle \to^+ \langle \mathsf{D}^*, \rho' \rangle \to^+ \dots$$

is part of the transition system for $\langle \mathsf{D}, \rho \rangle$, and therefore $\langle \mathsf{D}^*, \rho \rangle \Downarrow$ is false which is absurd.

($\impliedby$) In this case we want to prove that if $\langle \mathsf{D}^* \rangle \rho$ is finite and there are no cycles in any derivation sequence starting from $\langle \mathsf{D}, \rho \rangle$ then $\langle \mathsf{D}, \rho \rangle \Downarrow$. We work again by contradiction. Suppose that we have an infinite derivation sequence starting from $\langle \mathsf{D}^*, \rho \rangle$. It must be that $\forall i, j \in \mathbb{N}\ i \neq j,\ \rho_i \neq \rho_j$ with $\rho_0 = \rho$, otherwise there would be a cycle, which would contradict the hypothesis. Therefore the derivation sequence has the shape

$$\langle \mathsf{D}^*, \rho \rangle \to^* \langle \mathsf{D}^*, \rho_1 \rangle \to^* \langle \mathsf{D}^*, \rho_2 \rangle \to^* \langle \mathsf{D}^*, \rho_3 \rangle \to^* \dots$$

We can notice that for all $\rho' \in \{\rho, \rho_1, \dots\}$ and for the star_{fix} rule, $\langle \mathsf{D}^*, \rho' \rangle \to \rho'$ and therefore $\rho' \in \langle \mathsf{D}^* \rangle \rho$. This would mean that $\langle \mathsf{D}^* \rangle \rho$ is infinite, which is absurd.

To conclude we can observe that there is a finite amount of reachable states from $\langle \mathsf{D}^*, \rho \rangle$. Where by reachable we mean that there exists some derivation sequence ending up in that state.

We can notice that starting from any state $\langle \mathsf{D}^*, \rho' \rangle$ with $\rho' \in \langle \mathsf{D}^* \rangle \rho$ we have 2 possibilities:

- we either apply the star_{fix}rule, resulting in a finite derivation sequence

$$\langle \mathsf{D}^*, \rho' \rangle \to \rho'$$

  and therefore in a finite number of reached states;

- or we apply the star rule

$$\langle \mathsf{D}^*, \rho' \rangle \to \langle \mathsf{D}; \mathsf{D}^*, \rho' \rangle$$

  by lemma 2.32 we know that $\langle \mathsf{D}, \rho' \rangle \downdownarrows$ and $|\mathsf{TS}(\langle \mathsf{D}, \rho' \rangle)| < \infty$, therefore there is a finite number of environments ρ'' s.t. $\langle \mathsf{D}, \rho' \rangle \to^* \rho''$. For each one of them we can use the composition lemma and observe that

$$\langle \mathsf{D}; \mathsf{D}^*, \rho' \rangle \to^* \langle \mathsf{D}^*, \rho'' \rangle$$

  Ending up in a state $\langle \mathsf{D}^*, \rho'' \rangle$ where we can apply the same reasoning

Therefore starting from any state $\langle \mathsf{D}^*, \rho' \rangle$ with $\rho' \in \langle \mathsf{D}^* \rangle \rho$ (in particular ρ), we either terminate our derivation sequence or we end up in some state $\langle \mathsf{D}^*, \rho' \rangle$ again, with $\rho' \in \langle \mathsf{D}^* \rangle \rho$. Since there is a finite amount of states $\rho' \in \langle \mathsf{D}^* \rangle \rho$, the number of reachable states from $\langle \mathsf{D}^*, \rho \rangle$ is finite.

□

Chapter 3

Abstract domains

In the following chapters we present two domains that will play a relevant role in the sequel: the *interval* domain and the *non-relational* collecting domain. The two domains are in the class of *non-relational* domains, meaning that they do not represent the relation between variables. We are interested in these two domains as the properties that we will discuss in Chapter 4 will apply to these domains, with some restrictions that we will discuss later. In Section 3.2 we will talk about the interval domain, with its characterization in Section **??** and the domain properties in Section 3.2.2. Later, in Section 3.3 we will talk about the non-relational collecting abstraction by also showing some properties of the abstraction in Section 3.3.2.

3.1 Abstract inductive semantics

In order to talk about analysis over some abstract domain $\mathbb{A}$, we preliminarly introduce the definition of abstract semantics provided an abstract domain.

Definition 3.1 (**Abstract inductive semantic**)**.** Given a domain $\mathbb{A}$ and an abstract semantics $(\!(\cdot)\!)^{\mathbb{A}} : \mathsf{Exp} \to \mathbb{A} \to \mathbb{A}$ for basic expressions, the *abstract inductive semantics* over $\mathbb{A}$ is defined as the strict (i.e., preserving $\bot$) extension of the following function $[\![\cdot]\!]^{\mathbb{A}} : \mathsf{Imp} \to \mathbb{A} \to \mathbb{A}$. For all $\eta \in \mathbb{A}$

$$
\begin{aligned}
[\![\mathsf{e}]\!]^{\mathbb{A}}\eta &\triangleq (\!(\mathsf{e})\!)^{\mathbb{A}}\eta \\
[\![\mathsf{C}_1 + \mathsf{C}_2]\!]^{\mathbb{A}}\eta &\triangleq [\![\mathsf{C}_1]\!]^{\mathbb{A}}\eta \sqcup [\![\mathsf{C}_2]\!]^{\mathbb{A}}\eta \\
[\![\mathsf{C}_1; \mathsf{C}_2]\!]^{\mathbb{A}}\eta &\triangleq [\![\mathsf{C}_2]\!]^{\mathbb{A}}\left([\![\mathsf{C}_1]\!]^{\mathbb{A}}\eta\right) \\
[\![\mathsf{C}^*]\!]^{\mathbb{A}}\eta &\triangleq \bigsqcup_{i\in\mathbb{N}} \left([\![\mathsf{C}]\!]^{\mathbb{A}}\right)^i(\eta) \\
[\![\mathsf{fix}(\mathsf{C})]\!]^{\mathbb{A}}\eta &\triangleq \mathrm{lfp}(\lambda\mu.(\eta \sqcup [\![\mathsf{C}]\!]^{\mathbb{A}}\mu))
\end{aligned}
$$

From this definition we can observe that soundness is preserved from the base cases, i.e., if we have two domains $\mathbb{A}$ and $\mathbb{A}^\sharp$ s.t. $\mathbb{A} \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} \mathbb{A}^\sharp$ according to some abstraction and concretization maps α and γ then the analysis over $\mathbb{A}^\sharp$ is *sound* w.r.t. the analysis performed over $\mathbb{A}$, provided that the base cases are sound.

Theorem 3.2 (Abstraction soundness)**.** *Let $C \in \mathsf{Imp}$ and $\langle \mathbb{A}, \sqsubseteq\rangle, \langle \mathbb{A}^\sharp, \sqsubseteq^\sharp\rangle$ be two domains equipped with their partial order s.t. $\mathbb{A} \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} \mathbb{A}^\sharp$ for some abstraction and concretization maps α, γ such that*

$$\forall \mathsf{e} \in \mathsf{Exp} \quad ((\!(\mathsf{e})\!)^{\mathbb{A}} \circ \gamma)\eta^\sharp \sqsubseteq (\gamma \circ (\!(\mathsf{e})\!)^{\mathbb{A}^\sharp})\eta^\sharp$$

i.e., the analysis over the base cases are sound. Then for all $\eta^\sharp \in \mathbb{A}^\sharp$:

$$([\![\mathsf{C}]\!]^{\mathbb{A}} \circ \gamma)\ \eta^\sharp \sqsubseteq (\gamma \circ [\![\mathsf{C}]\!]^{\mathbb{A}^\sharp})\ \eta^\sharp$$

i.e., the abstract analysis over $\mathbb{A}^\sharp$ is sound w.r.t. the analysis over $\mathbb{A}$.

Proof. The proof will proceed again by induction on C.

Case (e). In this case by hypothesis it holds that

$$([\![\mathsf{e}]\!]^{\mathbb{A}} \circ \gamma)\eta^\sharp = (((\mathsf{e}))^{\mathbb{A}} \circ \gamma)\eta^\sharp \sqsubseteq (\gamma \circ ((\mathsf{e}))^{\mathbb{A}^\sharp})\eta^\sharp = (\gamma \circ [\![\mathsf{e}]\!]^{\mathbb{A}^\sharp})\eta^\sharp$$

Which is exactly our thesis.

Case $(\mathsf{C}_1 + \mathsf{C}_2)$. In this case by inductive hypothesis we know that both the following hold:

$$\left([\![\mathsf{C}_1]\!]^{\mathbb{A}} \circ \gamma\right) \eta^\sharp \sqsubseteq \left(\gamma \circ [\![\mathsf{C}_1]\!]^{\mathbb{A}^\sharp}\right) \eta^\sharp \tag{3.1}$$

$$\left([\![\mathsf{C}_2]\!]^{\mathbb{A}} \circ \gamma\right) \eta^\sharp \sqsubseteq \left(\gamma \circ [\![\mathsf{C}_2]\!]^{\mathbb{A}^\sharp}\right) \eta^\sharp \tag{3.2}$$

and $[\![\mathsf{C}_1 + \mathsf{C}_2]\!]^{\mathbb{A}^\sharp}\eta^\sharp = [\![\mathsf{C}_1]\!]^{\mathbb{A}^\sharp}\eta^\sharp \sqcup [\![\mathsf{C}_2]\!]^{\mathbb{A}^\sharp}\eta^\sharp$. What we have to prove is that

$$\left([\![\mathsf{C}_1 + \mathsf{C}_2]\!]^{\mathbb{A}} \circ \gamma\right) \eta^\sharp \sqsubseteq \left(\gamma \circ [\![\mathsf{C}_1 + \mathsf{C}_2]\!]^{\mathbb{A}^\sharp}\right) \eta^\sharp$$

or, equivalently

$$[\![\mathsf{C}_1 + \mathsf{C}_2]\!]^{\mathbb{A}} \left(\gamma\eta^\sharp\right) \sqsubseteq \gamma \left([\![\mathsf{C}_1 + \mathsf{C}_2]\!]^{\mathbb{A}^\sharp}\eta^\sharp\right)$$

$$[\![\mathsf{C}_1]\!]^{\mathbb{A}} \left(\gamma\eta^\sharp\right) \sqcup [\![\mathsf{C}_2]\!]^{\mathbb{A}} \left(\gamma\eta^\sharp\right) \sqsubseteq \gamma \left([\![\mathsf{C}_1]\!]^{\mathbb{A}^\sharp}\eta^\sharp \sqcup [\![\mathsf{C}_2]\!]^{\mathbb{A}^\sharp}\eta^\sharp\right)$$

Now we can notice that by Property 4 of Galois connections

$$\gamma \left([\![\mathsf{C}_1]\!]^{\mathbb{A}^\sharp}\eta^\sharp \sqcup [\![\mathsf{C}_2]\!]^{\mathbb{A}^\sharp}\eta^\sharp\right) = \bigsqcup \left\{\rho \in \mathbb{A} \mid \alpha(\rho) \sqsubseteq [\![\mathsf{C}_1]\!]^{\mathbb{A}^\sharp}\eta^\sharp \sqcup [\![\mathsf{C}_2]\!]^{\mathbb{A}^\sharp}\eta^\sharp\right\} \tag{3.3}$$

Now

$$\begin{aligned}
\left(\alpha \circ [\![\mathsf{C}_1]\!]^{\mathbb{A}} \circ \gamma\right) \eta^\sharp &\sqsubseteq \left(\alpha \circ \gamma \circ [\![\mathsf{C}_1]\!]^{\mathbb{A}^\sharp}\right) \eta^\sharp && \text{by monotonicity of } \alpha \text{ in (3.1)} \\
&\sqsubseteq \left([\![\mathsf{C}_1]\!]^{\mathbb{A}^\sharp}\right) \eta^\sharp && \text{by reductivity of } \alpha
\end{aligned}$$

and the same applies for (3.2). Hence because of (3.3) we can observe that

$$\begin{aligned}
[\![\mathsf{C}_1]\!]^{\mathbb{A}} \left(\gamma\eta^\sharp\right) \sqcup [\![\mathsf{C}_2]\!]^{\mathbb{A}} \left(\gamma\eta^\sharp\right) &\sqsubseteq \bigsqcup \left\{\rho \in \mathbb{A} \mid \alpha(\rho) \sqsubseteq [\![\mathsf{C}_1]\!]^{\mathbb{A}^\sharp}\eta^\sharp \sqcup [\![\mathsf{C}_2]\!]^{\mathbb{A}^\sharp}\eta^\sharp\right\} \\
&= \gamma \left([\![\mathsf{C}_1]\!]^{\mathbb{A}^\sharp}\eta^\sharp \sqcup [\![\mathsf{C}_2]\!]^{\mathbb{A}^\sharp}\eta^\sharp\right)
\end{aligned}$$

which is our thesis.

Case $(\mathsf{C}_1; \mathsf{C}_2)$. In this case we have to prove that

$$\left([\![\mathsf{C}_1; \mathsf{C}_2]\!]^{\mathbb{A}} \circ \gamma\right) \eta^\sharp \sqsubseteq \left(\gamma \circ [\![\mathsf{C}_1; \mathsf{C}_2]\!]^{\mathbb{A}^\sharp}\right) \eta^\sharp$$

or equivalently

$$\left([\![\mathsf{C}_2]\!]^{\mathbb{A}} \circ [\![\mathsf{C}_1]\!]^{\mathbb{A}} \circ \gamma\right) \eta^\sharp \sqsubseteq \left(\gamma \circ [\![\mathsf{C}_2]\!]^{\mathbb{A}^\sharp} \circ [\![\mathsf{C}_1]\!]^{\mathbb{A}^\sharp}\right) \eta^\sharp$$

Now we can notice that by inductive hypothesis $[\![\mathsf{C}_1]\!]^{\mathbb{A}^\sharp}$ and $[\![\mathsf{C}_2]\!]^{\mathbb{A}^\sharp}$ are sound abstractions of respectively $[\![\mathsf{C}_1]\!]^{\mathbb{A}}$ and $[\![\mathsf{C}_2]\!]^{\mathbb{A}}$, hence we have the hypothesis to apply Theorem 1.25 and deduce that

$$\left([\![\mathsf{C}_2]\!]^{\mathbb{A}} \circ [\![\mathsf{C}_1]\!]^{\mathbb{A}} \circ \gamma\right) \sqsubseteq \left(\gamma \circ [\![\mathsf{C}_2]\!]^{\mathbb{A}^\sharp} \circ [\![\mathsf{C}_1]\!]^{\mathbb{A}^\sharp}\right)$$

which is our thesis.

Case ($\mathsf{fix}(\mathsf{C})$). In this case we have to prove that

$$\left(\llbracket \mathsf{fix}(\mathsf{C}) \rrbracket^{\mathbb{A}} \circ \gamma\right) \eta^\sharp \sqsubseteq \left(\gamma \circ \llbracket \mathsf{fix}(\mathsf{C}) \rrbracket^{\mathbb{A}^\sharp}\right) \eta^\sharp$$

we know by definition and Fixpoint Theorem 1.13 that

$$\left(\gamma \circ \llbracket \mathsf{fix}(\mathsf{C}) \rrbracket^{\mathbb{A}^\sharp}\right) \eta^\sharp = \gamma(\mathrm{lfp}(\lambda\mu.\eta^\sharp \sqcup \llbracket \mathsf{C} \rrbracket^{\mathbb{A}^\sharp} \mu)) = \gamma\left(\bigsqcup \left\{ \left(\lambda\mu.\eta^\sharp \sqcup \llbracket \mathsf{C} \rrbracket^{\mathbb{A}^\sharp} \mu\right)^n \bot^\sharp \mid n \in \mathbb{N} \right\}\right)$$

$$\left(\llbracket \mathsf{fix}(\mathsf{C}) \rrbracket^{\mathbb{A}} \circ \gamma\right) \eta^\sharp = \mathrm{lfp}(\lambda\mu.\gamma(\eta^\sharp) \sqcup \llbracket \mathsf{C} \rrbracket^{\mathbb{A}} \mu) = \bigsqcup \left\{ \left(\lambda\mu.\gamma(\eta^\sharp) \sqcup \llbracket \mathsf{C} \rrbracket^{\mathbb{A}} \mu\right)^n \bot \mid n \in \mathbb{N} \right\}$$

We can now prove by induction on n that the two are in a $\sqsubseteq$ relation. We do this by first proving that for all $k \in \mathbb{N}$

$$f^k \bot \sqsubseteq \gamma\left(\left(f^\sharp\right)^k \bot^\sharp\right)$$

by induction on k.

Case ($n = 0$). In this case

$$\gamma\left(\left(\lambda\mu.\eta^\sharp \sqcup \llbracket \mathsf{C} \rrbracket^{\mathbb{A}^\sharp} \mu\right)^0 \bot^\sharp\right) = \gamma(\bot^\sharp)$$

$$\left(\lambda\mu.\gamma(\eta^\sharp) \sqcup \llbracket \mathsf{C} \rrbracket^{\mathbb{A}} \mu\right)^0 \bot = \bot$$

hence $\bot \sqsubseteq \gamma(\bot^\sharp)$ and our thesis holds.

Case ($n \implies n+1$). Let's call $f^\sharp = \lambda\mu.\eta^\sharp \sqcup \llbracket \mathsf{C} \rrbracket^{\mathbb{A}^\sharp} \mu$ and $f = \lambda\mu.\gamma(\eta^\sharp) \sqcup \llbracket \mathsf{C} \rrbracket^{\mathbb{A}} \mu$. First we can observe that

$$f^{n+1} \bot = f(f^n \bot) = \gamma\left(\eta^\sharp\right) \sqcup \llbracket \mathsf{C} \rrbracket^{\mathbb{A}}(f^n \bot)$$

$$f^{\sharp\, n+1} \bot^\sharp = f^\sharp(f^{\sharp\, n} \bot) = \eta^\sharp \sqcup \llbracket \mathsf{C} \rrbracket^{\mathbb{A}^\sharp}(f^{\sharp\, n} \bot^\sharp)$$

From this we can observe that

$$\begin{aligned}
\gamma\left(f^\sharp(f^{\sharp\, n} \bot^\sharp)\right) &= \gamma\left(\eta^\sharp \sqcup \llbracket \mathsf{C} \rrbracket^{\mathbb{A}^\sharp}(f^{\sharp\, n} \bot^\sharp)\right) \\
&= \bigsqcup \left\{ c \in \mathbb{A} \mid \alpha(c) \sqsubseteq \eta^\sharp \sqcup \llbracket \mathsf{C} \rrbracket^{\mathbb{A}^\sharp}(f^{\sharp\, n} \bot^\sharp) \right\} && \text{by Property 4 of Galois connections.} \\
&\sqsupseteq \gamma(\eta^\sharp) \sqcup \gamma\left(\llbracket \mathsf{C} \rrbracket^{\mathbb{A}^\sharp}(f^{\sharp\, n} \bot^\sharp)\right) && \text{by } (\alpha \circ \gamma) \text{ reductivity} \\
&\sqsupseteq \gamma(\eta^\sharp) \sqcup \llbracket \mathsf{C} \rrbracket^{\mathbb{A}} \gamma(f^{\sharp\, n} \bot^\sharp) && \text{by induction on } \mathsf{C} \\
&\sqsupseteq \gamma(\eta^\sharp) \sqcup \llbracket \mathsf{C} \rrbracket^{\mathbb{A}}(f^n \bot) && \text{by induction on } n \text{ and monotonicity of } \llbracket \cdot \rrbracket^{\mathbb{A}}
\end{aligned}$$

which is our thesis.

Hence $f^n \bot \sqsubseteq \gamma(f^{\sharp\, n} \bot^\sharp)$, for all $n \in \mathbb{N}$, therefore

$$\begin{aligned}
\left(\llbracket \mathsf{fix}(\mathsf{C}) \rrbracket^{\mathbb{A}} \circ \gamma\right) \eta^\sharp &= \bigsqcup \left\{ \left(\lambda\mu.\gamma(\eta^\sharp) \sqcup \llbracket \mathsf{C} \rrbracket^{\mathbb{A}} \mu\right)^n \bot \mid n \in \mathbb{N} \right\} \\
&\sqsubseteq \gamma\left(\bigsqcup \left\{ \left(\lambda\mu.\eta^\sharp \sqcup \llbracket \mathsf{C} \rrbracket^{\mathbb{A}^\sharp} \mu\right)^n \bot^\sharp \mid n \in \mathbb{N} \right\}\right) \\
&= \left(\gamma \circ \llbracket \mathsf{fix}(\mathsf{C}) \rrbracket^{\mathbb{A}^\sharp}\right) \eta^\sharp
\end{aligned}$$

Which is our thesis.

□

We can also observe that best correct approximations (from Definition 1.24) induce sound semantics:

Corollary 3.3 (**bca induces soundness**). *Let* $\langle \mathbb{A}, \sqsubseteq \rangle, \langle \mathbb{A}^\sharp, \sqsubseteq^\sharp \rangle$ *be two abstract domains equipped with their respective orders s.t.* $\mathbb{A} \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} \mathbb{A}^\sharp$. *If for base expressions* $(\!(\cdot)\!)^{\mathbb{A}^\sharp} : \mathsf{Exp} \to \mathbb{A}^\sharp \to \mathbb{A}^\sharp$ *is defined as*

$$(\!(\mathsf{e})\!)^{\mathbb{A}^\sharp} \eta^\sharp \triangleq \alpha \left((\!(\mathsf{e})\!)^{\mathbb{A}} \gamma \left(\eta^\sharp \right) \right)$$

Then

$$\left([\![\mathsf{C}]\!]^{\mathbb{A}} \circ \gamma \right) \eta^\sharp \sqsubseteq \left(\gamma \circ [\![\mathsf{C}]\!]^{\mathbb{A}^\sharp} \right) \eta^\sharp$$

i.e., the abstract inductive semantics over $\mathbb{A}^\sharp$ *is sound w.r.t. the abstract inductive semantics over* $\mathbb{A}$.

Proof. The proof follows from Theorem 3.2, where we have to prove that for base cases the two semantics are sound. In this case we know that $(\!(\mathsf{e})\!)^{\mathbb{A}^\sharp} \eta^\sharp = \alpha((\!(\mathsf{e})\!)^{\mathbb{A}} \gamma(\eta^\sharp))$ and we have to prove that

$$((\!(\mathsf{e})\!)^{\mathbb{A}} \circ \gamma)\eta^\sharp \sqsubseteq (\gamma \circ (\!(\mathsf{e})\!)^{\mathbb{A}^\sharp})\eta^\sharp$$

equivalently, we can substitute and notice that we can prove that

$$(\!(\mathsf{e})\!)^{\mathbb{A}}(\gamma(\eta^\sharp)) \sqsubseteq \gamma(\alpha((\!(\mathsf{e})\!)^{\mathbb{A}} \gamma(\eta^\sharp))).$$

Here we can call $\rho = (\!(\mathsf{e})\!)^{\mathbb{A}}(\gamma(\eta^\sharp))$ and notice that by extensivity $\forall \rho \in \mathbb{A}$

$$\rho \sqsubseteq (\gamma \circ \alpha)\rho$$
$$(\!(\mathsf{e})\!)^{\mathbb{A}}(\gamma(\eta^\sharp)) \sqsubseteq (\gamma \circ \alpha) \left((\!(\mathsf{e})\!)^{\mathbb{A}}(\gamma(\eta^\sharp)) \right)$$

which is our thesis. □

Lemma 3.4 ($\mathsf{fix}(\mathsf{C})$ **is syntactic sugar**). *For all* $\eta \in \mathbb{A}$, $[\![\mathsf{fix}(\mathsf{C})]\!]^{\mathbb{A}} \eta = [\![(\mathsf{true} + \mathsf{C})^*]\!]^{\mathbb{A}} \eta$.

Proof. First, let

$$f = \lambda \mu. (\eta \sqcup \mu \sqcup [\![\mathsf{C}]\!]^{\mathbb{A}} \mu)$$
$$g = \lambda \mu. (\mu \sqcup [\![\mathsf{C}]\!]^{\mathbb{A}} \mu)$$

Let us first show by induction that

$$\forall i \geqslant 0 \quad f^{i+1}(\bot) = g^i(\eta) \tag{3.4}$$

Case $(i = 0)$. $f(\bot) = \eta \sqcup \bot \sqcup [\![\mathsf{C}]\!]^{\mathbb{A}} \bot = \eta = g^0(\eta)$.

Case $(i + 1)$.

$$\begin{aligned}
g^{i+1}(\eta) &= g(g^i(\eta)) \\
&= g(f^{i+1}(\bot)) && \text{By induction on } i \\
&= f^{i+1}(\bot) \sqcup [\![\mathsf{C}]\!]^{\mathbb{A}} f^{i+1}(\bot) \\
&= \eta \sqcup f^{i+1}(\bot) \sqcup [\![\mathsf{C}]\!]^{\mathbb{A}} f^{i+1}(\bot) && \text{Since } \eta \sqsubseteq f(\bot) \\
&= f(f^{i+1}(\bot)) \\
&= f^{i+2}(\bot)
\end{aligned}$$

Let us also show that:

$$\mathrm{lfp}(g) = \mathrm{lfp}(f) \tag{3.5}$$

Observe that $\mathrm{lfp}(g) = g(\mathrm{lfp}(g)) = \eta \sqcup [\![\mathsf{C}]\!]^{\mathbb{A}}(\mathrm{lfp}(g))$, so we have that:

$$\eta \sqcup \mathrm{lfp}(g) \sqcup [\![\mathsf{C}]\!]^{\mathbb{A}}(\mathrm{lfp}(g)) \sqsubseteq \mathrm{lfp}(g)$$

As a consequence, $\mathrm{lfp}(f) \sqsubseteq \mathrm{lfp}(g)$ holds. The reverse inequality follows because, for all μ,

$$g(\mu) = \eta \sqcup [\![\mathsf{C}]\!]^{\mathbb{A}}\mu \sqsubseteq \eta \sqcup \mu \sqcup [\![\mathsf{C}]\!]^{\mathbb{A}}\mu = f(\mu)$$

Then, we have that:

$$\begin{aligned}
[\![\mathsf{fix}(\mathsf{C})]\!]^{\mathbb{A}}\eta &= \mathrm{lfp}\left(\lambda\mu.\left(\eta \sqcup [\![\mathsf{C}]\!]^{\mathbb{A}}\mu\right)\right) \\
&= \mathrm{lfp}\left(\lambda\mu.\left(\eta \sqcup \mu \sqcup [\![\mathsf{C}]\!]^{\mathbb{A}}\mu\right)\right) && \text{By (3.5)} \\
&= \bigsqcup_{i\in\mathbb{N}} f^i\bot && \text{By Knaster-Tarski Theorem} \\
&= \bot \sqcup \bigsqcup_{i\in\mathbb{N}} f^{i+1}\bot \\
&= \bigsqcup_{i\in\mathbb{N}} g^i\eta && \text{By (3.4)} \\
&= [\![(\mathsf{true} + \mathsf{C})^*]\!]^{\mathbb{A}}\eta
\end{aligned}$$

□

3.2 Interval domain

Interval analysis are among the most well known standard abstract domains in abstract interpretation. They are generally studied as simple non-relational domains, as intervals are not able to capture the relation between variables occurring in the program. The following chapter aims at proving that interval analysis is decidable without a widening operator, i.e., despite the presence of infinite ascending chains the exact value of the analysis can be computed.

We first define what the set of intervals $\mathbb{I}$ is and its abstraction and concretization map to the powerset of integers.

Definition 3.5 (Integer intervals)**.** We call

$$\mathbb{I} \triangleq \{[a,b] \mid a \in \mathbb{Z} \cup \{-\infty\} \wedge b \in \mathbb{Z} \cup \{+\infty\} \wedge a \leqslant b\} \cup \{\bot\}$$

the set of integer intervals. In the rest of the thesis we will write $\top$ instead of $[-\infty, +\infty]$

In order to later do the variable-wise lifting of the intervals domain and relate it to the concrete environment $\mathcal{C}$ we need to define concretization and abstraction maps for the intervals domain

Definition 3.6. We define the *concretization map* $\gamma : \mathbb{I} \to \wp(\mathbb{Z})$ as

$$\begin{aligned}
\gamma([a,b]) &\triangleq \{x \in \mathbb{Z} \mid a \leqslant x \leqslant b\} \\
\gamma(\bot) &\triangleq \varnothing
\end{aligned}$$

And the *abstraction map* $\alpha : \wp(\mathbb{Z}) \to \mathbb{I}$ as

$$\begin{aligned}
\alpha(\varnothing) &\triangleq \bot \\
\alpha(X) &\triangleq \begin{cases} \bot & \text{if } X = \varnothing \\ [\min(X), \max(X)] & \text{otherwise} \end{cases}
\end{aligned}$$

The next step is to define some order on $\mathbb{I}$. For this purpose we define a partial order $\sqsubseteq$ based on the concretization map.

Definition 3.7 (Partial order on $\mathbb{I}$)**.** Let $I, J \in \mathbb{I}$. Then

$$I \sqsubseteq J \iff \gamma(I) \subseteq \gamma(J)$$

Observe that $\langle \mathbb{I}, \sqsubseteq \rangle$ is a complete lattice. We next characterise least upper bound and greatest lower bound on the domain $\mathbb{I}$. Let $[a, b], [c, d] \in \mathbb{I}$

$$[a, b] \sqcup [c, d] \triangleq [\min(a, c), \max(b, d)]$$
$$[a, b] \sqcap [c, d] \triangleq \begin{cases} [\max(a, c), \min(b, d)] & \text{if } \min(b, d) < \max(a, c) \\ \bot & \text{otherwise} \end{cases}$$

The generalization to infinite sets is obtained in the obvious way, by replacing min and *max* with inf and sup. The next building block is the definition of some more operations on intervals, namely the addition and subtraction of an integer constant:

Definition 3.8 (Interval addition and subtraction)**.** For a nonempty interval $[a, b] \in \mathbb{I}$ and $c \in \mathbb{N}$ define $[a, b] \pm c \triangleq [a \pm c, b \pm c]$ (recall that conventionally $\pm\infty + c = \pm\infty - c = \pm\infty$).

3.2.1 Variable-wise lifting

We can therefore proceed to introduce the variable-wise lifting of the $\mathbb{I}$ domain, building the abstract domain $\dot{\mathbb{I}}$.

Definition 3.9 (Abstract integer domain)**.** Let $\mathbb{I}_* \triangleq \mathbb{I} \setminus \{\bot\}$. The abstract domain $\dot{\mathbb{I}}$ for program analysis is the variable-wise lifting of $\mathbb{I}$:

$$\dot{\mathbb{I}} \triangleq (\mathit{Var} \to \mathbb{I}_*) \cup \{\bot\}$$

In this domain, we define again abstraction and concretization maps, building a Galois connection with the concrete domain. We do so by overloading the α and γ functions, to refer also to the abstraction and concretization of abstract environments.

Definition 3.10. We define the *concretization map* of abstract environments $\eta \in \dot{\mathbb{I}}$, i.e., $\gamma : \dot{\mathbb{I}} \to \wp(\mathsf{Env})$ as follows

$$\dot{\gamma}(\bot) \triangleq \varnothing$$
$$\dot{\gamma}(\eta) \triangleq \{\rho \in \mathsf{Env} \mid \forall \mathtt{x} \in \mathit{Var} \quad \rho(\mathtt{x}) \in \gamma(\eta \mathtt{x})\}$$

and the *abstraction map* of sets of concrete environments $X \in \wp(\mathsf{Env})$, i.e., $\alpha : \wp(\mathsf{Env}) \to \dot{\mathbb{I}}$ as

$$\dot{\alpha}(\varnothing) \triangleq \bot$$
$$\dot{\alpha}(X) \triangleq \lambda \mathtt{x} \,.\, \alpha(\{\rho(\mathtt{x}) \mid \rho \in X\})$$

We can again define a notion of order for elements of $\dot{\mathbb{I}}$ based on the concretization map. We do by overloading the $\sqsubseteq$ notation. Let $\eta, \vartheta \in \dot{\mathbb{I}}$, then

$$\eta \sqsubseteq \vartheta \text{ iff } \dot{\gamma}(\eta) \subseteq \dot{\gamma}(\vartheta)$$

Notice that because of the definition of the concretization map (Definition 3.10)

$$\eta \sqsubseteq \vartheta \iff \forall \mathtt{x} \in \mathit{Var} \quad \eta(\mathtt{x}) \sqsubseteq \vartheta(\mathtt{x})$$

i.e., two abstract environments are ordered if every variable's interval of the first environment is contained in the interval of the second abstract environment. Also, the least upper bounds and greatest lower bounds are obtained by lifting the $\sqcup$ and $\sqcap$ operations, i.e., let $\eta, \vartheta \in \dot{\mathbb{I}}$, then

$$\eta \sqcap \vartheta = \sigma \quad \text{if } \sigma(\mathtt{x}) = \eta(\mathtt{x}) \sqcap \vartheta(\mathtt{x}) \quad \forall \mathtt{x} \in \mathit{Var}$$
$$\eta \sqcup \vartheta = \sigma \quad \text{if } \sigma(\mathtt{x}) = \eta(\mathtt{x}) \sqcup \vartheta(\mathtt{x}) \quad \forall \mathtt{x} \in \mathit{Var}$$

Again we can notice that $\langle \dot{\mathbb{I}}, \sqsubseteq \rangle$ is a complete lattice, as for every two elements $\eta, \vartheta \in \dot{\mathbb{I}}$ there exists both $\eta \sqcup \vartheta$ and $\eta \sqcap \vartheta$. With these premises we can define our abstract inductive semantics on intervals, by defining the base operations $((\cdot))^{\dot{\mathbb{I}}} : \mathsf{Exp} \to \dot{\mathbb{I}} \to \dot{\mathbb{I}}$

Definition 3.11 (Base expressions on intervals)**.** Let $\eta \in \dot{\mathbb{I}}$ then the base expressions semantics $(\!(\cdot)\!)^{\dot{\mathbb{I}}} : \mathsf{Exp} \to \dot{\mathbb{I}} \to \dot{\mathbb{I}}$ is recursively defined as

$$(\!(\mathtt{x} \in I)\!)^{\dot{\mathbb{I}}}\eta \triangleq \begin{cases} \eta[\mathtt{x} \mapsto \eta\mathtt{x} \sqcap I] & \text{if } \eta\mathtt{x} \sqcap I \neq \bot \\ \bot & \text{otherwise} \end{cases}$$

$$(\!(\mathtt{x} := k)\!)^{\dot{\mathbb{I}}}\eta \triangleq \eta[\mathtt{x} \mapsto [k, k]]$$

$$(\!(\mathtt{x} := \mathtt{y} + k)\!)^{\dot{\mathbb{I}}}\eta \triangleq \eta[\mathtt{x} \mapsto \eta\mathtt{y} + k]$$

With these base operations, $[\![\cdot]\!]^{\dot{\mathbb{I}}}$ is defined accordingly to Definition 3.1.

3.2.2 Properties

We can immediately see how in the abstract interval domain, the semantics of the Kleene star and the fixpoint operator is not the same. This intuitively happens because the Kleene star is the least upper bound of a chain of intervals, while the fix operator keeps iterating over least upper bounds.

Example 3.12. In the case exposed in Code 3.1, for instance, the following program P represents the difference between the Kleene Star and the Fix operator:

```
1  while x < 8 do
2    if x = 2
3      x := x+6;
4    endif;
5    x := x-3;
6    if x <= 0
7      x:=0;
8    endif;
9  done;
```

Code 3.1: Program P denoting $\mathsf{fix}(\mathsf{C})$ and C^* difference

starting with the finite interval $[3, 4]$ we get the following loop invariants:

$$\text{Kleene: } \sqcup\{[3,4],[0,1],[0,0],[0,0],\ldots\} = [0,4]$$
$$\text{Fix: } \sqcup\{\bot,[3,4],[0,4],[0,5],[0,5],\ldots\} = [0,5]$$

Both invariants are correct, because they over-approximate the most precise concrete invariant $\{0, 1, 3, 4\}$, however the Kleene invariant is strictly more precise than the Fix one.

3.3 Non relational collecting

We first define *non-relational collecting* analysis for the Imp language in a standard way, taking again the best correct approximation (bca) for the basic expressions in Exp. Unlike the Intervals domain, where we needed to define the set of intervals, the non-relational collecting analysis will rely on $\wp(\mathbb{Z})$ for the abstract values of each variable in the variable-wise lifting. As we already observed, $\langle \wp(\mathbb{Z}), \subseteq \rangle$ is a complete lattice, where the notions of $\cap$ and $\cup$ are well-known. The next building block is the definition of some more operations on intervals, namely the addition and subtraction of an integer constant:

Definition 3.13 (Set addition and subtraction)**.** For a nonempty set $S \in \wp(\mathbb{Z})$ and $c \in \mathbb{N}$ define $S \pm c \triangleq \{x \pm c \mid x \in S\}$ (recall that $\pm\infty + c = \pm\infty - c = \pm\infty$).

3.3.1 Variable-wise lifting

We can therefore proceed by introducing the variable-wise lifting of the domain $\wp(\mathbb{Z})$, building the abstract domain $\mathbb{C}$:

Definition 3.14 (Abstract Non relational collecting domain)**.** Let $\wp^*(\mathbb{Z}) = \wp(\mathbb{Z}) \setminus \{\varnothing\}$. The abstract domain $\mathbb{C}$ for program analysis is the variable-wise lifting of $\wp(\mathbb{Z})$:

$$\mathbb{C} \triangleq (\mathit{Var} \to \wp^*(\mathbb{Z})) \cup \{\bot\}$$

In this domain, we define again abstraction and concretization maps, building a Galois connection with the concrete domain

Definition 3.15. We define the *concretization map* of abstract environments $\eta \in \mathbb{C}$, i.e., $\gamma : \mathbb{C} \to \wp(\mathsf{Env})$ as follows

$$\begin{aligned}\gamma(\bot) &\triangleq \varnothing \\ \gamma(\eta) &\triangleq \{\rho \in \mathsf{Env} \mid \forall \mathtt{x} \in \mathit{Var} \quad \rho(\mathtt{x}) \in \eta\mathtt{x}\}\end{aligned}$$

and the *abstraction map* of sets of concrete environments $X \in \wp(\mathsf{Env})$, i.e., $\alpha : \wp(\mathsf{Env}) \to \mathbb{C}$ as

$$\begin{aligned}\alpha(\varnothing) &\triangleq \bot \\ \alpha(X) &\triangleq \lambda \mathtt{x} \,.\, \{\rho(\mathtt{x}) \mid \rho \in X\}\end{aligned}$$

We can again define a notion of order for elements of $\mathbb{C}$ based on the concretization map. Let $\eta, \vartheta \in \mathbb{C}$, then

$$\eta \dot{\subseteq} \vartheta \text{ iff } \gamma(\eta) \subseteq \gamma(\vartheta)$$

Notice that because of the definition of the concretization map (Definition 3.15)

$$\eta \dot{\subseteq} \vartheta \iff \forall \mathtt{x} \in \mathit{Var}\ \eta(\mathtt{x}) \dot{\subseteq} \vartheta(\mathtt{x})$$

we can notice that $\langle \mathbb{C}, \dot{\subseteq} \rangle$ is a complete lattice, as for every two elements $\eta, \vartheta \in \mathbb{C}$ there exists both $\eta \dot{\cup} \vartheta$ and $\eta \dot{\cap} \vartheta$ by characterising least upper bounds and greatest lower bounds as the lifting of $\sqcup$ and $\sqcap$ operations. Let again $\eta, \vartheta \in \mathbb{C}$, then

$$\begin{aligned}\eta \dot{\cap} \vartheta = \sigma \quad &\text{if } \sigma(\mathtt{x}) = \eta(\mathtt{x}) \cap \vartheta(\mathtt{x}) \quad \forall \mathtt{x} \in \mathit{Var} \\ \eta \dot{\cup} \vartheta = \sigma \quad &\text{if } \sigma(\mathtt{x}) = \eta(\mathtt{x}) \cup \vartheta(\mathtt{x}) \quad \forall \mathtt{x} \in \mathit{Var}\end{aligned}$$

Again With these premises we can now define base operations on the non-relational collecting abstraction:

Definition 3.16 (Base expressions on non-relational collecting)**.** Let $\eta \in \mathbb{C}$ and γ from Definition 3.6. The base expressions semantics $(\!(\cdot)\!)^{\mathbb{C}} : \mathsf{Exp} \to \mathbb{C} \to \mathbb{C}$ is recursively defined as

$$(\!(\mathtt{x} \in I)\!)^{\mathbb{C}}\eta \triangleq \begin{cases}\eta[\mathtt{x} \mapsto \eta\mathtt{x} \cap \gamma(I)] & \text{if } \eta\mathtt{x} \cap \gamma(I) \neq \varnothing \\ \bot & \text{otherwise}\end{cases}$$

$$(\!(\mathtt{x} := k)\!)^{\mathbb{C}}\eta \triangleq \begin{cases}\eta[\mathtt{x} \mapsto \{k\}] & \text{if } \eta\mathtt{x} \neq \top \\ \eta & \text{otherwise}\end{cases}$$

$$(\!(\mathtt{x} := \mathtt{y} + k)\!)^{\mathbb{C}}\eta \triangleq \begin{cases}\eta[\mathtt{x} \mapsto \eta\mathtt{y} + k] & \text{if } \eta\mathtt{x} \neq \top \\ \eta & \text{otherwise}\end{cases}$$

With these base operations, $[\![\cdot]\!]^{\mathbb{C}}$ is defined accordingly to Definition 3.1.

3.3.2 Properties

The non-relational collecting semantics is similar to the interval semantics we defined in Section 3.2, in the sense that both of them do not model relation between variables. Differing from interval analysis however, non-relational collecting semantics grains back additivity, which we loast with interval semantics. With additivity we can infer that $\mathsf{fix}(\mathsf{C})$ and C^* have the same semantics (with Proposition 3.18).

Let's denote as $\langle\!\langle \cdot \rangle\!\rangle$ the abstract semantics over $\mathbb{C}$, i.e., $\langle\!\langle \cdot \rangle\!\rangle = [\![\cdot]\!]^{\mathbb{C}}$.

Lemma 3.17 (Additivity)**.** *Let* $\eta, \vartheta \in \mathbb{C}$*,* $\mathsf{C} \in \mathsf{Imp}$ *then*

$$\langle\!\langle \mathsf{C} \rangle\!\rangle \left(\eta \dot\cup \vartheta\right) = (\langle\!\langle \mathsf{C} \rangle\!\rangle \eta) \dot\cup (\langle\!\langle \mathsf{C} \rangle\!\rangle \vartheta)$$

Proof. We can work by induction on C:

Case ($\mathtt{x} \in S$). Then

$$\begin{aligned}
\langle\!\langle \mathtt{x} \in S \rangle\!\rangle (\eta \dot\cup \vartheta) &= (\eta \dot\cup \vartheta)[\mathtt{x} \mapsto (\eta \dot\cup \vartheta)\mathtt{x} \cap S] \\
&= (\eta \dot\cup \vartheta)[\mathtt{x} \mapsto (\eta\mathtt{x} \cap S) \cup (\vartheta\mathtt{x} \cap S)] \\
&= (\eta[\mathtt{x} \mapsto (\eta\mathtt{x} \cap S)]) \dot\cup (\vartheta[\mathtt{x} \mapsto \vartheta\mathtt{x} \cap S]) \\
&= \langle\!\langle \mathtt{x} \in S \rangle\!\rangle \eta \dot\cup \langle\!\langle \mathtt{x} \in S \rangle\!\rangle \vartheta
\end{aligned}$$

Case ($\mathtt{x} := k$). Then

$$\begin{aligned}
\langle\!\langle \mathtt{x} := k \rangle\!\rangle (\eta \dot\cup \vartheta) &= (\eta \dot\cup \vartheta)[\mathtt{x} \mapsto \{k\}] \\
&= (\eta[\mathtt{x} \mapsto \{k\}]) \dot\cup (\vartheta[\mathtt{x} \mapsto \{k\}]) \\
&= \langle\!\langle \mathtt{x} := k \rangle\!\rangle \eta \dot\cup \langle\!\langle \mathtt{x} := k \rangle\!\rangle \vartheta
\end{aligned}$$

Case ($\mathtt{x} := \mathtt{y} + k$). Then

$$\begin{aligned}
\langle\!\langle \mathtt{x} := \mathtt{y} + k \rangle\!\rangle (\eta \dot\cup \vartheta) &= (\eta \dot\cup \vartheta)[\mathtt{x} \mapsto \mathtt{y} + k] \\
&= (\eta[\mathtt{x} \mapsto \mathtt{y} + k]) \dot\cup (\vartheta \mapsto \mathtt{y} + k) \\
&\langle\!\langle \mathtt{x} := \mathtt{y} + k \rangle\!\rangle \eta \dot\cup \langle\!\langle \mathtt{x} := \mathtt{y} + k \rangle\!\rangle \vartheta
\end{aligned}$$

Case ($\mathsf{C} \equiv \mathsf{C}_1 + \mathsf{C}_2$). Then

$$\begin{aligned}
\langle\!\langle \mathsf{C}_1 + \mathsf{C}_2 \rangle\!\rangle (\eta \dot\cup \sigma) &= \langle\!\langle \mathsf{C}_1 \rangle\!\rangle (\eta \dot\cup \sigma) \dot\cup \langle\!\langle \mathsf{C}_2 \rangle\!\rangle (\eta \dot\cup \sigma) && \text{by definition} \\
&= \langle\!\langle \mathsf{C}_1 \rangle\!\rangle \eta \dot\cup \langle\!\langle \cup_1 \rangle\!\rangle \vartheta \dot\cup \langle\!\langle \mathsf{C}_2 \rangle\!\rangle \eta \dot\cup \langle\!\langle \cup_2 \rangle\!\rangle \vartheta && \text{by inductive hypothesis} \\
&= \langle\!\langle \mathsf{C}_1 + \mathsf{C}_2 \rangle\!\rangle \eta \dot\cup \langle\!\langle \mathsf{C}_1 + \mathsf{C}_2 \rangle\!\rangle \vartheta
\end{aligned}$$

Case ($\mathsf{C} \equiv \mathsf{C}_1; \mathsf{C}_2$). Then

$$\begin{aligned}
\langle\!\langle \mathsf{C}_1; \mathsf{C}_2 \rangle\!\rangle (\eta \dot\cup \sigma) &= \langle\!\langle \mathsf{C}_2 \rangle\!\rangle (\langle\!\langle \mathsf{C}_1 \rangle\!\rangle (\eta \dot\cup \vartheta)) \\
&= \langle\!\langle \mathsf{C}_2 \rangle\!\rangle \left(\langle\!\langle \mathsf{C}_1 \rangle\!\rangle \eta \dot\cup \langle\!\langle \cup_1 \rangle\!\rangle \vartheta\right) && \text{by inductive hypothesis} \\
&= \langle\!\langle \mathsf{C}_2 \rangle\!\rangle (\langle\!\langle \mathsf{C}_1 \rangle\!\rangle \eta) \dot\cup \langle\!\langle \mathsf{C}_2 \rangle\!\rangle (\langle\!\langle \mathsf{C}_1 \rangle\!\rangle \vartheta) && \text{by inductive hypothesis}
\end{aligned}$$

Case ($\mathsf{C} \equiv \mathsf{C}^*$). Then

$$\langle\!\langle \mathsf{C}^* \rangle\!\rangle (\eta \dot\cup \vartheta) = \dot\bigcup_{i \in \mathbb{N}} \langle\!\langle \mathsf{C} \rangle\!\rangle^i (\eta \dot\cup \vartheta)$$

What we have to show now is that $\forall i \in \mathbb{N}\ \langle\!\langle \mathsf{C} \rangle\!\rangle^i (\eta \dot\cup \vartheta) = \langle\!\langle \mathsf{C} \rangle\!\rangle^i \eta \dot\cup \langle\!\langle \mathsf{C} \rangle\!\rangle^i \vartheta$. We can show this by induction on i:

- $i = 0$. Then
$$\langle\!\langle \mathsf{C} \rangle\!\rangle^0 (\eta \dot\cup \vartheta) = \eta \dot\cup \vartheta = \langle\!\langle \mathsf{C} \rangle\!\rangle^0 \eta \dot\cup \langle\!\langle \mathsf{C} \rangle\!\rangle^0 \vartheta$$
and the statement holds.
- $i \implies i + 1$. Notice that
$$\begin{aligned}
\langle\!\langle \mathsf{C} \rangle\!\rangle^{i+1} (\eta \dot\cup \vartheta) &= \langle\!\langle \mathsf{C} \rangle\!\rangle \left(\langle\!\langle \mathsf{C} \rangle\!\rangle^i (\eta \dot\cup \vartheta)\right) \\
&= \langle\!\langle \mathsf{C} \rangle\!\rangle (\langle\!\langle \mathsf{C} \rangle\!\rangle^i \eta \dot\cup \langle\!\langle \mathsf{C} \rangle\!\rangle^i \vartheta) && \text{by inductive hypothesis} \\
&= \langle\!\langle \mathsf{C} \rangle\!\rangle^{i+1} \eta \dot\cup \langle\!\langle \mathsf{C} \rangle\!\rangle^{i+1} \vartheta && \text{by additivity}
\end{aligned}$$

Therefore

$$\begin{aligned}
\langle\!\langle \mathsf{C}^* \rangle\!\rangle(\eta \dot\cup \vartheta) &= \dot\bigcup_{i\in\mathbb{N}} \langle\!\langle \mathsf{C} \rangle\!\rangle^i(\eta \dot\cup \vartheta) \\
&= \dot\bigcup_{i\in\mathbb{N}} \langle\!\langle \mathsf{C} \rangle\!\rangle^i(\eta \dot\cup \vartheta) \\
&= \dot\bigcup_{i\in\mathbb{N}} \langle\!\langle \mathsf{C} \rangle\!\rangle^i\eta \dot\cup \langle\!\langle \mathsf{C} \rangle\!\rangle^i\vartheta \\
&= \left(\dot\bigcup_{i\in\mathbb{N}} \langle\!\langle \mathsf{C} \rangle\!\rangle^i\eta\right) \dot\cup \left(\dot\bigcup_{i\in\mathbb{N}} \langle\!\langle \mathsf{C} \rangle\!\rangle^i\vartheta\right) \\
&= \langle\!\langle \mathsf{C}^* \rangle\!\rangle\eta \dot\cup \langle\!\langle \mathsf{C}^* \rangle\!\rangle\vartheta
\end{aligned}$$

□

Proposition 3.18. $\mathsf{fix}(\mathsf{C})$ *and* C^* *semantics coincide:*

$$\langle\!\langle \mathsf{fix}(\mathsf{C}) \rangle\!\rangle = \langle\!\langle \mathsf{C}^* \rangle\!\rangle$$

Proof. Let $f = \lambda\mu.(\eta \dot\cup \langle\!\langle \mathsf{C} \rangle\!\rangle\mu)$

$$\begin{aligned}
\langle\!\langle \mathsf{fix}(\mathsf{C}) \rangle\!\rangle\eta &= \mathrm{lfp}(f) \\
&= \dot\bigcup_{i\in\mathbb{N}} \{f^n\bot \mid n \in \mathbb{N}\} && \text{by fixpoint Theorem 1.13} \\
&= \dot\bigcup_{i\in\mathbb{N}} \langle\!\langle \mathsf{C} \rangle\!\rangle^i\eta \\
&= \langle\!\langle \mathsf{C}^* \rangle\!\rangle\eta
\end{aligned}$$

□

Chapter 4

Program bounds and analysis termination

In this chapter we argue that for the language Imp the abstract semantics is computable in finite time without widening for abstract domains with some properties. Observe that the exact computation provides, already for our simple language, a precision which is not obtainable with (basic) widening and narrowing. In the example in Code 4.1 if we consider the intervals abstract domain, the semantics maps `x` and `y` to $[0, 2]$ and $[6, 8]$ respectively, while widening/narrowing to $[0, +\infty]$ and $[6, +\infty]$.

```
1   x:=0;
2   y:=0;
3   while (x<=5) do
4      if (y=0) then
5         y=y+1;
6      endif;
7      if (x==0) then
8         x:=y+7;
9      endif;
10  done;
```

Code 4.1: Code sample where analysis of $\mathsf{fix}(\mathsf{C})$ is less precise than C^*

Of course, for the collecting semantics this is not the case. Already computing a finite upper bound for loop invariants when they are finite is impossible as this would allow to decide termination, as we have seen in Section 2.5. First let's formalize the problem we want to solve.

Problem 4.1 (Analysis termination)**.** Given a program $\mathsf{C} \in \mathsf{Imp}$ and an abstract domain $\mathbb{A}$ with some top element $\top$, for all $\eta \in \mathbb{A}$, decide

$$[\![\mathsf{C}]\!]^{\mathbb{A}}\eta =^{?} \top$$

The main idea, based on previous research is to *bound* the domain $\mathbb{A}$. Each program is associated to a bound, an ideal value above which for each variable we can safely assume that the program diverges. First, given a program, we associate the program with a *lower bound* and an *upper bound*. The rough idea is that, whenever a variable is beyond its bound, the behavior of the program with respect to that variable becomes stable.

4.1 Program bounds

Definition 4.2 (**Program bound**). The *upper bound* associated with a command $\mathsf{C} \in \mathsf{Imp}$ is an integer number, denoted $(\mathsf{C})^{\mathsf{b}} \in \mathbb{N}$, defined inductively as follows:

$$
\begin{aligned}
(\mathtt{x} \in I)^{\mathsf{b}} &\triangleq \begin{cases} |\max(I)| & \text{if } \max(I) \in \mathbb{Z} \\ |\min(I)| & \text{if } \max(I) = +\infty \wedge \min(S) \neq -\infty \\ 0 & \text{otherwise} \end{cases} \\
(\mathtt{x} := k)^{\mathsf{b}} &\triangleq |k| \\
(\mathtt{x} := \mathtt{y} + k)^{\mathsf{b}} &\triangleq |k| \\
(\mathsf{C}_1 + \mathsf{C}_2)^{\mathsf{b}} &\triangleq (\mathsf{C}_1)^{\mathsf{b}} + (\mathsf{C}_2)^{\mathsf{b}} \\
(\mathsf{C}_1; \mathsf{C}_2)^{\mathsf{b}} &\triangleq (\mathsf{C}_1)^{\mathsf{b}} + (\mathsf{C}_2)^{\mathsf{b}} \\
(\mathsf{fix}(\mathsf{C}))^{\mathsf{b}} &\triangleq (|\mathit{vars}(\mathsf{C})| + 1)(\mathsf{C})^{\mathsf{b}}
\end{aligned}
$$

while the *lower bound* associated with a command $\mathsf{C} \in \mathsf{Imp}$ is again an integer number, denoted $(\mathsf{C})_{\mathsf{b}} \in \mathbb{N}$, defined inductively as follows:

$$
\begin{aligned}
(\mathtt{x} \in S)_{\mathsf{b}} &\triangleq \begin{cases} |\max(S)| & \text{if } \min(S) = -\infty \\ |\min(S)| & \text{if } \min(S) \in \mathbb{Z} \end{cases} \\
(\mathtt{x} := k)_{\mathsf{b}} &\triangleq |k| \\
(\mathtt{x} := \mathtt{y} + k)_{\mathsf{b}} &\triangleq |k| \\
(\mathsf{C}_1 + \mathsf{C}_2)_{\mathsf{b}} &\triangleq (\mathsf{C}_1)_{\mathsf{b}} + (\mathsf{C}_2)_{\mathsf{b}} \\
(\mathsf{C}_1; \mathsf{C}_2)_{\mathsf{b}} &\triangleq (\mathsf{C}_1)_{\mathsf{b}} + (\mathsf{C}_2)_{\mathsf{b}} \\
(\mathsf{fix}(\mathsf{C}))_{\mathsf{b}} &\triangleq (|\mathit{vars}(\mathsf{C})| + 1)(\mathsf{C})_{\mathsf{b}}
\end{aligned}
$$

where $\mathit{vars}(\mathsf{C})$ denotes the set of variables occurring in C.

We can notice that the two definitions of the bound $(\mathsf{C})^{\mathsf{b}}$ and $(\mathsf{C})_{\mathsf{b}}$ coincide, except for the filtering instruction $\mathtt{x} \in S$.

4.2 Bounding interval analysis

The following section aims at proving that by bounding the interval domain to a subdomain with no infinite ascending chains, i.e., where every chain converges in finite time, we can still compute the most precise interval representation for each variable in our program. To do so, we first prove an easy graph-theoretic property which will later be helpful. Consider a finite directed and edge-weighted graph $\langle X, \rightarrow \rangle$ where $\rightarrow \subseteq X \times \mathbb{Z} \times X$ and $x \rightarrow_h x'$ denotes that $(x, h, x') \in \rightarrow$. Consider a finite path in $\langle X, \rightarrow \rangle$

$$p = x_0 \rightarrow_{h_0} x_1 \rightarrow_{h_1} x_2 \rightarrow_{h_2} \ldots \rightarrow_{h_{\ell-1}} x_\ell$$

where:

(i). $\ell \geqslant 1$

(ii). the carrier size of p is $s(p) \triangleq |\{x_0, ..., x_\ell\}|$

(iii). the weight of p is $w(p) \triangleq \Sigma_{k=0}^{\ell-1} h_k$

(iv). the length of p is $|p| \triangleq \ell$

(v). given indices $0 \leqslant i < j \leqslant \ell$, $p_{i,j}$ denotes the subpath of p given by $x_i \to_{h_i} x_{i+1} \to_{i+1} \cdots \to_{h_{j-1}} x_j$ whose length is $j - i$; $p_{i,j}$ is a cycle if $x_i = x_j$.

Lemma 4.3 (**Positive cycles in weighted directed graphs**). *Let p be a finite path*

$$p = x_0 \to_{h_0} x_1 \to_{h_1} x_2 \to_{h_2} \cdots \to_{h_{\ell-1}} x_\ell$$

with $m \triangleq \max\{|h_j| \mid j \in \{0, \ldots, \ell-1\}\} \in \mathbb{N}$ and $w(p) > (|X| - 1)m$. Then, p has a subpath which is a cycle having a strictly positive weight.

Proof. First note that $w(p) = \Sigma_{k=0}^{\ell-1} h_k > (|X| - 1)m$ implies that $|p| = \ell \geqslant |X|$. Then, we show our claim by induction on $|p| = \ell \geqslant |X|$.
($|p| = |X|$): Since the path p includes exactly $|X|+1 = \ell+1$ nodes, there exist indices $0 \leqslant i < j \leqslant \ell$ such that $x_i = x_j$, i.e., $p_{i,j}$ is a subpath of p which is a cycle. Moreover, since this cycle $p_{i,j}$ includes at least one edge, we have that

$$\begin{aligned}
w(p_{i,j}) = w(p) - (\Sigma_{k=0}^{i-1} h_k + \Sigma_{k=j}^{\ell-1} h_k) > & \qquad \text{as } w(p) > (|X| - 1)m \\
(|X| - 1)\, m - (\Sigma_{k=0}^{i-1} h_k + \Sigma_{k=j}^{\ell-1} h_k) \geqslant & \qquad \text{as } \Sigma_{k=0}^{i-1} h_k + \Sigma_{k=j}^{\ell-1} h_k \leqslant (\ell - 1)m \\
(|X| - 1)m - (\ell - 1)m = & \qquad [\text{as } \ell = |X|] \\
(|X| - 1)m - (|X| - 1)m = 0 &
\end{aligned}$$

so that $w(p_{i,j}) > 0$ holds.

($|p| > |X|$): Since the path p includes at least $|X| + 2$ nodes, as in the base case, we have that p has a subpath which is a cycle. Then, we consider a cycle $p_{i,j}$ in p, for some indices $0 \leqslant i < j \leqslant \ell$, which is maximal, i.e., such that if $p_{i',j'}$ is a cycle in p, for some $0 \leqslant i' < j' \leqslant \ell$, then $p_{i,j}$ is not a proper subpath of $p_{i',j'}$.
If $w(p_{i,j}) > 0$ then we are done. Otherwise we have that $w(p_{i,j}) \leqslant 0$ and we consider the path p' obtained from p by stripping off the cycle $p_{i,j}$, i.e.,

$$p' \equiv \overbrace{x_0 \to_{h_0} x_1 \to_{h_1} \cdots \to_{h_{i-1}} x_i}^{p'_{0,i}} = \overbrace{x_j \to_{h_{j+1}} \cdots \to_{h_{\ell-1}} x_\ell}^{p'_{j+1,\ell}}$$

Since $|p'| < |p|$ and $w(p') = w(p) - w(p_{i,j}) \geqslant w(p) > (|X| - 1)m$, we can apply the inductive hypothesis on p'. We therefore derive that p' has a subpath q which is a cycle having strictly positive weight. This cycle q is either entirely in $p'_{0,i}$ or in $p'_{j+1,\ell}$, otherwise q would include the cycle $p_{i,j}$ thus contradicting the maximality of $p_{i,j}$. Hence, q is a cycle in the original path p having a strictly positive weight. □

We also preliminarly need to define the max function for intervals. More in detail $\max : \mathbb{I} \to \mathbb{Z}$ is defined as follows

$$\begin{aligned}
\max(\bot) &\triangleq -\infty \\
\max([a, b]) &\triangleq b
\end{aligned}$$

Notice in particular that since $\top = [-\infty, +\infty]$, $\max(\top) = +\infty$.

We will now prove a fundamental property of analaysis over the lattice of intervals: if a variable in a program does not diverge, then the increment of that variable is bounded by the constants in the program. This property will later be useful to restrict the domain of intervals (which incorporates infinite ascending and descending chains) to one of its subsets that does not contain such chains.

Notation 4.4. For the following proof and whenever we will refer to the abstract semantics over intervals we will use the notation $[\![\cdot]\!]$ to refer to $[\![\cdot]\!]^{\dot{\mathbb{I}}}$.

Lemma 4.5. *Let $\mathsf{C} \in \mathsf{Imp}$. For all $\eta \in \dot{\mathbb{I}}$ and $\mathsf{y} \in Var$, if $\max([\![\mathsf{C}]\!]\eta\mathsf{y}) \neq +\infty$ and $\max([\![\mathsf{C}]\!]\eta\mathsf{y}) > (\mathsf{C})^{\mathsf{b}}$ then there exist a variable $\mathsf{z} \in Var$ and an integer $h \in \mathbb{Z}$ such that $|h| \leqslant (\mathsf{C})^{\mathsf{b}}$ and the following two properties hold:*

(i) $\max([\![\mathsf{C}]\!]\eta\mathtt{y}) = \max(\eta\mathtt{z}) + h$;

(ii) *for all* $\eta' \in \dot{\mathbb{I}}$, *if* $\eta' \sqsupseteq \eta$ *then* $\max([\![\mathsf{C}]\!]\eta'\mathtt{y}) \geqslant \max(\eta'\mathtt{z}) + h$.

Proof. We preliminarly observe that we can safely assume $\eta \neq \bot$. In fact, if $\eta = \bot$ then $[\![\mathsf{C}]\!]\bot = \bot$ and thus $\max([\![\mathsf{C}]\!]\eta\mathtt{y}) = -\infty \leqslant (\mathsf{C})^{\mathsf{b}}$, against the hypothesis $\max([\![\mathsf{C}]\!]\eta\mathtt{y}) > (\mathsf{C})^{\mathsf{b}}$. Moreover, when quantifying over η' such that $\eta' \sqsupseteq \eta$ in (ii), if $\max([\![\mathsf{C}]\!]\eta'\mathtt{y}) = +\infty$ holds, then $\max([\![\mathsf{C}]\!]\eta'\mathtt{y}) \geqslant \max(\eta'\mathtt{z}) + h$ trivially holds, hence we will sometimes silently omit this case.

Case $(\mathtt{x} \in S)$. Take $\eta \in \dot{\mathbb{I}}$ and assume $+\infty \neq \max([\![\mathtt{x} \in S]\!]\eta\mathtt{y}) > (\mathtt{x} \in S)^{\mathsf{b}}$. Clearly $[\![\mathtt{x} \in S]\!]\eta \neq \bot$, otherwise we would get the contradiction $\max([\![\mathtt{x} \in S]\!]\eta\mathtt{y}) = -\infty \leqslant (\mathtt{x} \in S)^{\mathsf{b}}$.

We distinguish two cases:

- If $\mathtt{y} \neq \mathtt{x}$, then for all $\eta' \in \dot{\mathbb{I}}$ such that $\eta \sqsubseteq \eta'$ it holds

$$\bot \neq [\![\mathtt{x} \in S]\!]\eta' = \eta'[\mathtt{x} \mapsto \alpha_{\mathbb{I}}(\gamma_{\mathbb{I}}(\eta'(\mathtt{x})) \cap \gamma_{\mathbb{I}}(S))]$$

  and thus

$$\max([\![\mathtt{x} \in S]\!]\eta'\mathtt{y}) = \max(\eta'\mathtt{y}) = \max(\eta'\mathtt{y}) + 0$$

  hence the thesis follows with $\mathtt{z} = \mathtt{y}$ and $h = 0$.

- If $\mathtt{y} = \mathtt{x}$ then

$$\max([\![\mathtt{x} \in S]\!]\eta\mathtt{y}) = \max(\alpha_{\mathbb{I}}(\gamma_{\mathbb{I}}(\eta\mathtt{x}) \cap \gamma_{\mathbb{I}}(S)))$$

  Note that it cannot be $\max(S) \in \mathbb{Z}$. Otherwise, by Definition 4.2, $\max(\alpha_{\mathbb{I}}(\gamma_{\mathbb{I}}(\eta\mathtt{x}) \cap \gamma_{\mathbb{I}}(S))) \leqslant \max(S) = (\mathtt{x} \in S)^{\mathsf{b}}$, violating the assumption $\max([\![\mathtt{x} \in S]\!]\eta\mathtt{y}) > (\mathtt{x} \in S)^{\mathsf{b}}$. Hence, $\max(S) = +\infty$ must hold and therefore $\max(\alpha_{\mathbb{I}}(\gamma_{\mathbb{I}}(\eta\mathtt{x}) \cap \gamma_{\mathbb{I}}(S))) = \max(\eta(\mathtt{x})) = \max(\eta(\mathtt{x}))+0$. It is immediate to check that the same holds for all $\eta' \sqsupseteq \eta$, i.e.,

$$\max(\alpha_{\mathbb{I}}(\gamma_{\mathbb{I}}(\eta'\mathtt{x}) \cap \gamma_{\mathbb{I}}(S))) = \max(\eta'\mathtt{x}) + 0$$

  and thus the thesis follows with $\mathtt{z} = \mathtt{y} = \mathtt{x}$ and $h = 0$.

Case $(\mathtt{x} := k)$. Take $\eta \in \dot{\mathbb{I}}$ and assume $\max([\![\mathtt{x} := k]\!]\eta\mathtt{y}) > (\mathtt{x} := k)^{\mathsf{b}} = |k|$.

Observe that it cannot be $\mathtt{x} = \mathtt{y}$. In fact, since $[\![\mathtt{x} := k]\!]\eta = \eta[\mathtt{x} \mapsto \alpha_{\mathbb{I}}(\{k\})]$, we would have $[\![\mathtt{x} := k]\!]\eta\mathtt{y} = \alpha_{\mathbb{I}}(\{k\}) = [k, k]$ and thus

$$\max([\![\mathtt{x} := k]\!]\eta\mathtt{y}) = k \leqslant (\mathtt{x} := k)^{\mathsf{b}}$$

violating the assumption. Therefore, it must be $\mathtt{y} \neq \mathtt{x}$. Now, for all $\eta' \sqsupseteq \eta$, we have $[\![\mathtt{x} := k]\!]\eta'\mathtt{y} = \eta'\mathtt{y}$ and thus

$$\max([\![\mathtt{x} := k]\!]\eta'\mathtt{y}) = \max(\eta'\mathtt{y}) = \max(\eta'\mathtt{y}) + 0,$$

hence the thesis holds with $h = 0 \leqslant (\mathtt{x} := k)^{\mathsf{b}}$ and $\mathtt{z} = \mathtt{y}$.

Case $(\mathtt{x} := \mathtt{w} + k)$. Take $\eta \in \dot{\mathbb{I}}$ and assume $\max([\![\mathtt{x} := \mathtt{w} + k]\!]\eta\mathtt{y}) > (\mathtt{x} := \mathtt{w} + k)^{\mathsf{b}} = |k|$. Recall that $[\![\mathtt{x} := \mathtt{w} + k]\!]\eta = \eta[\mathtt{x} \mapsto \eta\mathtt{w} + k]$.

We distinguish two cases:

- If $\mathtt{y} \neq \mathtt{x}$, then for all $\eta' \sqsupseteq \eta$, we have $[\![\mathtt{x} := \mathtt{w} + k]\!]\eta'\mathtt{y} = \eta'\mathtt{y}$ and thus

$$\max([\![\mathtt{x} := \mathtt{w} + k]\!]\eta'\mathtt{y}) = \max(\eta'\mathtt{y})$$

  hence the thesis follows with $h = 0 \leqslant (\mathtt{x} := \mathtt{w} + k)^{\mathsf{b}}$ and $\mathtt{z} = \mathtt{y}$.

- If $\mathtt{x} = \mathtt{y}$ then for all $\eta' \sqsupseteq \eta$, we have $[\![\mathtt{x} := \mathtt{w} + k]\!]\eta'\mathtt{y} = \eta'\mathtt{w} + k$ and thus

$$\max([\![\mathtt{x} := \mathtt{w} + k]\!]\eta'\mathtt{y}) = \max(\eta'\mathtt{w}) + k$$

  hence, the thesis follows with $h = k$ (recall that $k \leqslant |k| = (\mathtt{x} := \mathtt{w} + k)^{\mathsf{b}}$) and $\mathtt{z} = \mathtt{w}$.

Case $(\mathsf{C}_1 + \mathsf{C}_2)$. Take $\eta \in \dot{\mathbb{I}}$ and assume $\max([\![\mathsf{C}_1 + \mathsf{C}_2]\!]\eta) > (\mathsf{C}_1 + \mathsf{C}_2)^{\mathsf{b}} = (\mathsf{C}_1)^{\mathsf{b}} + (\mathsf{C}_2)^{\mathsf{b}}$. Recall that $[\![\mathsf{C}_1 + \mathsf{C}_2]\!]\eta = [\![\mathsf{C}_1]\!]\eta \sqcup [\![\mathsf{C}_2]\!]\eta$. Hence, since $\max([\![\mathsf{C}_1 + \mathsf{C}_2]\!]\eta\mathtt{y}) \neq +\infty$, we have that $\max([\![\mathsf{C}_1]\!]\eta\mathtt{y}) \neq \infty \neq \max([\![\mathsf{C}_2]\!]\eta\mathtt{y})$. Moreover

$$\begin{aligned}\max([\![\mathsf{C}_1 + \mathsf{C}_2]\!]\eta\mathtt{y}) &= \max([\![\mathsf{C}_1]\!]\eta\mathtt{y} \sqcup [\![\mathsf{C}_2]\!]\eta\mathtt{y}) \\ &= \max\{\max([\![\mathsf{C}_1]\!]\eta\mathtt{y}), \max([\![\mathsf{C}_2]\!]\eta\mathtt{y})\}\end{aligned}$$

Thus $\max([\![\mathsf{C}_1 + \mathsf{C}_2]\!]\eta\mathtt{y}) = \max([\![\mathsf{C}_i]\!]\eta\mathtt{y})$ for some $i \in \{1, 2\}$. We can assume, without loss of generality, that the maximum is realized by the first component, i.e., $\max([\![\mathsf{C}_1 + \mathsf{C}_2]\!]\eta\mathtt{y}) = \max([\![\mathsf{C}_1]\!]\eta\mathtt{y}) > (\mathsf{C}_1 + \mathsf{C}_2)^{\mathsf{b}}$. Hence we can use the inductive hypothesis on C_1 and state that there exists $h \in \mathbb{Z}$ with $|h| \leqslant (\mathsf{C}_1)^{\mathsf{b}}$ and $\mathtt{z} \in \mathit{Var}$ such that $\max([\![\mathsf{C}_1]\!]\eta\mathtt{y}) = \max(\eta\mathtt{z}) + h$ and for all $\eta' \in \dot{\mathbb{I}}$, $\eta \sqsubseteq \eta'$,

$$\max([\![\mathsf{C}_1]\!]\eta'\mathtt{y}) \geqslant \max(\eta'\mathtt{z}) + h$$

Therefore

$$\max([\![\mathsf{C}_1 + \mathsf{C}_2]\!]\eta\mathtt{y}) = \max([\![\mathsf{C}_1]\!]\eta\mathtt{y}) = \max(\eta\mathtt{z}) + h$$

and and for all $\eta' \in \dot{\mathbb{I}}$, $\eta \sqsubseteq \eta'$,

$$\begin{aligned}\max([\![\mathsf{C}_1 + \mathsf{C}_2]\!]\eta'\mathtt{y}) &= \max\{\max([\![\mathsf{C}_1]\!]\eta'\mathtt{y}), \max([\![\mathsf{C}_2]\!]\eta'\mathtt{y})\} \\ &\geqslant \max([\![\mathsf{C}_1]\!]\eta'\mathtt{y}) \\ &\geqslant \max(\eta'\mathtt{z}) + h\end{aligned}$$

with $|h| \leqslant (\mathsf{C}_1)^{\mathsf{b}} \leqslant (\mathsf{C}_1 + \mathsf{C}_2)^{\mathsf{b}}$, as desired.

Case $(\mathsf{C}_1; \mathsf{C}_2)$. Take $\eta \in \dot{\mathbb{I}}$ and assume $\max([\![\mathsf{C}_1; \mathsf{C}_2]\!]\eta\mathtt{y}) > (\mathsf{C}_1; \mathsf{C}_2)^{\mathsf{b}} = (\mathsf{C}_1)^{\mathsf{b}} + (\mathsf{C}_2)^{\mathsf{b}}$. Recall that $[\![\mathsf{C}_1; \mathsf{C}_2]\!]\eta = [\![\mathsf{C}_2]\!]([\![\mathsf{C}_1]\!]\eta)$. If we define

$$[\![\mathsf{C}_1]\!]\eta = \eta_1$$

since $\max([\![\mathsf{C}_2]\!]\eta_1\mathtt{y}) \neq \infty$ and $\max([\![\mathsf{C}_2]\!]\eta_1\mathtt{y}) > (\mathsf{C}_1; \mathsf{C}_2)^{\mathsf{b}} \geqslant (\mathsf{C}_2)^{\mathsf{b}}$, by inductive hypothesis on C_2, there are $|h_2| \leqslant (\mathsf{C}_2)^{\mathsf{b}}$ and $\mathtt{w} \in \mathit{Var}$ such that $\max([\![\mathsf{C}_2]\!]\eta_1\mathtt{y}) = \max(\eta_1\mathtt{w}) + h_2$ and for all $\eta_1' \in \dot{\mathbb{I}}$ with $\eta_1 \sqsubseteq \eta_1'$

$$\max([\![\mathsf{C}_2]\!]\eta_1'\mathtt{y}) \geqslant \max(\eta_1'\mathtt{w}) + h_2 \tag{4.1}$$

Now observe that $\max([\![\mathsf{C}_1]\!]\eta\mathtt{w}) = \max(\eta_1\mathtt{w}) > (\mathsf{C}_1)^{\mathsf{b}}$. Otherwise, if it were $\max(\eta_1\mathtt{w}) \leqslant (\mathsf{C}_1)^{\mathsf{b}}$ we would have

$$\max([\![\mathsf{C}_2]\!]\eta_1\mathtt{y}) = \max(\eta_1\mathtt{w}) + h_2 \leqslant (\mathsf{C}_1)^{\mathsf{b}} + (\mathsf{C}_2)^{\mathsf{b}} = (\mathsf{C}_1; \mathsf{C}_2)^{\mathsf{b}},$$

violating the hypotheses. Moreover, $\max([\![\mathsf{C}_1]\!]\eta\mathtt{w}) \neq +\infty$, otherwise we would have $\max([\![\mathsf{C}_2]\!]\eta_1\mathtt{y}) = \max(\eta_1\mathtt{w}) + h_2 = +\infty$, contradicting the hypotheses. Therefore we can apply the inductive hypothesis also to C_1 and deduce that there are $|h_1| \leqslant (\mathsf{C}_1)^{\mathsf{b}}$ and $\mathtt{w}' \in \mathit{Var}$ such that $\max([\![\mathsf{C}_1]\!]\eta\mathtt{w}) = \max(\eta\mathtt{w}') + h_1$ and for all $\eta' \in \dot{\mathbb{I}}$ with $\eta \sqsubseteq \eta'$

$$\max([\![\mathsf{C}_1]\!]\eta'\mathtt{w}) \geqslant \max(\eta'\mathtt{w}') + h_1 \tag{4.2}$$

Summing up:

$$\begin{aligned}\max([\![\mathsf{C}_1; \mathsf{C}_2]\!]\eta\mathtt{y}) &= \max([\![\mathsf{C}_2]\!]([\![\mathsf{C}_1]\!]\eta)\mathtt{y}) \\ &= \max([\![\mathsf{C}_2]\!]\eta_1\mathtt{y}) \\ &= \max(\eta_1\mathtt{w}) + h_2 \\ &= \max([\![\mathsf{C}_1]\!]\eta\mathtt{w}) + h_2 \\ &= \max(\eta\mathtt{w}') + h_1 + h_2.\end{aligned}$$

Now, for all $\eta' \in \dot{\mathbb{I}}$ with $\eta \sqsubseteq \eta'$ we have that:

$$\begin{array}{rl} \max([\![\mathsf{C}_1;\mathsf{C}_2]\!]\eta'\mathtt{y}) = & \\ \max([\![\mathsf{C}_2]\!]([\![\mathsf{C}_1]\!]\eta')\mathtt{y}) \geqslant & \\ \max([\![\mathsf{C}_1]\!]\eta'\mathtt{w}) + h_2 \geqslant & \text{by (4.1), since } \eta_1 = [\![\mathsf{C}_1]\!]\eta \sqsubseteq [\![\mathsf{C}_1]\!]\eta' \text{ and monotonicity} \\ (\max(\eta'\mathtt{w}') + h_1) + h_2 & \text{by (4.2)} \end{array}$$

Thus, the thesis holds with $h = h_1 + h_2$, as $|h| = |h_1 + h_2| \leqslant |h_1| + |h_2| \leqslant (\mathsf{C}_1)^{\mathsf{b}} + (\mathsf{C}_2)^{\mathsf{b}} = (\mathsf{C}_1;\mathsf{C}_2)^{\mathsf{b}}$, as needed.

Case ($\mathsf{fix}(\mathsf{C})$). Let $\eta \in \dot{\mathbb{I}}$ such that $\max([\![\mathsf{fix}(\mathsf{C})]\!]\eta\mathtt{y}) \neq +\infty$. Recall that $[\![\mathsf{fix}(\mathsf{C})]\!]\eta = \mathrm{lfp}\,(\lambda\mu.([\![\mathsf{C}]\!]\mu \sqcup \eta))$. Observe that the least fixpoint of $\lambda\mu.([\![\mathsf{C}]\!]\mu \sqcup \eta)$ coincides with the least fixpoint of $\lambda\mu.([\![\mathsf{C}]\!]\mu \sqcup \mu) = \lambda\mu.[\![\mathsf{C} + \mathsf{true}]\!]\mu$ above η. Hence, if

$$\begin{array}{c} \eta_0 \triangleq \eta \\ \text{for all } i \in \mathbb{N} \quad \eta_{i+1} \triangleq [\![\mathsf{C}]\!]\eta_i \sqcup \eta_i = [\![\mathsf{C} + \mathsf{true}]\!]\eta_i \sqsupseteq \eta_i \end{array}$$

then we define an increasing chain $\{\eta_i\}_{i\in\mathbb{N}} \subseteq \dot{\mathbb{I}}$ such that

$$[\![\mathsf{fix}(\mathsf{C})]\!]\eta = \bigsqcup_{i\in\mathbb{N}} \eta_i.$$

Since $\max([\![\mathsf{fix}(\mathsf{C})]\!])\eta\mathtt{y} \neq +\infty$, we have that for all $i \in \mathbb{N}$, $\max(\eta_i\mathtt{y}) \neq +\infty$. Moreover, $\bigsqcup_{i\in\mathbb{N}} \eta_i$ on $\mathtt{y}$ is finitely reached in the chain $\{\eta_i\}_{i\in\mathbb{N}}$, i.e., there exists $m \in \mathbb{N}$ such that for all $i \geqslant m+1$

$$\max([\![\mathsf{fix}(\mathsf{C})]\!]\eta\mathtt{y}) = \max(\eta_i\mathtt{y}).$$

The inductive hypothesis holds for C and true, hence for $\mathsf{C} + \mathsf{true}$, therefore for all $\mathtt{x} \in \mathit{Var}$ and $j \in \{0, 1, \ldots, m\}$, if $\max(\eta_{j+1}\mathtt{x}) > (\mathsf{C} + \mathsf{true})^{\mathsf{b}} = (\mathsf{C})^{\mathsf{b}}$ then there exist $\mathtt{z} \in \mathit{Var}$ and $h \in \mathbb{Z}$ such that $|h| \leqslant (\mathsf{C})^{\mathsf{b}}$ and

(a) $+\infty \neq \max(\eta_{j+1}\mathtt{x}) = \max(\eta_j\mathtt{z}) + h$,

(b) $\forall \eta' \sqsupseteq \eta_j.\, \max([\![\mathsf{C} + \mathsf{true}]\!]\eta'\mathtt{x}) \geqslant \max(\eta'\mathtt{z}) + h$.

To shortly denote that the two conditions (a) and (b) hold, we write

$$(\mathtt{z}, j) \to_h (\mathtt{x}, j+1)$$

Now, assume that for some variable $\mathtt{y} \in \mathit{Var}$

$$\max([\![\mathsf{fix}(\mathsf{C})]\!]\eta\mathtt{y}) = \max(\eta_{m+1}\mathtt{y}) > (\mathsf{fix}(\mathsf{C}))^{\mathsf{b}} = (n+1)(\mathsf{C})^{\mathsf{b}}$$

where $n = |\mathit{vars}(\mathsf{C})|$. We want to show that the thesis holds, i.e., that there exist $\mathtt{z} \in \mathit{Var}$ and $h \in \mathbb{Z}$ with $|h| \leqslant (\mathsf{fix}(\mathsf{C}))^{\mathsf{b}}$ such that:

$$\max([\![\mathsf{fix}(\mathsf{C})]\!]\eta\mathtt{y}) = \max(\eta\mathtt{z}) + h \tag{4.3}$$

and for all $\eta' \sqsupseteq \eta$,

$$\max([\![\mathsf{fix}(\mathsf{C})]\!]\eta'\mathtt{y}) \geqslant \max(\eta'\mathtt{z}) + h \tag{4.4}$$

Let us consider (4.3). We first observe that we can define a path

$$\sigma \triangleq (\mathtt{y}_0, 0) \to_{h_0} (\mathtt{y}_1, 1) \to_{h_1} \ldots \to_{h_m} (\mathtt{y}_{m+1}, m+1) \tag{4.5}$$

such that $\mathtt{y}_{m+1} = \mathtt{y}$ and for all $j \in \{0, \ldots, m+1\}$, $\mathtt{y}_j \in \mathit{Var}$ and $\max(\eta_j\mathtt{y}_j) > (\mathsf{C})^{\mathsf{b}}$. In fact, if, by contradiction, this were not the case, there would exist an index $i \in \{0, \ldots, m\}$

(as $\max(\eta_{m+1}\mathtt{y}_{m+1}) > (\mathsf{C})^{\mathsf{b}}$ already holds) such that $\max(\eta_i\mathtt{y}_i) \leqslant (\mathsf{C})^{\mathsf{b}}$, while for all $j \in \{i+1,\ldots,m+1\}$, $\max(\eta_j\mathtt{y}_j) > (\mathsf{C})^{\mathsf{b}}$. Thus, in such a case, we consider the nonempty path:

$$\pi \triangleq (\mathtt{y}_i, i) \to_{h_i} (\mathtt{y}_{i+1}, i+1) \to_{h_{i+1}} \ldots \to_{h_m} (\mathtt{y}_{m+1}, m+1) \tag{4.6}$$

and we have that:

$$\begin{aligned}
&\Sigma_{j=i}^{m} h_j = \\
&\Sigma_{j=i}^{m} \max(\eta_{j+1}\mathtt{y}_{j+1}) - \max(\eta_j\mathtt{y}_j) = \\
&\max(\eta_{m+1}\mathtt{y}_{m+1}) - \max(\eta_i\mathtt{y}_i) = \\
&\max(\eta_{m+1}\mathtt{y}) - \max(\eta_i\mathtt{y}_i) > \\
&(n+1)(\mathsf{C})^{\mathsf{b}} - (\mathsf{C})^{\mathsf{b}} = n(\mathsf{C})^{\mathsf{b}}
\end{aligned}$$

with $|h_j| \leqslant (\mathsf{C})^{\mathsf{b}}$ for $j \in \{i,\ldots,m\}$. Hence we can apply Lemma 4.3 to the projection π_p of the nodes of this path π to the variable component to deduce that π_p has a subpath which is a cycle with a strictly positive weight. More precisely, there exist $i \leqslant k_1 < k_2 \leqslant m+1$ such that $\mathtt{y}_{k_1} = \mathtt{y}_{k_2}$ and $h = \Sigma_{j=k_1}^{k_2-1} h_j > 0$. If we denote $\mathtt{w} = \mathtt{y}_{k_1} = \mathtt{y}_{k_2}$, then we have that

$$\begin{aligned}
\max(\eta_{k_2}\mathtt{w}) &= h_{k_2-1} + \max(\eta_{k_2-1}\mathtt{w}) \\
&= h_{k_2-1} + h_{k_2-2} + \max(\eta_{k_2-2}\mathtt{w}) \\
&= \Sigma_{j=k_1}^{k_2-1} h_j + \max(\eta_{k_1}\mathtt{w}) \\
&= h + \max(\eta_{k_1}\mathtt{w})
\end{aligned}$$

Thus,

$$\max(\llbracket \mathsf{C} + \mathsf{true} \rrbracket^{k_2-k_1} \eta_{k_1}\mathtt{w}) = \max(\eta_{k_1}\mathtt{w}) + h$$

Observe that for all $\eta' \sqsupseteq \eta_{k_1}$

$$\max\left(\llbracket \mathsf{C} + \mathsf{true} \rrbracket^{k_2-k_1} \eta'\mathtt{w}\right) \geqslant \max(\eta'\mathtt{w}) + h \tag{4.7}$$

Let us show Property (4.7) by induction on $\ell = k_2 - k_1 \geqslant 1$.

Case ($\ell = 1$). Notice that by (b) used to build π in (4.6) it holds that $\forall \eta' \sqsupseteq \eta_{k_1} \sqsupseteq \eta$

$$\max\left(\llbracket \mathsf{C} + \mathsf{true} \rrbracket \eta'\mathtt{w}\right) \geqslant \max(\eta'\mathtt{w}) + h$$

hence the thesis holds.

Case ($\ell \implies \ell+1$). Recall that

$$\left(\llbracket \mathsf{C} + \mathsf{true} \rrbracket\right)^{\ell+1} \eta' = \left(\llbracket \mathsf{C} + \mathsf{true} \rrbracket\right) \left(\left(\left(\llbracket \mathsf{C} + \mathsf{true} \rrbracket\right)^{\ell}\right) \eta'\right)$$

and by inductive hypothesis $\max\left(\left(\llbracket \mathsf{C} + \mathsf{true} \rrbracket\right)^{\ell} \eta'\mathtt{w}\right) \geqslant \max\left(\eta'\mathtt{w}\right) + h$. Recall that for all $\eta'' \in \dot{\mathbb{I}}\ \llbracket \mathsf{C} + \mathsf{true} \rrbracket \eta'' = \eta'' \sqcup \llbracket \mathsf{C} \rrbracket \eta''$. Hence we can notice that $\max(\llbracket \mathsf{C} + \mathsf{true} \rrbracket \eta'')\mathtt{x} \geqslant \max(\eta'')\mathtt{x}$ for all $\mathtt{x} \in \mathit{Var}$. Therefore

$$\max\left(\llbracket \mathsf{C} + \mathsf{true} \rrbracket \left(\left(\llbracket \mathsf{C} + \mathsf{true} \rrbracket\right)^{\ell} \eta'\right) \mathtt{w}\right) \geqslant \max\left(\left(\llbracket \mathsf{C} + \mathsf{true} \rrbracket\right)^{\ell} \eta'\mathtt{w}\right) \geqslant \max(\eta'\mathtt{w}) + h$$

which is our thesis for Property (4.7).

Then, an inductive argument allows us to show that for all $r \in \mathbb{N}$:

$$\max(\llbracket \mathsf{C} + \mathsf{true} \rrbracket^{r(k_2-k_1)} \eta_{k_1}\mathtt{w}) \geqslant \max(\eta_{k_1}\mathtt{w}) + rh \tag{4.8}$$

In fact, for $r = 0$ the claim trivially holds. Assuming the validity for $r \geqslant 0$ then we have that

$$\begin{aligned}
&\max(\llbracket \mathsf{C} + \mathsf{true} \rrbracket^{(r+1)(k_2-k_1)} \eta_{k_1} \mathtt{w}) = \\
&\max(\llbracket \mathsf{C} + \mathsf{true} \rrbracket^{k_2-k_1} (\llbracket \mathsf{C} + \mathsf{true} \rrbracket^{r(k_2-k_1)} \eta_{k_1}) \mathtt{w}) \geqslant \quad \text{by (4.7) as } \eta_{k_1} \sqsubseteq \llbracket \mathsf{C} + \mathsf{true} \rrbracket^{r(k_2-k_1)} \eta_{k_1} \\
&\max(\llbracket \mathsf{C} + \mathsf{true} \rrbracket^{r(k_2-k_1)} \eta_{k_1} \mathtt{w}) + h \geqslant \quad \text{by inductive hypothesis} \\
&\max(\eta_{k_1} \mathtt{w}) + rh + h \geqslant \max(\eta_{k_1} \mathtt{w}) + (r+1)h
\end{aligned}$$

However, this would contradict the hypothesis $\llbracket \mathsf{fix}(\mathsf{C}) \rrbracket \eta \mathtt{y} \neq \infty$. In fact the inequality (4.8) would imply

$$\begin{aligned}
\llbracket \mathsf{fix}(\mathsf{C}) \rrbracket \eta \mathtt{w} &= \bigsqcup_{i \in \mathbb{N}} \llbracket \mathsf{C} + \mathsf{true} \rrbracket^i \eta \mathtt{w} = \\
&= \bigsqcup_{i \in \mathbb{N}} \llbracket \mathsf{C} + \mathsf{true} \rrbracket^i \eta_{k_1} \mathtt{w} \\
&= \bigsqcup_{r \in \mathbb{N}} \llbracket \mathsf{C} + \mathsf{true} \rrbracket^{r(k_2-k_1)} \eta_{k_1} \mathtt{w} \\
&= +\infty
\end{aligned}$$

Now, from (4.5) we deduce that for all $\eta' \sqsupseteq \eta_{k_1}$, for $j \in \{k_1, \ldots, m\}$, if we let $\mu_{k_1} = \eta'$ and $\mu_{j+1} = \llbracket \mathsf{C} + \mathsf{true} \rrbracket \mu_j$, by the choice of the subsequence, since $k_1 \geqslant i$, we have that

$$\max(\mu_{j+1} \mathtt{y}_{j+1}) \geqslant \max(\mu_{j+1} \mathtt{y}_j) + h_j$$

and thus

$$\llbracket \mathsf{C} + \mathsf{true} \rrbracket^{m-k_1+1} \eta' \mathtt{y} = \mu_{m+1} \mathtt{y}_{m+1} \geqslant \max(\mathtt{y}_{k_1}) + \Sigma_{i=k_1}^m h_i = \max(\eta' \mathtt{w}) + \Sigma_{i=k_1}^m h_i$$

Since $\eta' = \llbracket \mathsf{fix}(\mathsf{C}) \rrbracket \eta \sqsupseteq \eta_{k_1}$ we conclude

$$\begin{aligned}
\max\left(\llbracket \mathsf{fix}(\mathsf{C}) \rrbracket \eta \mathtt{y}\right) &= \max\left(\llbracket \mathsf{C} + \mathsf{true} \rrbracket^{m-k_1+1} \llbracket \mathsf{fix}(\mathsf{C}) \rrbracket \eta \mathtt{w}\right) \\
&= \max\left(\llbracket \mathsf{fix}(\mathsf{C}) \rrbracket \eta \mathtt{w}\right) + \Sigma_{i=k_1}{}^m h_i \\
&\geqslant +\infty + \Sigma_{i=k_1}^m h_i = +\infty
\end{aligned}$$

contradicting the assumption.

Therefore, the path σ of (4.5) must exist, and consequently

$$\max(\llbracket \mathsf{fix}(\mathsf{C}) \rrbracket \eta \mathtt{y}) = \max(\eta_{m+1} \mathtt{y}) = \max(\eta \mathtt{y}_0) + \Sigma_{i=0}^m h_i$$

and $\Sigma_{i=0}^m h_i \leqslant (\mathsf{fix}(\mathsf{C}))^{\mathsf{b}} = (n+1)(\mathsf{C})^{\mathsf{b}}$, otherwise we could use the same argument above for inferring the contradiction $\max(\llbracket \mathsf{fix}(\mathsf{C}) \rrbracket \eta \mathtt{y}) = +\infty$.

Let us now show (4.4). Given $\eta' \sqsupseteq \eta$ from (4.5) we deduce that for all $j \in \{0, \ldots, m\}$, if we let $\mu_0 = \eta'$ and $\mu_{j+1} = \llbracket \mathsf{C} + \mathsf{true} \rrbracket \mu_j$, we have that

$$\max(\mu_{j+1} \mathtt{y}_{j+1}) \geqslant \max(\mu_{j+1} \mathtt{y}_j) + h_j.$$

Therefore, since $\llbracket \mathsf{fix}(\mathsf{C}) \rrbracket \eta' \sqsupseteq \mu_{m+1}$ (observe that the convergence of $\llbracket \mathsf{fix}(\mathsf{C}) \rrbracket \eta'$ could be at an index greater than $m+1$), we conclude that:

$$\max(\llbracket \mathsf{fix}(\mathsf{C}) \rrbracket \eta' \mathtt{y}) \geqslant \max(\mu_{m+1} \mathtt{y}) = \max(\mu_{m+1} \mathtt{y}_{m+1}) \geqslant \max(\eta' \mathtt{y}_0) + \Sigma_{i=0}^m h_i$$

as desired.

□

We can now notice that this proof also works for the min value of each variable's interval. I.e., the following property also holds:

Lemma 4.6. *Let* $\mathsf{C} \in \mathsf{Imp}$.
For all $\eta \in \dot{\mathbb{I}}$ *and* $\mathtt{y} \in \mathit{Var}$, *if* $\min([\![\mathsf{C}]\!]\eta\mathtt{y}) \neq -\infty$ *and* $\min([\![\mathsf{C}]\!]\eta\mathtt{y}) < -(\mathsf{C})_{\mathsf{b}}$ *then there exist a variable* $\mathtt{z} \in \mathit{Var}$ *and an integer* $h \in \mathbb{Z}$ *s.t.* $|h| \leqslant (\mathsf{C})_{\mathsf{b}}$ *s.t. the following two properties hold:*

(i) $\min([\![\mathsf{C}]\!]\eta\mathtt{y}) = \min(\eta\mathtt{z}) + h$;

(ii) for all $\eta' \in \dot{\mathbb{I}}$, *if* $\eta' \sqsupseteq \eta$ *then* $\min([\![\mathsf{C}]\!]\eta'\mathtt{y}) \leqslant \min(\eta'\mathtt{z}) + h$.

Proof. The full proof is available at Appendix A.1, as Lemma A.2. Intuitively the proof works by considering the integers $\mathbb{Z}$ with the reverse ordering $<$ and a new bound, $(\mathsf{C})_{\mathsf{b}}$, computed by considering the reverse ordering. □

4.3 Computing interval semantics

Lemma 4.5 provides an effective algorithm for computing the abstract semantics of commands. This means that we can apply Lemma 4.5 on the intervals domain $\dot{\mathbb{I}}$. First, we define the max and min values of the point wise lifting intervals in the following way:

Definition 4.7 (min and max)**.** Given a command C, the corresponding finite set of variables $\mathit{Var}_{\mathsf{C}} \triangleq \mathit{vars}(\mathsf{C})$, and an interval environment $\rho : \mathit{Var}_{\mathsf{C}} \to \mathbb{I}$, we define both the min and the max value of an interval environment:

$$\max(\rho) \triangleq \max\{\ \max\{\max(\rho(\mathtt{x})) \mid \mathtt{x} \in \mathit{Var}_{\mathsf{C}} \wedge \max(\rho(\mathtt{x})) \neq +\infty\}\ ,\ 0\ \}$$
$$\min(\rho) \triangleq \min\{\ \min\{\min(\rho(\mathtt{x})) \mid \mathtt{x} \in \mathit{Var}_{\mathsf{C}} \wedge \min(\rho(\mathtt{x})) \neq -\infty\}\ ,\ 0\ \}$$

Notice that it holds that $\max(\rho) \geqslant 0$ and $\min(\rho) \leqslant 0$. This will later be useful for the base cases of Lemma 4.5 and Lemma 4.17. Now, when computing $[\![\mathsf{C}]\!]\rho$ on such ρ having a finite domain, we can restrict to an interval domain bounded by some constant $k \in \mathbb{N}$:

Definition 4.8 (Bounded interval)**.** We define $\dot{\mathbb{I}}_{k_1}^{k_2} \triangleq (\mathit{Var}_{\mathsf{C}} \to \mathbb{I}_{k_1}^{k_2}) \cup \{\bot\}$ where

$$\begin{aligned}\mathbb{I}_{k_1}^{k_2} \triangleq\ & \{[a,b] \mid a,b \in \mathbb{Z}\ \wedge\ k_1 \leqslant a \leqslant b \leqslant k_2\}\\ & \cup \{[a,+\infty] \mid a \in \mathbb{Z}\ \wedge\ a \geqslant k_1\}\\ & \cup \{[-\infty,b] \mid b \in \mathbb{Z}\ \wedge\ b \leqslant k_2\}\end{aligned}$$

We visualize the Hasse diagram of the bounded integer domain in Figure 4.1 and notice that by definition there are no infinite ascending chains. Now we can notice that given $k_1, k_2 \in \mathbb{Z}$ we can build a Galois Connection (Definition 1.16) between the interval domain $\dot{\mathbb{I}}$ and the bounded interval domain $\dot{\mathbb{I}}_{k_1}^{k_2}$ playing here the role of concrete and abstract domain respectively. To do so we first need to define a concretization and abstraction maps.

Definition 4.9. Given $k_1, k_2 \in \mathbb{Z}$ we define a concretization map $\gamma_{k_1,k_2} : \mathbb{I}_{k_1}^{k_2} \to \mathbb{I}$ as the function

$$\forall a \in \dot{\mathbb{I}}_{k_1}^{k_2} \quad \gamma_{k_1,k_2}(a) = a$$

i.e., $\gamma_{k_1,k_2} = \mathsf{id}$. While we define an abstraction map $\alpha_{k_1,k_2} : \mathbb{I} \to \mathbb{I}_{k_1}^{k_2}$ in the following way

$$\alpha_{k_1,k_2}(\bot) = \bot$$
$$\alpha_{k_1,k_2}([a,b]) = \begin{cases}[a,b] & \text{if } a \geqslant k_1 \wedge b \leqslant k_2\\ [-\infty,b] & \text{if } a < k_1 \wedge b \leqslant k_2\\ [a,+\infty] & \text{if } a \geqslant k_1 \wedge b > k_2\\ [-\infty,+\infty] & \text{otherwise}\end{cases}$$

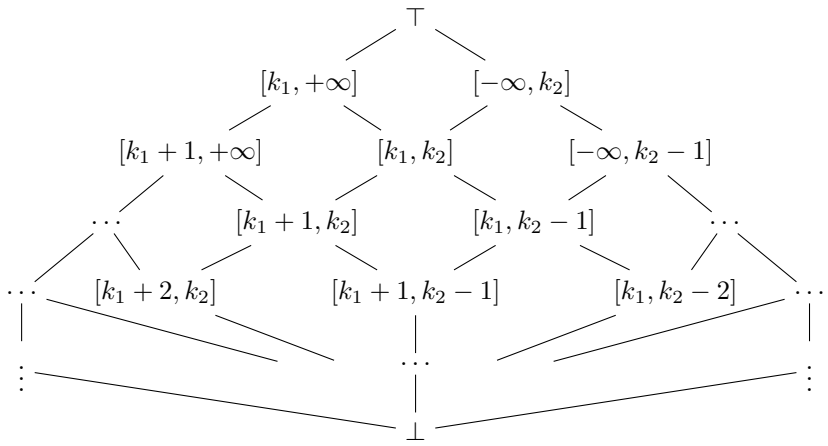


Figure 4.1: $\mathbb{I}_{k_1}^{k_2}$ Hasse diagram

Next, we prove that given $k_1, k_2 \in \mathbb{Z}$ we in fact have a Galois Connection:

Lemma 4.10. *Given $k_1, k_2 \in \mathbb{Z}$ s.t. $k_1 \leqslant k_2$*

$$\langle \mathbb{I}, \sqsubseteq \rangle \underset{\alpha_{k_1,k_2}}{\overset{\mathsf{id}}{\leftrightarrows}} \langle \mathbb{I}_{k_1}^{k_2}, \sqsubseteq \rangle$$

i.e., $\langle \alpha_{k_1,k_2}, \mathbb{I}, \mathbb{I}_{k_1}^{k_2}, \mathsf{id} \rangle$ is a Galois Connection.

Proof. We want to prove that id and α_{k_1,k_2} satisfy the property as in Theorem 1.17:

(1) $\alpha_{k_1,k_2}, \mathsf{id}$ are monotonic;

(2) $\mathsf{id} \circ \alpha_{k_1,k_2}$ is extensive, i.e., $\forall \iota \in \mathbb{I}$ it holds that $\iota \sqsubseteq \mathsf{id}(\alpha_{k_1,k_2}(\iota))$;

(3) $\alpha_{k_1,k_2} \circ \mathsf{id}$ is reductive, i.e., $\forall \iota_b \in \mathbb{I}_{k_1}^{k_2}$ it holds that $\alpha_{k_1,k_2}(\mathsf{id}(\iota_b)) \sqsubseteq \iota_b$.

Let us show (1). The functionid is monotone since $\forall \iota, \kappa \in \mathbb{I}_{k_1}^{k_2}$ it holds that $\iota \sqsubseteq \kappa \implies \iota \sqsubseteq \kappa$. For α_{k_1,k_2} we have to prove that for all $\iota, \kappa \in \mathbb{I}$ it holds that $\iota \sqsubseteq \kappa \implies \alpha_{k_1,k_2}(\iota) \sqsubseteq \alpha_{k_1,k_2}(\kappa)$. Now notice that $\iota \sqsubseteq \kappa$ means that $\min(\iota) \geqslant \min(\kappa)$ and $\max(\iota) \leqslant \max(\kappa)$. Hence, by Definition 4.9 of α_{k_1,k_2} it holds that $\alpha_{k_1,k_2}(\iota) \sqsubseteq \alpha_{k_1,k_2}(\kappa)$, which is our thesis.

Let us now show (2). We have to prove that $\forall \iota \in \mathbb{I}$ it holds that $\iota \sqsubseteq \gamma(\alpha_{k_1,k_2}(\iota))$. By hypothesis $\gamma = \mathsf{id}$, hence we just have to prove that $\iota \sqsubseteq \alpha_{k_1,k_2}(\iota)$. Based on the definition of α_{k_1,k_2} from Definition 4.9 both the following hold:

$$\min(\alpha_{k_1,k_2}(\iota)) \leqslant \min(\iota)$$
$$\max(\alpha_{k_1,k_2}(\iota)) \geqslant \max(\iota)$$

Hence it holds that

$$\iota \sqsubseteq \alpha_{k_1,k_2}(\iota) \tag{4.9}$$

We can finally prove (3): $\alpha_{k_1,k_2} \circ \gamma$ is reductive, i.e., $\forall \iota_b \in \mathbb{I}_{k_1}^{k_2}, \alpha_{k_1,k_2}(\mathsf{id}(\iota_b)) \sqsubseteq \iota_b$. Notice that $\forall \iota_b \in \mathbb{I}_{k_1}^{k_2}$ it holds that

$$\alpha_{k_1,k_2}(\iota_b) = \iota_b \tag{4.10}$$

hence it holds that $\alpha_{k_1,k_2}(\iota_b) \sqsubseteq \iota_b$ □

Notice that because of Equation (4.10) holds we know that $\alpha_{k_1,k_2} \circ \gamma_{k_1,k_2} = \mathsf{id}$, hence we not only have a Galois Connection but a Galois Injection (Definition 1.20):

$$\langle \mathbb{I}, \sqsubseteq \rangle \underset{\alpha_{k_1,k_2}}{\overset{\mathsf{id}}{\leftrightarrows}} \langle \mathbb{I}_{k_1}^{k_2}, \sqsubseteq \rangle \tag{4.11}$$

because of the latter observation and since $\dot{\mathbb{I}}, \dot{\mathbb{I}}_{k_1}^{k_2}$ are the point(variable)-wise lifting of $\mathbb{I}, \mathbb{I}_{k_1}^{k_2}$ respectively, by Theorem 1.22 it holds that

$$\langle \dot{\mathbb{I}}, \sqsubseteq \rangle \underset{\dot{\alpha}_{k_1,k_2}}{\overset{\mathsf{id}}{\leftrightarrows}} \langle \dot{\mathbb{I}}_{k_1}^{k_2}, \sqsubseteq \rangle \tag{4.12}$$

where $\dot{\alpha}_{k_1,k_2}(\eta) = \lambda \mathsf{x}.\alpha_{k_1,k_2}(\eta \mathsf{x})$. We can therefore define our analysis in $\dot{\mathbb{I}}_{k_1}^{k_2}$ by means of best correct approximations over $\dot{\mathbb{I}}_{k_1}^{k_2}$.

Notation 4.11. For the following definition and whenever we will need to talk about the abstract semantics over the interval domain bounded over some constants $k_1, k_2 \in \mathbb{Z}$ we will write $[\![\cdot]\!]_{k_1}^{k_2}$ to refer to $[\![\cdot]\!]_{k_1}^{k_2}$.

Definition 4.12 (Bounded interval analysis)**.** Let $\rho \in \dot{\mathbb{I}}_{k_1}^{k_2}$ for some $k_1, k_2 \in \mathbb{Z}$ s.t. $k_1 \leqslant k_2$ and $\mathsf{C} \in \mathsf{Imp}$. We define $[\![\mathsf{C}]\!]_{k_1}^{k_2}\rho$ as follows

$$\begin{aligned}
[\![\mathsf{e}]\!]_{k_1}^{k_2}\rho &\triangleq \dot{\alpha}_{k_1,k_2}\left([\![\mathsf{e}]\!]\rho\right) \\
[\![\mathsf{C}_1 + \mathsf{C}_2]\!]_{k_1}^{k_2}\rho &\triangleq [\![\mathsf{C}_1]\!]_{k_1}^{k_2}\rho \sqcup [\![\mathsf{C}_2]\!]_{k_1}^{k_2}\rho \\
[\![\mathsf{C}_1; \mathsf{C}_2]\!]_{k_1}^{k_2}\rho &\triangleq \left([\![\mathsf{C}_2]\!]_{k_1}^{k_2} \circ [\![\mathsf{C}_1]\!]_{k_1}^{k_2}\right)\rho \\
[\![\mathsf{C}^*]\!]_{k_1}^{k_2}\rho &\triangleq \bigsqcup_{i\in\mathbb{N}} \left([\![\mathsf{C}]\!]_{k_1}^{k_2}\right)^i \rho \\
[\![\mathsf{fix}(\mathsf{C})]\!]_{k_1}^{k_2}\rho &\triangleq \mathrm{lfp}\left(\lambda\mu.\rho \sqcup [\![\mathsf{C}]\!]_{k_1}^{k_2}\mu\right)
\end{aligned}$$

where $\mathsf{e} \in \mathsf{Exp}$.

Notice that for basic expressions we are using the best correct approximation $\dot{\alpha}_{k_1,k_2} \circ [\![\mathsf{e}]\!] \circ \mathsf{id}$, which allows us to prove the soundness of the analysis over $\dot{\mathbb{I}}_{k_1}^{k_2}$ w.r.t. the analysis over $\dot{\mathbb{I}}$:

Lemma 4.13. *for all $k_1, k_2 \in \mathbb{Z}$ s.t. $k_1 \leqslant k_2$, $\rho \in \dot{\mathbb{I}}_{k_1}^{k_2}$*

$$[\![\mathsf{C}]\!]\rho \sqsubseteq [\![\mathsf{C}]\!]_{k_1}^{k_2}\rho$$

i.e., with $\dot{\mathbb{I}}_{k_1}^{k_2}$ we have an over-approximation of $\dot{\mathbb{I}}$.

Proof. The theorem follows from the fact that there is a Galois connection

$$\dot{\mathbb{I}} \underset{\dot{\alpha}_{k_1,k_2}}{\overset{\mathsf{id}}{\leftrightarrows}} \dot{\mathbb{I}}_{k_1}^{k_2}$$

between $\dot{\mathbb{I}}$ and $\dot{\mathbb{I}}_{k_1}^{k_2}$ for all $k_1, k_2 \in \mathbb{Z} \mid k_1 \leqslant k_2$. Hence by Theorem 3.2 follows that for all $\mathsf{C} \in \mathsf{Imp}, \rho \in \dot{\mathbb{I}}_{k_1}^{k_2}$

$$\left([\![\mathsf{C}]\!] \circ \mathsf{id}\right)\ \rho \sqsubseteq \left(\mathsf{id} \circ [\![\mathsf{C}]\!]_{k_1}^{k_2}\right)\ \rho$$

hence our thesis. □

Now we define a new bound, it will be useful later in Theorem 4.16.

Definition 4.14. Let $\mathsf{C} \in \mathsf{Imp}$. Then $(\cdot)^{\mathsf{b}}_{+} : \mathsf{Imp} \to \mathbb{N}$ is the *updated bound*, recursively defined as follows:

$$\begin{aligned}(\mathsf{e})^{\mathsf{b}}_{+} &\triangleq (\mathsf{e})^{\mathsf{b}} \\ (\mathsf{C}_1 + \mathsf{C}_2)^{\mathsf{b}}_{+} &\triangleq (\mathsf{C}_1)^{\mathsf{b}}_{+} + (\mathsf{C}_2)^{\mathsf{b}}_{+} \\ (\mathsf{C}_1; \mathsf{C}_2)^{\mathsf{b}}_{+} &\triangleq (\mathsf{C}_1)^{\mathsf{b}}_{+} + (\mathsf{C}_2)^{\mathsf{b}}_{+} \\ (\mathsf{fix}(\mathsf{C}))^{\mathsf{b}}_{+} &\triangleq (n+2)(\mathsf{C})^{\mathsf{b}}_{+}\end{aligned}$$

where $n = \mathit{vars}(\mathsf{C})$. Similarly, $(\cdot)^{+}_{\mathsf{b}} : \mathsf{Imp} \to \mathbb{N}$ is the *updated lower bound* of commands, recursively defined as follows:

$$\begin{aligned}(\mathsf{e})^{+}_{\mathsf{b}} &\triangleq (\mathsf{e})_{\mathsf{b}} \\ (\mathsf{C}_1 + \mathsf{C}_2)^{+}_{\mathsf{b}} &\triangleq (\mathsf{C}_1)^{+}_{\mathsf{b}} + (\mathsf{C}_2)^{+}_{\mathsf{b}} \\ (\mathsf{C}_1; \mathsf{C}_2)^{+}_{\mathsf{b}} &\triangleq (\mathsf{C}_1)^{+}_{\mathsf{b}} + (\mathsf{C}_2)^{+}_{\mathsf{b}} \\ (\mathsf{fix}(\mathsf{C}))^{+}_{\mathsf{b}} &\triangleq (n+2)(\mathsf{C})^{+}_{\mathsf{b}}\end{aligned}$$

Notice that the updated bounds differ to bounds of Definition 4.2 only in the case of the $\mathsf{fix}(\mathsf{C})$ command. Thanks to the latter definition, we can now also define the notion of domain bounded by initial state and program.

Definition 4.15. Let $\mathsf{C} \in \mathsf{Imp}$ and $\rho \in \dot{\mathbb{I}}$. Then the *bounded interval domain* $\dot{\mathbb{I}}_{\mathsf{C},\rho}$ is a bounded interval domain $\dot{\mathbb{I}}^{k_2}_{k_1}$ where

$$\begin{aligned}k_1 &= \min(\rho) - (\mathsf{C})^{+}_{\mathsf{b}} \\ k_2 &= \max(\rho) + (\mathsf{C})^{\mathsf{b}}_{+}\end{aligned}$$

With this consideration we can now proceed to prove that the analysis on our bounded lattice $\dot{\mathbb{I}}_{\mathsf{C},\rho}$ produces the same result as the analysis on $\dot{\mathbb{I}}$.

Theorem 4.16. *Let $\mathsf{C} \in \mathsf{Imp}$ be a command. Then, for all finitely supported $\rho : \mathit{Var} \to \mathbb{I}$ and $k_1, k_2 \in \mathbb{Z}$ s.t. $\dot{\mathbb{I}}_{\mathsf{C},\rho} \sqsubseteq \dot{\mathbb{I}}^{k_2}_{k_1}$, i.e., $k_1 \leqslant \min(\rho) - (\mathsf{C})^{+}_{\mathsf{b}}$ and $k_2 \geqslant \max(\rho) + (\mathsf{C})^{\mathsf{b}}_{+}$*

$$[\![\mathsf{C}]\!]\rho = [\![\mathsf{C}]\!]^{k_2}_{k_1}\rho \tag{4.13}$$

i.e., the abstract semantics $[\![\mathsf{C}]\!]\rho$ computed in $\dot{\mathbb{I}}$ and the one computed in $\dot{\mathbb{I}}^{k_2}_{k_1}$ coincide.

Proof. Notice that because of Lemma 4.13 the statement $[\![\mathsf{C}]\!]\rho \sqsubseteq [\![\mathsf{C}]\!]^{k_2}_{k_1}\rho$ already holds. Therefore what we are left to prove is that

$$[\![\mathsf{C}]\!]\rho \sqsupseteq [\![\mathsf{C}]\!]^{k_2}_{k_1}\rho$$

The proof will proceed by induction on the command $\mathsf{C} \in \mathsf{Imp}$.

Case $(\mathtt{x} \in S)$. In this case we want to prove that $[\![\mathtt{x} \in S]\!]\rho \sqsupseteq [\![\mathtt{x} \in S]\!]^{k_2}_{k_1}\rho$. Recall that we are considering $k_1 \leqslant \min(\rho) - (\mathtt{x} \in S)^{+}_{\mathsf{b}} = \min(\rho) - (\mathtt{x} \in S)_{\mathsf{b}}$ and $k_2 \geqslant \max(\rho) + (\mathtt{x} \in S)^{\mathsf{b}}_{+} = \max(\rho) + (\mathtt{x} \in S)^{\mathsf{b}}$. Notice that either $\rho\mathtt{x} \sqcap S = \bot$, which implies that $[\![\mathtt{x} \in S]\!]\rho = \bot$, and therefore $\alpha_{k_1,k_2}([\![\mathtt{x} \in S]\!])\rho = \alpha_{k_1,k_2}(\bot) = \bot$ and therefore $\bot \sqsupseteq \bot$ holds, or $\rho\mathtt{x} \sqcap S = [a, b] \neq \bot$, but in this case $[\![\mathtt{x} \in S]\!]\rho = \rho[\mathtt{x} \mapsto \rho\mathtt{x} \sqcap S]$ and we can observe that both the following hold:

$$\begin{aligned}\min(\rho) - (\mathtt{x} \in S)_{\mathsf{b}} \leqslant \min(\rho) \leqslant \min(\rho\mathtt{x} \sqcap S) \\ \max(\rho\mathtt{x} \sqcap S) \leqslant \max(\rho) \leqslant \max(\rho) + (\mathtt{x} \in S)^{\mathsf{b}}\end{aligned}$$

hence

$$[\![\mathtt{x} \in S]\!]\rho = \rho[\mathtt{x} \mapsto \rho\mathtt{x} \sqcap S] = \dot{\alpha}_{k_1,k_2}([\![\mathtt{x} \in S]\!]\rho) = [\![\mathtt{x} \in S]\!]^{k_2}_{k_1}\rho$$

which is our thesis.

Case $(\mathtt{x} := k)$. In this case we have to prove that $[\![\mathtt{x} := k]\!]\rho \sqsupseteq [\![\mathtt{x} := k]\!]^{k_2}_{k_1}\rho$. Recall that we are considering $k_1 \leqslant \min(\rho) - (\mathtt{x} := k)^+_{\mathsf{b}} = \min(\rho) - (\mathtt{x} := k)_{\mathsf{b}}$ and $k_2 \geqslant \max(\rho) + (\mathtt{x} := k)^{\mathsf{b}}_+$. We can notice similarly to the previous case, that because of the values of k_1 and k_2 it holds that

$$[\![\mathtt{x} := k]\!]\rho = \rho[\mathtt{x} \mapsto [k,k]] = \dot{\alpha}_{k_1,k_2}\left([\![\mathtt{x} := k]\!]\rho\right) = [\![\mathtt{x} := k]\!]^{k_2}_{k_1}\rho$$

hence our thesis holds.

Case $(\mathtt{x} := \mathtt{y} + k)$. In this case we have to prove that $[\![\mathtt{x} := \mathtt{y} + k]\!]\rho \sqsupseteq [\![\mathtt{x} := \mathtt{y} + k]\!]^{k_2}_{k_1}\rho$. Recall that we are considering $k_1 \leqslant \min(\rho) - (\mathtt{x} := \mathtt{y} + k)^+_{\mathsf{b}}$ and $k_2 \geqslant \max(\rho) + (\mathtt{x} := \mathtt{y} + k)^{\mathsf{b}}_+$. Notice also that $(\mathtt{x} := \mathtt{y} + k)^+_{\mathsf{b}} = k = (\mathtt{x} := \mathtt{y} + k)^{\mathsf{b}}_+$ and since $[\![\mathtt{x} := \mathtt{y} + k]\!]\rho = \rho[\mathtt{x} \mapsto \rho\mathtt{y} + k]$ we can notice that for each variable $\mathtt{w} \in \mathit{Var}$ it holds that

$$\min(\rho) - k \leqslant \min\left(\rho[\mathtt{x} \mapsto \rho\mathtt{y} + k]\mathtt{w}\right)$$
$$\max(\rho) + k \geqslant \max\left(\rho[\mathtt{x} \mapsto \rho\mathtt{y} + k]\mathtt{w}\right)$$

hence

$$[\![\mathtt{x} := \mathtt{y} + k]\!]^{k_2}_{k_1}\rho = \dot{\alpha}_{k_1,k_2}\left(\rho[\mathtt{x} \mapsto \rho\mathtt{y} + k]\right) = \rho[\mathtt{x} \mapsto \rho\mathtt{y} + k] = [\![\mathtt{x} := \mathtt{y} + k]\!]\rho$$

which is our thesis

Case $(\mathsf{C}_1 + \mathsf{C}_2)$. In this case we have to prove that $[\![\mathsf{C}_1 + \mathsf{C}_2]\!]\rho \sqsupseteq [\![\mathsf{C}_1 + \mathsf{C}_2]\!]^{k_2}_{k_1}\rho$. Recall that we are considering $k_1 \leqslant \min(\rho) - (\mathsf{C}_1 + \mathsf{C}_2)^+_{\mathsf{b}}$ and $k_2 \geqslant \max(\rho) + (\mathsf{C}_1 + \mathsf{C}_2)^{\mathsf{b}}_+$. By inductive hypothesis it holds that

$$[\![\mathsf{C}_1]\!]\rho = [\![\mathsf{C}_1]\!]^{k_2}_{k_1}\rho$$

for all $k_1 \leqslant \min(\rho) - (\mathsf{C}_1)^+_{\mathsf{b}}$ and $k_2 \geqslant \max(\rho) + (\mathsf{C}_1)^{\mathsf{b}}_+$. Again by inductive hypothesis it holds that

$$[\![\mathsf{C}_2]\!]\rho = [\![\mathsf{C}_2]\!]^{k_2}_{k_1}\rho$$

for all $k_1 \leqslant \min(\rho) - (\mathsf{C}_2)^+_{\mathsf{b}}$ and $k_2 \geqslant \max(\rho) + (\mathsf{C}_2)^{\mathsf{b}}_+$. In particular, both hold for

$$k_1 \leqslant \min(\rho) - (\mathsf{C}_1)^+_{\mathsf{b}} - (\mathsf{C}_2)^+_{\mathsf{b}} = \min(\rho) - (\mathsf{C}_1 + \mathsf{C}_2)^+_{\mathsf{b}}$$
$$k_2 \geqslant \max(\rho) + (\mathsf{C}_1)^{\mathsf{b}}_+ + (\mathsf{C}_2)^{\mathsf{b}}_+ = \max(\rho) + (\mathsf{C}_1 + \mathsf{C}_2)^{\mathsf{b}}_+$$

i.e., our initial choice of k_1, k_2. We can conclude by closure over $\sqcup$

$$[\![\mathsf{C}_1 + \mathsf{C}_2]\!]\rho = [\![\mathsf{C}_1]\!]\rho \sqcup [\![\mathsf{C}_2]\!]\rho = [\![\mathsf{C}_1]\!]^{k_2}_{k_1}\rho \sqcup [\![\mathsf{C}_2]\!]^{k_2}_{k_1}\rho = [\![\mathsf{C}_1 + \mathsf{C}_2]\!]^{k_2}_{k_1}\rho$$

which is our thesis.

Case $(\mathsf{C}_1; \mathsf{C}_2)$. In this case we have to prove that $[\![\mathsf{C}_1; \mathsf{C}_2]\!]\rho \sqsupseteq [\![\mathsf{C}_1; \mathsf{C}_2]\!]^{k_2}_{k_1}\rho$ for all $k_1 \leqslant \min(\rho) - (\mathsf{C}_1; \mathsf{C}_2)^+_{\mathsf{b}}$ and $k_2 \geqslant \max(\mathsf{C}) + (\mathsf{C}_1; \mathsf{C}_2)^{\mathsf{b}}_+$. Recall that $[\![\mathsf{C}_1; \mathsf{C}_2]\!]\rho = ([\![\mathsf{C}_2]\!] \circ [\![\mathsf{C}_1]\!])\rho$. By inductive hypothesis it holds that

$$[\![\mathsf{C}_1]\!]\rho = [\![\mathsf{C}_1]\!]^{k_2}_{k_1}\rho \qquad \forall k_1 \leqslant \min(\rho) - (\mathsf{C}_1)^+_{\mathsf{b}} \ \wedge \ k_2 \geqslant \max(\rho) + (\mathsf{C}_1)^{\mathsf{b}}_+ \tag{4.14}$$
$$[\![\mathsf{C}_2]\!]\rho' = [\![\mathsf{C}_2]\!]^{k_4}_{k_3}\rho' \qquad \forall k_3 \leqslant \min(\rho') - (\mathsf{C}_2)^+_{\mathsf{b}} \ \wedge \ k_4 \geqslant \max(\rho') + (\mathsf{C}_2)^{\mathsf{b}}_+ \tag{4.15}$$

where $\rho' = [\![\mathsf{C}_1]\!]\rho$. In particular notice that both (4.14) and (4.15) hold for all n, m s.t.

$$m \leqslant \min(\rho) - (\mathsf{C}_1)^+_{\mathsf{b}} - (\mathsf{C}_2)^+_{\mathsf{b}}$$
$$n \geqslant \max(\rho) + (\mathsf{C}_1)^{\mathsf{b}}_+ + (\mathsf{C}_2)^{\mathsf{b}}_+$$

Hence

$$[\![\mathsf{C}_1; \mathsf{C}_2]\!]\rho = \left([\![\mathsf{C}_2]\!] \circ [\![\mathsf{C}_1]\!]\right)\rho = \left([\![\mathsf{C}_2]\!]^n_m \circ [\![\mathsf{C}_1]\!]^n_m\right)\rho = [\![\mathsf{C}_1; \mathsf{C}_2]\!]^n_m\rho$$

which is our thesis.

Case ($\mathsf{fix}(\mathsf{C})$). What we want to prove in this case is that $[\![\mathsf{fix}(\mathsf{C})]\!]\rho \sqsupseteq [\![\mathsf{fix}(\mathsf{C})]\!]_{k_1}^{k_2}\rho$ for all $k_1 \leqslant \min(\rho) - (\mathsf{fix}(\mathsf{C}))_{\mathsf{b}}^{+}$ and $k_2 \geqslant \max(\rho) + (\mathsf{fix}(\mathsf{C}))_{+}^{\mathsf{b}}$. Recall that by Lemma 3.4 $[\![\mathsf{fix}(\mathsf{C})]\!]$ is syntactic sugar for $[\![(\mathsf{C} + \mathsf{true})^*]\!]$, therefore

$$[\![\mathsf{fix}(\mathsf{C})]\!]\rho = [\![(\mathsf{C} + \mathsf{true})^*]\!]\rho = \bigsqcup_{i\in\mathbb{N}} ([\![\mathsf{C} + \mathsf{true}]\!])^i\rho \tag{4.16}$$

$$[\![\mathsf{fix}(\mathsf{C})]\!]_{k_1}^{k_2}\rho = [\![(\mathsf{C} + \mathsf{true})^*]\!]_{k_1}^{k_2}\rho = \bigsqcup_{i\in\mathbb{N}} \left([\![\mathsf{C} + \mathsf{true}]\!]_{k_1}^{k_2}\right)^i\rho \tag{4.17}$$

By latter equation we want to prove that for every $i \in \mathbb{N}$ it holds that

$$[\![\mathsf{fix}(\mathsf{C})]\!]\rho \sqsupseteq \left([\![\mathsf{C} + \mathsf{true}]\!]_{k_1}^{k_2}\right)^i\rho \tag{4.18}$$

Case ($i = 0$). In this case we can observe that our thesis

$$[\![\mathsf{fix}(\mathsf{C})]\!]\rho \sqsupseteq \left([\![\mathsf{fix}(\mathsf{C})]\!]_{k_1}^{k_2}\right)^0\rho = \mathsf{id}(\rho) = \rho$$

holds by (4.16).

Case ($i \implies i+1$). In this case we can first notice that

$$\begin{aligned}[\![\mathsf{C} + \mathsf{true}]\!]([\![\mathsf{fix}(\mathsf{C})]\!]\rho) &= [\![\mathsf{C}]\!]([\![\mathsf{fix}(\mathsf{C})]\!]\rho) \sqcup ([\![\mathsf{fix}(\mathsf{C})]\!]\rho) && \text{by definition of } \mathsf{C} + \mathsf{true}\\ &= [\![\mathsf{C}]\!](\mathrm{lfp}(\lambda\mu.\rho \sqcup [\![\mathsf{C}]\!]\mu)) \sqcup ([\![\mathsf{fix}(\mathsf{C})]\!]\rho) && (4.19)\end{aligned}$$

by definition of $\lambda\mu.\rho \sqcup [\![\mathsf{C}]\!]\mu$ it holds that $\mathrm{lfp}\,(\lambda\mu.\rho \sqcup [\![\mathsf{C}]\!]\mu) \sqsupseteq \rho$, hence

$$\begin{aligned}[\![\mathsf{C}]\!](\mathrm{lfp}(\lambda\mu.\rho \sqcup [\![\mathsf{C}]\!]\mu)) &= \rho \sqcup [\![\mathsf{C}]\!](\mathrm{lfp}(\lambda\mu.\rho \sqcup [\![\mathsf{C}]\!]\mu))\\ &= \mathrm{lfp}(\lambda\mu.\rho \sqcup [\![\mathsf{C}]\!]\mu)\\ &= [\![\mathsf{fix}(\mathsf{C})]\!]\rho && (4.20)\end{aligned}$$

therefore in (4.19)

$$\begin{aligned}[\![\mathsf{C}]\!](\mathrm{lfp}(\lambda\mu.\rho \sqcup [\![\mathsf{C}]\!]\mu)) \sqcup ([\![\mathsf{fix}(\mathsf{C})]\!]\rho) &= [\![\mathsf{fix}(\mathsf{C})]\!]\rho \sqcup [\![\mathsf{fix}(\mathsf{C})]\!]\rho && \text{by (4.20)}\\ &= [\![\mathsf{fix}(\mathsf{C})]\!]\rho.\end{aligned}$$

We can now continue. By calling $[\![\mathsf{fix}(\mathsf{C})]\!]\rho = \beta$ we have to prove that

$$[\![\mathsf{C} + \mathsf{true}]\!]\beta \sqsupseteq [\![\mathsf{C} + \mathsf{true}]\!]_{k_1}^{k_2}\beta. \tag{4.21}$$

for all $k_1 \leqslant \min(\rho) - (\mathsf{fix}(\mathsf{C}))_{\mathsf{b}}^{+}$ and $k_2 \geqslant \max(\rho) + (\mathsf{fix}(\mathsf{C}))_{+}^{\mathsf{b}}$. In other words what we want to prove is that for every $\mathsf{y} \in \mathit{Var}_{\mathsf{C}}$ both

$$\begin{aligned}\max([\![\mathsf{C} + \mathsf{true}]\!]\beta\mathsf{y}) &\leqslant k_2\\ \min([\![\mathsf{C} + \mathsf{true}]\!]\beta\mathsf{y}) &\geqslant k_1\end{aligned}$$

To start notice that $\max(\beta\mathsf{y}) \leqslant \max(\rho) + (\mathsf{fix}(\mathsf{C}))^{\mathsf{b}}$ by Lemma 4.5. Hence by Definition 4.7 $\max(\beta) \leqslant \max(\rho) + (\mathsf{fix}(\mathsf{C}))^{\mathsf{b}}$, and by calling $n = \mathit{vars}(\mathsf{C})$ we can notice the following:

$$\begin{aligned}\max([\![\mathsf{C} + \mathsf{true}]\!]\beta) &\leqslant \max(\beta) + (\mathsf{C})^{\mathsf{b}} && \text{by Lemma 4.5}\\ &\leqslant \max(\rho) + (\mathsf{fix}(\mathsf{C}))^{\mathsf{b}} + (\mathsf{C})^{\mathsf{b}}\\ &= \max(\rho) + (n+2)(\mathsf{C})^{\mathsf{b}}\\ &\leqslant \max(\rho) + (n+2)(\mathsf{C})_{+}^{\mathsf{b}}\\ &= \max(\rho) + (\mathsf{fix}(\mathsf{C}))_{+}^{\mathsf{b}} = k_2\end{aligned}$$

A similar procedure can be applied on the minimum to observe that

$$\min(\llbracket \mathsf{C} + \mathsf{true} \rrbracket \beta) \geqslant \min(\rho) - (\mathsf{C})^{+}_{\mathsf{b}} = k_1$$

Hence we can conclude by observing that

$$\begin{aligned} \beta = \llbracket \mathsf{C} + \mathsf{true} \rrbracket \beta &\sqsupseteq \llbracket \mathsf{C} + \mathsf{true} \rrbracket^{k_2}_{k_1} \beta && \text{by (4.21)} \\ &\sqsupseteq \llbracket \mathsf{C} + \mathsf{true} \rrbracket^{k_2}_{k_1} \left(\llbracket \mathsf{C} + \mathsf{true} \rrbracket^{k_2}_{k_1} \right)^{i} \rho && \text{by induction on } i \\ &= \left(\llbracket \mathsf{C} + \mathsf{true} \rrbracket^{k_2}_{k_1} \right)^{i+1} \rho \end{aligned}$$

Therefore for all $i \in \mathbb{N}$ $\llbracket \mathsf{fix}(\mathsf{C}) \rrbracket \rho \sqsupseteq \left(\llbracket \mathsf{C} + \mathsf{true} \rrbracket^{k_2}_{k_1} \right)^{i} \rho$. By this we can deduce that

$$\beta = \llbracket \mathsf{fix}(\mathsf{C}) \rrbracket \rho \sqsupseteq \bigsqcup_{i \in \mathbb{N}} \left(\llbracket \mathsf{C} + \mathsf{true} \rrbracket^{k_2}_{k_1} \right)^{i} \rho = \llbracket \mathsf{fix}(\mathsf{C}) \rrbracket^{k_2}_{k_1} \rho$$

which is our thesis.

□

Our last theorem proved that by bounding the interval domain according to the constants that appear in a program and its initial state we can ensure termination of the analysis while achieving the most precise abstract invariant for the program. The result is analogous to the findings of [Gaw+09], but is achieved by only looking at the maximal and minimal values of the intermediate elements of the analysis. This can already be seen as an hint on the goal of next sections: while we reasoned on the values of the intermediate analysis, we did not reason about the *internal* values of intervals. In other words if instead of intervals we considered arbitrary sets (i.e., possibly *non-convex* sets) our results should still be valid.

4.4 Bounded non-relational collecting semantics

In the following section we prove we will see that even though we are not able to compute the most precise invariant for any program in Imp we can however infer a sound invariant that gives us insights about the termination of the non-relational collecting analysis.

For an easier reading, we will refer to $\llbracket \cdot \rrbracket^{\mathbb{C}}$ with the same notation we used in Section 3.3.2: $\langle\!\langle \cdot \rangle\!\rangle = \llbracket \cdot \rrbracket^{\mathbb{C}}$.

Lemma 4.17. *Let* $\mathsf{C} \in \mathsf{Imp}$. *For all* $\eta \in \mathbb{C}$ *and* $\mathsf{y} \in \mathit{Var}$, *if* $\max(\langle\!\langle \mathsf{C} \rangle\!\rangle \eta \mathsf{y}) \neq +\infty$ *and* $\max(\langle\!\langle \mathsf{C} \rangle\!\rangle \eta \mathsf{y}) > (\mathsf{C})^{\mathsf{b}}$ *then there exist a variable* $\mathsf{z} \in \mathit{Var}$ *and an integer* $h \in \mathbb{Z}$ *such that* $|h| \leqslant (\mathsf{C})^{\mathsf{b}}$ *and the following two properties hold:*

(i) $\max(\langle\!\langle \mathsf{C} \rangle\!\rangle \eta \mathsf{y}) = \max(\eta \mathsf{z}) + h$;

(ii) for all $\eta' \in \mathbb{C}$, *if* $\eta' \dot{\supseteq} \eta$ *then* $\max(\langle\!\langle \mathsf{C} \rangle\!\rangle \eta' \mathsf{y}) \geqslant \max(\eta' \mathsf{z}) + h$.

Proof. The proof is left in Appendix A.2, since it is analogous to the proof of Lemma 4.5. □

Remark 4.18. The key point is that in the base case ($\mathsf{x} \in I$) we can say the same things we said for intervals. This is because the filtering happens on an interval $I \in \mathbb{I}$ instead on an arbitrary decidable set $S \in \wp(\mathbb{Z})$. If that was the case and we consider $\mathsf{y} = \mathsf{x}$ it happens that

remark sul fatto che funz
chè abbiamo limitato il l

$$\max(\langle\!\langle \mathsf{x} \in S \rangle\!\rangle \eta \mathsf{y}) = \max(\eta[\mathsf{x} \mapsto \eta \mathsf{x} \cap S]\mathsf{x}) = \max(\eta \mathsf{x} \cap S) \tag{4.22}$$

but since S is generally concave what happens is that generally if $\eta \mathsf{x} \cap S \neq \varnothing$ and $\max(S) = +\infty$ then

$$\max(\eta \mathsf{x} \cap S) \leqslant \max(\eta \mathsf{x}) \tag{4.23}$$

providing a potential counterexample to the Lemma. For example consider the program $(\mathtt{x} \in \mathbb{P})$ where $\mathbb{P}$ is the set of even numbers and initial environment $\eta \triangleq [\mathtt{x} \mapsto \mathbb{D} \cup \{2\}]$, where $\mathbb{D}$ is the set of odd numbers. Then

$$\langle\!\langle \mathtt{x} \in \mathbb{P} \rangle\!\rangle \eta \mathtt{x} = \{2\}$$

and $\max(\langle\!\langle \mathtt{x} \in \mathbb{P} \rangle\!\rangle \eta \mathtt{x}) = 2$, while $(\langle\!\langle \mathtt{x} \in \mathbb{P} \rangle\!\rangle \eta \mathtt{x})^{\mathsf{b}} = 0$.

Hence both $\max(\langle\!\langle \mathtt{x} \in \mathbb{P} \rangle\!\rangle \eta \mathtt{x}) \neq +\infty$ and $\max(\langle\!\langle \mathtt{x} \in \mathbb{P} \rangle\!\rangle \eta \mathtt{x}) > (\langle\!\langle \mathtt{x} \in \mathbb{P} \rangle\!\rangle \eta \mathtt{x})^{\mathsf{b}}$ hold and what the Lemma would state is that $\exists \mathtt{w} \in (\mathtt{x} \in \mathbb{P})$ and $h \in \mathbb{Z} \mid |h| \leqslant (\mathtt{x} \in \mathbb{P})^{\mathsf{b}}$ s.t.

(i) $\max(\langle\!\langle \mathtt{x} \in \mathbb{P} \rangle\!\rangle \eta \mathtt{x}) = \max(\eta \mathtt{w}) + h$

(ii) $\forall \eta' \sqsupseteq \eta \quad \max(\langle\!\langle \mathtt{x} \in \mathbb{P} \rangle\!\rangle \eta' \mathtt{y}) \geqslant \max(\eta' \mathtt{w}) + h$

and we can already see that (i) is false. In fact the only variable in the program is $\mathtt{x}$, hence $\mathtt{w} = \mathtt{x}$, but $\max(\eta \mathtt{x}) = +\infty$ and $\forall h \in \mathbb{Z}$ it happens that $+\infty + h = +\infty$, hence

$$\max(\langle\!\langle \mathtt{x} \in \mathbb{P} \rangle\!\rangle \eta \mathtt{x}) = 2 = +\infty = \max(\eta \mathtt{x}) + h$$

which is false.

The same applies for the increment on the lower bound, in a similar fashion as for the intervals:

Lemma 4.19. *Let* $\mathsf{C} \in \mathsf{Imp}$. *For all* $\eta \in \mathbb{C}$ *and* $\mathtt{y} \in \mathit{Var}$, *if* $\min(\langle\!\langle \mathsf{C} \rangle\!\rangle \eta \mathtt{y}) \neq -\infty$ *and* $\min(\langle\!\langle \mathsf{C} \rangle\!\rangle \eta \mathtt{y}) < -(\mathsf{C})^{\mathsf{b}}$ *then there exist a variable* $\mathtt{z} \in \mathit{Var}$ *and an integer* $h \in \mathbb{Z}$ *such that* $|h| \leqslant (\mathsf{C})^{\mathsf{b}}$ *and the following two properties hold:*

(i) $\min(\langle\!\langle \mathsf{C} \rangle\!\rangle \eta \mathtt{y}) = \min(\eta \mathtt{z}) + h$;

(ii) for all $\eta' \in \mathbb{C}$, *if* $\eta' \dot{\supseteq} \eta$ *then* $\min(\langle\!\langle \mathsf{C} \rangle\!\rangle \eta' \mathtt{y}) \leqslant \min(\eta' \mathtt{z}) + h$.

4.5 Computing non-relational collecting semantics

In the following section we follow the same scheme used in Section 4.2 in order to prove that we can also bound the non relational collecting domain to ensure convergence while obtaining the most precise interval. To start, we rely on Definition 4.7 of min and max values of an abstract environment ρ to bound the non relational collecting domain $\mathbb{C}$ in this way:

Definition 4.20 (Bounded non-relational collecting domain)**.** We define $\mathbb{C}_{k_1}^{k_2} \triangleq \mathit{Var}_{\mathsf{C}} \to \wp^*(\mathbb{Z})_{k_1}^{k_2}$ where

$$\wp^*(\mathbb{Z})_{k_1}^{k_2} = \{S \subseteq \mathbb{Z} \mid S \neq \varnothing \wedge \forall x \in S \quad k_1 \leqslant x \leqslant k_2\} \cup \{\top\}$$

Notice that contrary to $\dot{\mathbb{I}}_{k_1}^{k_2}$ we have no way of representing a diverging element. For bounded intervals we had the $[a, +\infty]$ and $[-\infty, b]$ elements with $a, b \in \mathbb{Z}$, but for arbitrary subsets of z we have to rely on a smashed $\top$ element.

We can already observe that by definition there are no infinite ascending nor descending chains, as every chain is bounded by above by some $k_2 \in \mathbb{Z}$ and below by some $k_1 \in \mathbb{Z}$. Moreover, there is a Galois connection between this abstract domain and its unbounded counterpart $\wp(\mathbb{Z})$. First let's define the concretization and abstraction maps

Definition 4.21. Let $k_1, k_2 \in \mathbb{Z}$ s.t. $k_1 \leqslant k_2$. We define a concretization map $\gamma_{k_1,k_2} : \wp^*(\mathbb{Z})_{k_1}^{k_2} \to \wp^*(\mathbb{Z})$ as the identity function

$$\gamma_{k_1,k_2} = \mathsf{id}$$

similarly we define an abstraction map $\alpha_{k_1,k_2} : \wp^*(\mathbb{Z}) \to \wp^*(\mathbb{Z})_{k_1}^{k_2}$ in the following way

$$\alpha_{k_1,k_2}(S) = \begin{cases} S & \text{if } \inf(S) \geqslant k_1 \wedge \sup(S) \leqslant k_2 \\ \top & \text{otherwise} \end{cases}$$

Lemma 4.22. *Given $k_1, k_2 \in \mathbb{Z}$ s.t. $k_1 \leqslant k_2$.*

$$\langle \wp^*(\mathbb{Z}), \subseteq \rangle \underset{\alpha_{k_1,k_2}}{\overset{\mathsf{id}}{\leftrightarrows}} \langle \wp^*(\mathbb{Z})^{k_2}_{k_1}, \subseteq \rangle$$

i.e., $\langle \alpha_{k_1,k_2}, \wp^*(\mathbb{Z}), \wp^*(\mathbb{Z})^{k_2}_{k_1}, \mathsf{id} \rangle$ is a Galois connection.

Proof. The proof consists in showing that γ_{k_1,k_2} and α_{k_1,k_2} satisfy the properties of Theorem 1.18:

(1) α_{k_1,k_2}, id are monotonic;

(2) $\mathsf{id} \circ \alpha_{k_1,k_2}$ is extensive, i.e., $\sigma \subseteq \alpha_{k_1,k_2}(\sigma)$ for all $\sigma \in \wp^*(\mathbb{Z})$;

(3) $\alpha_{k_1,k_2} \circ \gamma$ is reductive, i.e., $\alpha_{k_1,k_2}(\sigma_b) \subseteq \sigma_b$ for all $\sigma_b \in \wp^*(\mathbb{Z})^{k_2}_{k_1}$.

To start let's prove (1). Of course id is monotone by definition. For α_{k_1,k_2} we have to prove that given any $\sigma, \tau \in \wp^*(\mathbb{Z})$ s.t. $\sigma \subseteq \tau$ it holds that $\alpha_{k_1,k_2}(\sigma) \subseteq \alpha_{k_1,k_2}(\tau)$. Notice that since $\sigma \subseteq \tau$ it holds that $\max(\sigma) \leqslant \max(\tau)$ and $\min(\sigma) \geqslant \min(\tau)$, which means by Definition 4.21 $\alpha_{k_1,k_2}\sigma \subseteq \alpha_{k_1,k_2}\tau$, which is our thesis.

Both (2) and (3) follow from Definition 4.21. For (2) for all $\sigma \in \wp^*(\mathbb{Z})$ either $\alpha_{k_1,k_2}(\sigma) = \sigma$ or $\alpha_{k_1,k_2}(\sigma) = \top$, hence in both cases $\sigma \subseteq \alpha_{k_1,k_2}(\sigma)$ holds. For (3), for all $\sigma_b \in \wp^*(\mathbb{Z})^{k_2}_{k_1}$ it holds that $\max(\sigma_b) \leqslant k_2$ and $\min(\sigma_b) \geqslant k_1$, hence

$$\alpha_{k_1,k_2}(\sigma_b) = \sigma_b \tag{4.24}$$

and therefore $\alpha_{k_1,k_2}(\sigma_b) \subseteq \sigma_b$ holds. Moreover, (4.24) means that for all $\sigma_b \in \wp^*(\mathbb{Z})^{k_2}_{k_1}$ that $\alpha_{k_1,k_2} \circ \mathsf{id} = \mathsf{id}$, which means by Definition 1.20 that we formed a Galois insertion:

$$\langle \wp^*(\mathbb{Z}), \subseteq \rangle \underset{\alpha_{k_1,k_2}}{\overset{\mathsf{id}}{\leftrightarrows}} \langle \wp^*(\mathbb{Z})^{k_2}_{k_1}, \subseteq \rangle$$

□

Notice that since $\mathbb{C}$ and $\mathbb{C}^{k_2}_{k_1}$ are respectively the point-wise lifting of $\wp^*(\mathbb{Z})$ and $\wp^*(\mathbb{Z})^{k_2}_{k_1}$ there is also a Galois insertion between them:

$$\langle \mathbb{C}, \dot{\subseteq} \rangle \underset{\dot{\alpha}_{k_1,k_2}}{\overset{\mathsf{id}}{\leftrightarrows}} \langle \mathbb{C}^{k_2}_{k_1}, \dot{\subseteq} \rangle$$

Where $\dot{\alpha}_{k_1,k_2}(\eta) = \lambda \mathtt{x}.\alpha_{k_1,k_2}(\eta \mathtt{x})$. Since we have a Galois connection between the non relational collecting domain $\mathbb{C}$ and its bounded version $\mathbb{C}^{k_2}_{k_1}$ we can define an abstract inductive semantics which is sound by construction:

Definition 4.23 (Abstract bounded non relational collecting semantics). Let $k_1, k_2 \in \mathbb{Z}$ s.t. $k_1 \leqslant k_2$. We define basic expressions over the bounded non relational collecting semantics $(\!(\cdot)\!)^{\mathbb{C}^{k_2}_{k_1}} : \mathsf{Exp} \to \mathbb{C}^{k_2}_{k_1} \to \mathbb{C}^{k_2}_{k_1}$ as

$$(\!(\mathsf{e})\!)^{\mathbb{C}^{k_2}_{k_1}} \triangleq \dot{\alpha}_{k_1,k_2} \circ (\!(\mathsf{e})\!)^{\mathbb{C}}$$

i.e. the best correct abstraction.

Lemma 4.24 (Bounded non relational collecting is sound). *Let $k_1, k_2 \in \mathbb{Z}$ s.t. $k_1 \leqslant k_2$. For all $\eta^\sharp \in \mathbb{C}^{k_2}_{k_1}$ it holds that*

$$(\langle\!\langle \mathsf{C} \rangle\!\rangle \circ \mathsf{id})\, \eta^\sharp \mathrel{\dot{\subseteq}} \left(\mathsf{id} \circ \langle\!\langle \mathsf{C} \rangle\!\rangle^{k_2}_{k_1}\right) \eta^\sharp$$

i.e., $\langle\!\langle \cdot \rangle\!\rangle^{k_2}_{k_1}$ is sound w.r.t. $\langle\!\langle \cdot \rangle\!\rangle$.

Proof. The proof follows from the fact that $\langle\!\langle \cdot \rangle\!\rangle^{k_2}_{k_1}$ is defined as the bca on basic expressions over $\mathbb{C}$ and there is a Galois connection

$$\langle \mathbb{C}, \dot{\subseteq} \rangle \underset{\dot{\alpha}_{k_1,k_2}}{\overset{\mathsf{id}}{\leftrightarrows}} \langle \mathbb{C}^{k_2}_{k_1}, \dot{\subseteq} \rangle$$

Hence by Lemma 3.3 our thesis

$$(\langle\!\langle \mathsf{C} \rangle\!\rangle \circ \mathsf{id})\, \eta^\sharp \mathrel{\dot{\subseteq}} \left(\mathsf{id} \circ \langle\!\langle \mathsf{C} \rangle\!\rangle^{k_2}_{k_1}\right) \eta^\sharp$$

holds. □

By using k_1, k_2 properly, we can introduce a notion of order between bounded non relational collecting domain. More in detail, given $a, b, c, d \in \mathbb{Z}$ s.t. $a \leqslant b$ and $c \leqslant d$. Then $\preccurlyeq$ is a relation order s.t.

$$\mathbb{C}_a^b \preccurlyeq \mathbb{C}_c^d \iff a \leqslant c \wedge d \leqslant b$$

We bounded our analysis the same way we did with interval analysis in Definition 4.8. This initial solution however has a problem. Consider the following code snippet:

```
1  x := 0
2  y := 0
3  while (x < 1)
4    x := x + 1
5    y := y + 2
6  if (y = 1)
7    x := 2
```

Code 4.2: Snippet where bounded analysis diverges from the unbounded counterpart

before entering the `while` loop variables are bounded to singleton sets $\mathtt{x} \mapsto \{0\}, \mathtt{y} \mapsto \{0\}$. Non-relational collecting semantics can infer for $\mathtt{x}$ the set $\mathtt{x} \mapsto \{0, 1\}$, since the condition to enter the loop filters for $\mathtt{x} \mapsto \{0\}$. For $\mathtt{y}$ however the guard does not filter anything (since the condition is on $\mathtt{x}$ and the domain is non-relational). Hence after the loop non-relational collecting analysis infers the set of even numbers $\mathbb{P}$: $\mathtt{y} \mapsto \mathbb{P}$. Since the set is infinite at some point it will surely exceed the program bound, which is a number in $\mathbb{N}$. Hence the bounded analysis, after the loop can infer $\mathtt{x} \mapsto \{0, 1\}, \mathtt{y} \mapsto \top$. The last `if` is however where the two analysis diverge (while remaining sound): the original non-relational collecting before the `if` infers $[\mathtt{x} \mapsto \{0, 1\}, \mathtt{y} \mapsto \mathbb{P}]$, hence the filter $\mathtt{y} = 1$ filters $\bot$ and therefore after the `if` the invariant remains $[\mathtt{x} \mapsto \{0, 1\}, \mathtt{y} \mapsto \mathbb{P}]$. The bounded analysis however filters $[\mathtt{x} \mapsto \{0, 1\}, \mathtt{y} \mapsto \{1\}]$ and threfore after the `if` the inferred invariant is $[\mathtt{x} \mapsto \{0, 1, 2\}, \mathtt{y} \mapsto \top]$, hence diverging. The idea is that by being non-relational and smashing all infinite elements of $\wp(\mathbb{Z})$ to $\top$ the loss of information does not allow to infer the correct invariant even for variables with finite mappings.

Our guess is that it is possible to infer the precise infinite invariant, since all the information used to generate it are syntattically available: previous work on such matter is from James Worrell in [Lef+24], which however deals with Presburger arithmetics (which are outside of scope in this thesis).

For this reason our approach consists in smashing the $\top$ element of our analysis. Remember that the original problem we want to solve (roughly) is the non-termination of the anlaysis,

che accade quando l'analisi di una variabile diverge all'interno di un loop usando le iterazioni di kleene.

Definition 4.25 (Smashed $\top$ non realtional collecting)**.** Let

$$\wp(\mathbb{Z})_{k_1}^{k_2} \triangleq \{S \subseteq \mathbb{Z} \mid S \neq \varnothing \wedge \forall x \in S \quad k_1 \leqslant x \leqslant k_2\}.$$

We define $\overline{\mathbb{C}}_{k_1}^{k_2}$ as

$$\overline{\mathbb{C}}_{k_1}^{k_2} \triangleq (\mathit{Var} \to \wp(\mathbb{Z})_{k_1}^{k_2}) \cup \{\bot, \top\}$$

we can build a Galois connection with $\mathbb{C}_{k_1}^{k_2}$ for some fixed $k_1, k_2 \in \mathbb{Z}$:

Definition 4.26. Let $k_1, k_2 \in \mathbb{Z}$ s.t. $k_1 \leqslant k_2$, $\eta \in \mathbb{C}_{k_1}^{k_2}$ and $\overline{\eta} \in \overline{\mathbb{C}}_{k_1}^{k_2}$. Then the abstraction map $\overline{\alpha}_{k_1,k_2} : \mathbb{C}_{k_1}^{k_2} \to \overline{\mathbb{C}}_{k_1}^{k_2}$ is defined as

$$\overline{\alpha}_{k_1,k_2}(\eta) = \begin{cases} \top & \text{if } \exists \mathtt{x} \in \mathit{Var} \text{ s.t. } \eta\mathtt{x} = \top \\ \eta & \text{otherwise} \end{cases}$$

while concretization map $\overline{\gamma}_{k_1,k_2} : \overline{\mathbb{C}}_{k_1}^{k_2} \to \mathbb{C}_{k_1}^{k_2}$ is defined as

$$\overline{\gamma}_{k_1,k_2}(\top) = \lambda \mathtt{x} \in \mathit{Var}.\top$$
$$\overline{\gamma}_{k_1,k_2}(\overline{\eta}) = \overline{\eta}$$

We can now define base expressions based on the bca with the bounded non relational collecting semantics:

Definition 4.27. Let $\mathsf{e} \in \mathsf{Exp}$. The semantics of base expressions over $\overline{\mathbb{C}}^{k_2}_{k_1}$ is defined as

$$(\!(\mathsf{e})\!)^{\overline{\mathbb{C}}^{k_2}_{k_1}} \triangleq \overline{\alpha}_{k_1,k_2} \circ (\!(\mathsf{e})\!)^{\mathbb{C}^{k_2}_{k_1}}$$

i.e., the bca on the semantics of base expressions on bounded non-relational collecting analysis.

Once again, $[\![\cdot]\!]^{\overline{\mathbb{C}}^{k_2}_{k_1}}$ is defined accordingly to the abstract inductive semantics of Definition 3.1. Notice that contrary to latter definition of $\mathbb{C}^{k_2}_{k_1}$ in this case we have a smashed top element. The idea is that whenever a variable diverges we infer that the whole precise analysis diverges, in order to solve Problem 4.1 and decide analysis termination. For simplicity, from now on we will refer to $[\![\cdot]\!]^{\overline{\mathbb{C}}^{k_2}_{k_1}}$ as $\overline{\langle\!\langle \cdot \rangle\!\rangle}^{k_2}_{k_1}$.

We preliminarly prove a simple but useful property of $\overline{\langle\!\langle \cdot \rangle\!\rangle}^{k_2}_{k_1}$: it preserves the $\top$ element.

Lemma 4.28 ($\overline{\langle\!\langle \cdot \rangle\!\rangle}^{k_2}_{k_1}$ preserves $\top$)**.** *Let $k_1, k_2 \in \mathbb{Z}$ s.t. $k_1 \leqslant k_2$ and $\mathsf{C} \in \mathsf{Imp}$*

$$\overline{\langle\!\langle \mathsf{C} \rangle\!\rangle}^{k_2}_{k_1} \top = \top$$

Proof. We proceed by induction on the program C to prove that

$$\overline{\langle\!\langle \mathsf{C} \rangle\!\rangle}^{k_2}_{k_1} \top = \top$$

Case ($\mathtt{x} \in I$). In this case

$$\begin{aligned}\overline{\langle\!\langle \mathtt{x} \in I \rangle\!\rangle}^{k_2}_{k_1} \top &= (\overline{\alpha}_{k_1,k_2} \circ \dot{\alpha}_{k_1,k_2})(\langle\!\langle \mathtt{x} \in I \rangle\!\rangle(\lambda \mathtt{y}.\top)) \\ &= (\overline{\alpha}_{k_1,k_2} \circ \dot{\alpha}_{k_1,k_2}) f\end{aligned}$$

where

$$f(\mathtt{y}) = \begin{cases} \gamma_{k_1,k_2}(I) & \text{if } \mathtt{y} = \mathtt{x} \\ \top & \text{otherwise} \end{cases}$$

Now notice that for all $\mathtt{y} \neq \mathtt{x}$ it holds that $\dot{\alpha}_{k_1,k_2}(f)(\mathtt{y}) = \top$, hence $(\overline{\alpha}_{k_1,k_2} \circ \dot{\alpha}_{k_1,k_2})(f) = \top$, which is our thesis.

Case ($\mathtt{x} := k$). In this case

$$\begin{aligned}\overline{\langle\!\langle \mathtt{x} := k \rangle\!\rangle}^{k_2}_{k_1} \top &= (\overline{\alpha}_{k_1,k_2} \circ \dot{\alpha}_{k_1,k_2})(\langle\!\langle \mathtt{x} := k \rangle\!\rangle(\lambda \mathtt{y}.\top)) \\ &= (\overline{\alpha}_{k_1,k_2} \circ \dot{\alpha}_{k_1,k_2}) f\end{aligned}$$

where

$$f(\mathtt{y}) = \begin{cases} \{k\} & \text{if } \mathtt{y} = \mathtt{x} \\ \top & \text{otherwise} \end{cases}$$

Now notice that for all $\mathtt{y} \neq \mathtt{x}$ it holds that $\dot{\alpha}_{k_1,k_2}(f)(\mathtt{y}) = \top$, hence $(\overline{\alpha}_{k_1,k_2} \circ \dot{\alpha}_{k_1,k_2})(f) = \top$, which is our thesis.

Case ($\mathtt{x} := \mathtt{y} + k$). In this case

$$\begin{aligned}\overline{\langle\!\langle \mathtt{x} := \mathtt{y} + k \rangle\!\rangle}^{k_2}_{k_1} \top &= (\overline{\alpha}_{k_1,k_2} \circ \dot{\alpha}_{k_1,k_2})(\langle\!\langle \mathtt{x} := \mathtt{y} + k \rangle\!\rangle(\lambda \mathtt{w}.\top)) \\ &= (\overline{\alpha}_{k_1,k_2} \circ \dot{\alpha}_{k_1,k_2})(\lambda \mathtt{w}.\top) && \text{since } \top + k = \top \\ &= \top\end{aligned}$$

Case $(\mathsf{C}_1 + \mathsf{C}_2)$. In this case

$$\begin{aligned}\overline{\langle\!\langle \mathsf{C}_1 + \mathsf{C}_2 \rangle\!\rangle}^{k_2}_{k_1} \top &= \overline{\langle\!\langle \mathsf{C}_1 \rangle\!\rangle}^{k_2}_{k_1} \top \dot{\cup} \overline{\langle\!\langle \mathsf{C}_2 \rangle\!\rangle}^{k_2}_{k_1} \top \\ &= \top \dot{\cup} \top && \text{By inductive hypothesis} \\ &= \top\end{aligned}$$

Case $(\mathsf{C}_1; \mathsf{C}_2)$. In this case

$$\begin{aligned}\overline{\langle\!\langle \mathsf{C}_1; \mathsf{C}_2 \rangle\!\rangle}^{k_2}_{k_1} \top &= \overline{\langle\!\langle \mathsf{C}_2 \rangle\!\rangle}^{k_2}_{k_1} \left(\overline{\langle\!\langle \mathsf{C}_1 \rangle\!\rangle}^{k_2}_{k_1} \top \right) \\ &= \overline{\langle\!\langle \mathsf{C}_2 \rangle\!\rangle}^{k_2}_{k_1} \top && \text{By induction on } \mathsf{C}_1 \\ &= \top && \text{By induction on } \mathsf{C}_2\end{aligned}$$

Case $(\mathsf{fix}(\mathsf{C}))$. In this case

$$\begin{aligned}\overline{\langle\!\langle \mathsf{fix}(\mathsf{C}) \rangle\!\rangle}^{k_2}_{k_1} \top &= \mathrm{lfp}\left(\lambda \mu . \top \dot{\cup} \overline{\langle\!\langle \mathsf{C} \rangle\!\rangle}^{k_2}_{k_1} \mu \right) \dot{\supseteq} \top && \text{By definition of lfp} \\ &= \top && \text{By definition of } \top\end{aligned}$$

□

Theorem 4.29. *Let $\mathsf{C} \in \mathsf{Imp}$ be a program. Then, for all finitely supported $\eta \in \overline{\mathbb{C}}^{k_2}_{k_1}$ and $k_1, k_2 \in \mathbb{Z}$ s.t. $\mathbb{C}_{\mathsf{C},\eta} \preccurlyeq \mathbb{C}^{k_2}_{k_1}$, i.e., $k_1 \leqslant \min(\eta) - (\mathsf{C})^+_{\mathsf{b}}$ and $k_2 \geqslant \max(\eta) + (\mathsf{C})^{\mathsf{b}}_+$ then*

$$\overline{\langle\!\langle \mathsf{C} \rangle\!\rangle}^{k_2}_{k_1} \eta \neq \top \quad \Longrightarrow \quad \langle\!\langle \mathsf{C} \rangle\!\rangle \eta = \overline{\langle\!\langle \mathsf{C} \rangle\!\rangle}^{k_2}_{k_1} \eta$$

i.e., if the analysis over $\overline{\mathbb{C}}^{k_2}_{k_1}$ does not diverge, then the analysis over $\mathbb{C}$ converges to the same result.

Proof. The proof will proceed by induction on the program C, covering first the base cases of Exp expressions and then the inductive cases of Imp. Notice that because of Lemma 4.24

$$\langle\!\langle \mathsf{C} \rangle\!\rangle \overline{\gamma}_{k_1,k_2}(\overline{\eta}) \dot{\subseteq} [\![\mathsf{C}]\!]^{\mathbb{C}^{k_2}_{k_1}} \overline{\gamma}_{k_1,k_2}(\overline{\eta}) \dot{\subseteq} \overline{\gamma}_{k_1,k_2}(\overline{\langle\!\langle \mathsf{C} \rangle\!\rangle}^{k_2}_{k_1} \overline{\eta})$$

already holds for every $k_1, k_2 \in \mathbb{Z}$ s.t. $k_1 \leqslant k_2$ and $\overline{\eta} \in \overline{\mathbb{C}}^{k_2}_{k_1}$, hence what we have to prove for every case is that

$$\overline{\langle\!\langle \mathsf{C} \rangle\!\rangle}^{k_2}_{k_1} \eta \neq \top \implies \langle\!\langle \mathsf{C} \rangle\!\rangle \eta \dot{\supseteq} \overline{\langle\!\langle \mathsf{C} \rangle\!\rangle}^{k_2}_{k_1} \eta$$

First notice that it cannot be $\overline{\eta} = \top$, otherwise by Lemma 4.28 $\overline{\langle\!\langle \mathsf{C} \rangle\!\rangle}^{k_2}_{k_1} \top = \top$ and therefore the hypothesis $\overline{\langle\!\langle \mathsf{C} \rangle\!\rangle}^{k_2}_{k_1} \top \neq \top$ is not respceted. Furthermore, notice that $\overline{\langle\!\langle \mathsf{C} \rangle\!\rangle}^{k_2}_{k_1} \overline{\eta} \neq \top$ implies that $\overline{\gamma}_{k_1,k_2}(\overline{\langle\!\langle \mathsf{C} \rangle\!\rangle}^{k_2}_{k_1} \overline{\eta}) = \overline{\langle\!\langle \mathsf{C} \rangle\!\rangle}^{k_2}_{k_1} \overline{\eta}$, due to the definition of $\overline{\gamma}_{k_1,k_2}$.

Case (e). In this case we have to prove that

$$\overline{\langle\!\langle \mathsf{e} \rangle\!\rangle}^{k_2}_{k_1} \overline{\eta} \neq \top \implies \langle\!\langle \mathsf{e} \rangle\!\rangle \overline{\gamma}_{k_1,k_2}(\overline{\eta}) = \overline{\gamma}_{k_1,k_2}(\overline{\langle\!\langle \mathsf{e} \rangle\!\rangle}^{k_2}_{k_1} \overline{\eta})$$

First, if $\overline{\eta} = \bot$ we can notice that

$$(\overline{\alpha}_{k_1 k_2} \circ \dot{\alpha}_{k_1,k_2} \circ \langle\!\langle \mathsf{e} \rangle\!\rangle) \bot = \bot = \langle\!\langle \mathsf{e} \rangle\!\rangle \overline{\gamma}_{k_1,k_2}(\bot)$$

which is our thesis.

The last case is when $\top \neq \overline{\eta} \neq \bot$ and therefore for all $\mathtt{x} \in \mathit{Var}$ $\overline{\eta}\mathtt{x} \in \wp(\mathbb{Z})^{k_2}_{k_1}$. In this case by Lemma 4.17 and Lemma 4.19 for all $\mathtt{y} \in \mathit{Var}$ both

$$\begin{aligned}\max(\langle\!\langle \mathsf{e} \rangle\!\rangle \overline{\gamma}_{k_1,k_2}(\overline{\eta})\mathtt{y}) &\leqslant \max(\overline{\gamma}_{k_1,k_2}(\overline{\eta})) + (\mathsf{e})^{\mathsf{b}} \leqslant \max(\overline{\gamma}_{k_1,k_2}(\overline{\eta})) + (\mathsf{e})^{\mathsf{b}}_+ = k_2 \\ \min(\langle\!\langle \mathsf{e} \rangle\!\rangle \overline{\gamma}_{k_1,k_2}(\overline{\eta})\mathtt{y}) &\geqslant \min(\overline{\gamma}_{k_1,k_2}(\overline{\eta})) - (\mathsf{e})_{\mathsf{b}} \geqslant \min(\overline{\gamma}_{k_1,k_2}(\overline{\eta})) - (\mathsf{e})^+_{\mathsf{b}} = k_1\end{aligned}$$

hence by definition of $\dot{\alpha}_{k_1,k_2}$ and $\overline{\alpha}_{k_1,k_2}$

$$\left(\overline{\alpha}_{k_1,k_2} \circ \dot{\alpha}_{k_1,k_2}\right)\left(\langle\!\langle \mathsf{e} \rangle\!\rangle \overline{\gamma}_{k_1,k_2}(\overline{\eta})\right) = \langle\!\langle \mathsf{e} \rangle\!\rangle \overline{\gamma}_{k_1,k_2}(\overline{\eta})$$

which is our thesis.

Case $(\mathsf{C}_1 + \mathsf{C}_2)$. In this case we have to prove that

$$\overline{\langle\!\langle \mathsf{C}_1 + \mathsf{C}_2 \rangle\!\rangle}^{k_2}_{k_1}\eta \neq \top \implies \langle\!\langle \mathsf{C}_1 + \mathsf{C}_2 \rangle\!\rangle \eta = \overline{\langle\!\langle \mathsf{C}_1 + \mathsf{C}_2 \rangle\!\rangle}^{k_2}_{k_1}\eta$$

with $k_1 \leqslant \min(\eta) - (\mathsf{C}_1 + \mathsf{C}_2)^+_{\mathsf{b}}$ and $k_2 \geqslant \max(\eta) + (\mathsf{C}_1 + \mathsf{C}_2)^{\mathsf{b}}_+$. First we can notice that since $\overline{\langle\!\langle \mathsf{C}_1 + \mathsf{C}_2 \rangle\!\rangle}^{k_2}_{k_1}\eta\mathtt{x} = \overline{\langle\!\langle \mathsf{C}_1 \rangle\!\rangle}^{k_2}_{k_1}\eta\mathtt{x} \cup \overline{\langle\!\langle \mathsf{C}_2 \rangle\!\rangle}^{k_2}_{k_1}\eta\mathtt{x}$ our hypothesis $\overline{\langle\!\langle \mathsf{C}_1 + \mathsf{C}_2 \rangle\!\rangle}^{k_2}_{k_1}\eta\mathtt{x} \neq \top$ implies both $\overline{\langle\!\langle \mathsf{C}_1 \rangle\!\rangle}^{k_2}_{k_1}\eta\mathtt{x} \neq \top$ and $\overline{\langle\!\langle \mathsf{C}_2 \rangle\!\rangle}^{k_2}_{k_1}\eta\mathtt{x} \neq \top$. Hence by choice of k_1 and k_2 we can use the inductive hypothesis and state that

$$\langle\!\langle \mathsf{C}_1 \rangle\!\rangle \eta\mathtt{x} = \overline{\langle\!\langle \mathsf{C}_1 \rangle\!\rangle}^{k_2}_{k_1}\eta\mathtt{x}$$
$$\langle\!\langle \mathsf{C}_2 \rangle\!\rangle \eta\mathtt{x} = \overline{\langle\!\langle \mathsf{C}_2 \rangle\!\rangle}^{k_2}_{k_1}\eta\mathtt{x}$$

and by closure over $\cup$

$$\langle\!\langle \mathsf{C}_1 + \mathsf{C}_2 \rangle\!\rangle \eta\mathtt{x} = \langle\!\langle \mathsf{C}_1 \rangle\!\rangle \eta\mathtt{x} \cup \langle\!\langle \mathsf{C}_2 \rangle\!\rangle \eta\mathtt{x} = \overline{\langle\!\langle \mathsf{C}_1 \rangle\!\rangle}^{k_2}_{k_1}\eta\mathtt{x} \cup \overline{\langle\!\langle \mathsf{C}_2 \rangle\!\rangle}^{k_2}_{k_1}\eta\mathtt{x} = \overline{\langle\!\langle \mathsf{C}_1 + \mathsf{C}_2 \rangle\!\rangle}^{k_2}_{k_1}\eta\mathtt{x}$$

which is our thesis.

Case $(\mathsf{C}_1; \mathsf{C}_2)$. In this case we have to prove that

$$\overline{\langle\!\langle \mathsf{C}_1; \mathsf{C}_2 \rangle\!\rangle}^{k_2}_{k_1}\eta \neq \top \implies \langle\!\langle \mathsf{C}_1; \mathsf{C}_2 \rangle\!\rangle \eta = \overline{\langle\!\langle \mathsf{C}_1; \mathsf{C}_2 \rangle\!\rangle}^{k_2}_{k_1}\eta$$

for all $k_1 \leqslant \min(\eta) - (\mathsf{C}_1; \mathsf{C}_2)^+_{\mathsf{b}}$ and $k_2 \geqslant \max(\eta) + (\mathsf{C}_1; \mathsf{C}_2)^{\mathsf{b}}_+$. First let's recall that

$$\overline{\langle\!\langle \mathsf{C}_1; \mathsf{C}_2 \rangle\!\rangle}^{k_2}_{k_1}\overline{\eta} = \overline{\langle\!\langle \mathsf{C}_2 \rangle\!\rangle}^{k_2}_{k_1}\left(\overline{\langle\!\langle \mathsf{C}_1 \rangle\!\rangle}^{k_2}_{k_1}\overline{\eta}\right)$$

and we are under the hypothesis $\overline{\langle\!\langle \mathsf{C}_1; \mathsf{C}_2 \rangle\!\rangle}^{k_2}_{k_1}\overline{\eta} \neq \top$, which means that $\overline{\langle\!\langle \mathsf{C}_2 \rangle\!\rangle}^{k_2}_{k_1}\overline{\eta} \neq \top \neq \overline{\langle\!\langle \mathsf{C}_2 \rangle\!\rangle}^{k_2}_{k_1}\overline{\eta}'$ where $\overline{\eta}' = \overline{\langle\!\langle \mathsf{C}_1 \rangle\!\rangle}^{k_2}_{k_1}\overline{\eta}$, otherwise by Lemma 4.28 we would contraddict the hypothesis $\overline{\langle\!\langle \mathsf{C}_1 + \mathsf{C}_2 \rangle\!\rangle}^{k_2}_{k_1}\overline{\eta} \neq \top$. Then, by inductive hypothesis $\langle\!\langle \mathsf{C}_1 \rangle\!\rangle \overline{\eta} = \overline{\langle\!\langle \mathsf{C}_1 \rangle\!\rangle}^{k_2}_{k_1}\overline{\eta}$ for all $k_1 \leqslant \min(\eta) - (\mathsf{C}_1)^+_{\mathsf{b}}$ and $k_2 \geqslant \max(\eta) + (\mathsf{C}_2)^{\mathsf{b}}_+$. We can now call $\overline{\eta}' = \overline{\langle\!\langle \mathsf{C}_1 \rangle\!\rangle}^{k_2}_{k_1}\overline{\eta}$ and by inductive hypothesis again:

$$\overline{\langle\!\langle \mathsf{C}_2 \rangle\!\rangle}^{k_2}_{k_1}\eta' \neq \top \implies \langle\!\langle \mathsf{C}_2 \rangle\!\rangle \eta' = \overline{\langle\!\langle \mathsf{C}_2 \rangle\!\rangle}^{k_2}_{k_1}\eta'$$

for all $k_1 \leqslant \min(\eta') - (\mathsf{C}_2)^+_{\mathsf{b}}$ and $k_2 \geqslant \max(\eta') + (\mathsf{C})^{\mathsf{b}}_+$. Notice that $\min(\eta') \geqslant \min(\eta) - (\mathsf{C}_1)^+_{\mathsf{b}}$ and $\max(\eta') \leqslant \max(\eta) + (\mathsf{C}_1)^{\mathsf{b}}_+$ and therefore we can chose $k_1 \leqslant \min(\eta) - (\mathsf{C}_1)^+_{\mathsf{b}} - (\mathsf{C}_2)^+_{\mathsf{b}}$ and $k_2 \geqslant \max(\eta) + (\mathsf{C}_1)^{\mathsf{b}}_+ + (\mathsf{C}_2)^{\mathsf{b}}_+$. Since both inductive hypothesis hold, then following holds

$$\overline{\langle\!\langle \mathsf{C}_1; \mathsf{C}_2 \rangle\!\rangle}^{k_2}_{k_1}\eta \neq \top \implies \langle\!\langle \mathsf{C}_1; \mathsf{C}_2 \rangle\!\rangle \eta = \overline{\langle\!\langle \mathsf{C}_1; \mathsf{C}_2 \rangle\!\rangle}^{k_2}_{k_1}\eta$$

which is our thesis.

Case $(\mathsf{fix}(\mathsf{C}))$. In this case we want to prove that

$$\overline{\langle\!\langle \mathsf{fix}(\mathsf{C}) \rangle\!\rangle}^{k_2}_{k_1}\overline{\eta} \neq \top \implies \langle\!\langle \mathsf{fix}(\mathsf{C}) \rangle\!\rangle \overline{\eta} = \overline{\langle\!\langle \mathsf{fix}(\mathsf{C}) \rangle\!\rangle}^{k_2}_{k_1}\overline{\eta}$$

for all $k_1 \geqslant \min(\overline{\eta}) - (\mathsf{fix}(\mathsf{C}))^+_{\mathsf{b}}$ and $k_2 \leqslant \max(\overline{\eta}) + (\mathsf{fix}(\mathsf{C}))^{\mathsf{b}}_+$. Recall that by Lemma 4.24 it always holds that

$$\langle\!\langle \mathsf{fix}(\mathsf{C}) \rangle\!\rangle \overline{\eta} \mathrel{\dot{\subseteq}} \overline{\langle\!\langle \mathsf{fix}(\mathsf{C}) \rangle\!\rangle}^{k_2}_{k_1}\overline{\eta}$$

We have therefore to prove that

$$\overline{\langle\!\langle \mathsf{fix(C)} \rangle\!\rangle}^{k_2}_{k_1} \overline{\eta} \neq \top \implies \langle\!\langle \mathsf{fix(C)} \rangle\!\rangle \overline{\eta} \mathrel{\dot{\supseteq}} \overline{\langle\!\langle \mathsf{fix(C)} \rangle\!\rangle}^{k_2}_{k_1} \overline{\eta} \tag{4.25}$$

for all $k_1 \leqslant \min(\overline{\eta}) - (\mathsf{fix(C)})^{+}_{\mathsf{b}}$ and $k_2 \geqslant \max(\overline{\eta}) + (\mathsf{fix(C)})^{\mathsf{b}}_{+}$. To start notice that according to Lemma 3.4 $\langle\!\langle \mathsf{fix(C)} \rangle\!\rangle \overline{\eta} = \langle\!\langle (\mathsf{C} + \mathsf{true})^{*} \rangle\!\rangle \overline{\eta}$, hence we can alternatively prove that

$$\overline{\langle\!\langle \mathsf{fix(C)} \rangle\!\rangle}^{k_2}_{k_1} \overline{\eta} \neq \top \implies \langle\!\langle \mathsf{fix(C)} \rangle\!\rangle \overline{\eta} \mathrel{\dot{\supseteq}} \bigcup_{i \in \mathbb{N}} \left(\overline{\langle\!\langle \mathsf{C} + \mathsf{true} \rangle\!\rangle}^{k_2}_{k_1} \right)^{i} \overline{\eta}$$

which implies Equation 4.25. To start we will initially prove that for every $i \in \mathbb{N}$ it holds that

$$\langle\!\langle \mathsf{fix(C)} \rangle\!\rangle \overline{\eta} \neq \top \implies \langle\!\langle \mathsf{fix(C)} \rangle\!\rangle \overline{\eta} \mathrel{\dot{\supseteq}} \left(\overline{\langle\!\langle \mathsf{C} + \mathsf{true} \rangle\!\rangle}^{k_2}_{k_1} \right)^{i} \overline{\eta}$$

to then prove the first one by closure over $\cup$. We will prove it by induction on i:

Case $(i = 0)$. In this case we have to prove that

$$\overline{\langle\!\langle \mathsf{fix(C)} \rangle\!\rangle}^{k_2}_{k_1} \overline{\eta} \neq \top \implies \langle\!\langle \mathsf{fix(C)} \rangle\!\rangle \overline{\eta} \mathrel{\dot{\supseteq}} \overline{\eta}$$

We can notice that by definition of $\langle\!\langle \mathsf{fix(C)} \rangle\!\rangle$ the thesis holds.

Case $(i \implies i+1)$. In this case we have to prove that

$$\langle\!\langle \mathsf{fix(C)} \rangle\!\rangle \overline{\eta} \neq \top \implies \langle\!\langle \mathsf{fix(C)} \rangle\!\rangle \overline{\eta} \supseteq \left(\overline{\langle\!\langle \mathsf{C} \rangle\!\rangle}^{k_2}_{k_1} + \mathsf{true} \right)^{i+1} \overline{\eta}$$

First we can notice that

$$\begin{aligned}
\langle\!\langle \mathsf{C} + \mathsf{true} \rangle\!\rangle (\langle\!\langle \mathsf{fix(C)} \rangle\!\rangle \overline{\eta}) &= \langle\!\langle \mathsf{C} \rangle\!\rangle (\langle\!\langle \mathsf{fix(C)} \rangle\!\rangle \overline{\eta}) \cup \langle\!\langle \mathsf{fix(C)} \rangle\!\rangle \overline{\eta} \\
&= \langle\!\langle \mathsf{C} \rangle\!\rangle (\mathrm{lfp}(\lambda \mu. \overline{\eta} \cup \langle\!\langle \mathsf{C} \rangle\!\rangle \mu)) \cup \langle\!\langle \mathsf{fix(C)} \rangle\!\rangle \overline{\eta} \\
&= \overline{\eta} \cup \langle\!\langle \mathsf{C} \rangle\!\rangle (\mathrm{lfp}(\lambda \mu. \overline{\eta} \cup \langle\!\langle \mathsf{C} \rangle\!\rangle \mu)) \cup \langle\!\langle \mathsf{fix(C)} \rangle\!\rangle \overline{\eta} && \text{since } \overline{\eta} \subseteq \mathrm{lfp}(\lambda \mu. \overline{\eta} \cup \langle\!\langle \mathsf{C} \rangle\!\rangle \mu) \\
&= (\lambda \mu. \overline{\eta} \cup \langle\!\langle \mathsf{C} \rangle\!\rangle \mu)(\mathrm{lfp}(\lambda \mu. \overline{\eta} \cup \langle\!\langle \mathsf{C} \rangle\!\rangle \mu)) \cup \langle\!\langle \mathsf{fix(C)} \rangle\!\rangle \overline{\eta} \\
&= (\mathrm{lfp}(\lambda \mu. \overline{\eta} \cup \langle\!\langle \mathsf{C} \rangle\!\rangle \mu)) \cup \langle\!\langle \mathsf{fix(C)} \rangle\!\rangle \overline{\eta} && \text{by def. of lfp} \\
&= \langle\!\langle \mathsf{fix(C)} \rangle\!\rangle \overline{\eta} \cup \langle\!\langle \mathsf{fix(C)} \rangle\!\rangle \overline{\eta} \\
&= \langle\!\langle \mathsf{fix(C)} \rangle\!\rangle \overline{\eta}
\end{aligned}$$

Now we can preliminarly observe that by calling $\beta = \langle\!\langle \mathsf{fix(C)} \rangle\!\rangle \overline{\eta}$

$$\langle\!\langle \mathsf{C} + \mathsf{true} \rangle\!\rangle \beta \supseteq \overline{\langle\!\langle \mathsf{C} + \mathsf{true} \rangle\!\rangle}^{k_2}_{k_1} \beta \tag{4.26}$$

In fact, for all $\mathtt{x} \in \mathit{Var}$

$$\begin{aligned}
\max(\langle\!\langle \mathsf{C} + \mathsf{true} \rangle\!\rangle \beta \mathtt{x}) &\leqslant \max(\beta) + (\mathsf{C} + \mathsf{true})^{\mathsf{b}} = \max(\beta) + (\mathsf{C})^{\mathsf{b}} \\
&\leqslant \max(\overline{\eta}) + (\mathsf{fix(C)})^{\mathsf{b}} + (\mathsf{C})^{\mathsf{b}} && \text{by Lemma 4.17} \\
&\leqslant \max(\overline{\eta}) + (n+2)(\mathsf{C})^{\mathsf{b}} \\
&\leqslant \max(\overline{\eta}) + (n+2)(\mathsf{C})^{\mathsf{b}}_{+} \\
&\leqslant \max(\overline{\eta}) + (\mathsf{fix(C)})^{\mathsf{b}}_{+} = k_2
\end{aligned}$$

similarly for the min value

$$\min(\langle\!\langle \mathsf{C} + \mathsf{true} \rangle\!\rangle \beta \mathtt{x}) \geqslant \min(\overline{\eta}) - (\mathsf{fix(C)})^{+}_{\mathsf{b}} = k_1$$

hence

$$\begin{aligned}
\beta = \langle\!\langle \mathsf{C} + \mathsf{true} \rangle\!\rangle \beta &\supseteq \overline{\langle\!\langle \mathsf{C} + \mathsf{true} \rangle\!\rangle}^{k_2}_{k_1} \beta && \text{by (4.26)} \\
&\supseteq \overline{\langle\!\langle \mathsf{C} + \mathsf{true} \rangle\!\rangle}^{k_2}_{k_1} \left(\overline{\langle\!\langle \mathsf{C} + \mathsf{true} \rangle\!\rangle}^{k_2}_{k_1} \right)^{i} \overline{\eta} && \text{by induction on } i \\
&= \left(\overline{\langle\!\langle \mathsf{C} + \mathsf{true} \rangle\!\rangle}^{k_2}_{k_1} \right)^{i+1} \overline{\eta}
\end{aligned}$$

Hence our thesis, for all $i \in \mathbb{N}$

$$\overline{\langle\!\langle \mathsf{fix(C)} \rangle\!\rangle}^{k_2}_{k_1} \overline{\eta} \top \implies \langle\!\langle \mathsf{fix(C)} \rangle\!\rangle \overline{\eta} \supseteq \left(\overline{\langle\!\langle \mathsf{C} + \mathsf{true} \rangle\!\rangle}^{k_2}_{k_1} \right)^i \overline{\eta}$$

holds. We can now conclude by noticing that our original thesis

$$\overline{\langle\!\langle \mathsf{fix(C)} \rangle\!\rangle}^{k_2}_{k_1} \overline{\eta} \neq \top \implies \langle\!\langle \mathsf{fix(C)} \rangle\!\rangle \overline{\eta} \supseteq \bigcup_{i \in \mathbb{N}} \left(\overline{\langle\!\langle \mathsf{C} + \mathsf{true} \rangle\!\rangle}^{k_2}_{k_1} \right)^i \overline{\eta} = \overline{\langle\!\langle \mathsf{fix(C)} \rangle\!\rangle}^{k_2}_{k_1} \overline{\eta}$$

also holds.

□

The latter theorem is a result similar to the result for the interval domain with Theorem 4.16. In its essence it states that when doing static analysis with abstract interpretation using the non relational collecting domain $\mathbb{C}$ for some program $\mathsf{C} \in \mathsf{Imp}$ and an initial environment $\eta \in \mathbb{C}$ we can consider a bounded version of the domain $\mathbb{C}^{k_2}_{k_1}$ with $k_1 = \min(\eta) - (\mathsf{C})^+_{\mathsf{b}}$ and $k_2 = \max(\eta) + (\mathsf{C})^{\mathsf{b}}_+$ (hence computed accordingly to C and η). Each variable $\mathsf{x} \in \mathit{Var}_{\mathsf{C}}$ either

Chapter 5

Conclusion

In conclusion we provided an alternative method to [Gaw+09] to do exact analysis with the interval domain, and also showed that some results are extensible to non relational collecting semantics.

Appendix A

Additional proofs

A.1 Lemma 4.6 proof

We preliminarly observe that we can also prove a dual property of the Lemma 4.3:

Lemma A.1 (**Negative cycles in weighted directed graphs**). *Let p be a finite path*

$$p = x_0 \to_{h_0} x_1 \to_{h_1} x_2 \to_{h_2} \cdots \to_{h_{\ell-1}} x_\ell$$

with $m \triangleq \max\{|h_j| \mid j \in \{0, \ldots, \ell-1\}\} \in \mathbb{N}$ and $w(p) < -(|X|-1)m$. Then, p has a subpath which is a cycle having a strictly negative weight.

Proof. First note that $w(p) = \Sigma_{k=0}^{\ell-1} h_k < -m(|X|-1)$ implies that $|p| = \ell \geqslant |X|$. Then, we show our claim by induction on $|p| = \ell \geqslant |X|$.
Case ($|p| = |X|$). Since the path p includes exactly $|X|+1 = \ell+1$ nodes, there exist indices $0 \leqslant i < j \leqslant \ell$ such that $x_i = x_j$, i.e., $p_{i,j}$ is a subpath of p which is a cycle. Moreover, since this cycle $p_{i,j}$ includes at least one edge, we have that

$$\begin{aligned}
w(p_{i,j}) = w(p) - (\Sigma_{k=0}^{i-1} h_k + \Sigma_{k=j}^{\ell-1} h_k) < & \quad \text{as } w(p) < -m(|X|-1) \\
-m\,(|X|-1) - (\Sigma_{k=0}^{i-1} h_k + \Sigma_{k=j}^{\ell-1} h_k) \leqslant & \quad \text{as } \Sigma_{k=0}^{i-1} h_k + \Sigma_{k=j}^{\ell-1} h_k \geqslant -m(\ell-1) \\
-m(|X|-1) - (-m(\ell-1)) = & \quad \text{as } \ell = |X| \\
-m(|X|-1) + m(|X|-1) = 0 &
\end{aligned}$$

so that $w(p_{i,j}) < 0$ holds.

($|p| > |X|$): Since the path p includes at least $|X|+2$ nodes, as in the base case, we have that p has a subpath which is a cycle. Then, we consider a cycle $p_{i,j}$ in p, for some indices $0 \leqslant i < j \leqslant \ell$, which is maximal, i.e., such that if $p_{i',j'}$ is a cycle in p, for some $0 \leqslant i' < j' \leqslant \ell$, then $p_{i,j}$ is not a proper subpath of $p_{i',j'}$.

If $w(p_{i,j}) < 0$ then we are done. Otherwise we have that $w(p_{i,j}) \geqslant 0$ and we consider the path p' obtained from p by stripping off the cycle $p_{i,j}$, i.e.,

$$p' \equiv \overbrace{x_0 \to_{h_0} x_1 \to_{h_1} \cdots \to_{h_{i-1}} x_i}^{p'_{0,i}} = \overbrace{x_j \to_{h_{j+1}} \cdots \to_{h_{\ell-1}} x_\ell}^{p'_{j+1,\ell}}$$

Since $|p'| < |p|$ and $w(p') = w(p) - w(p_{i,j}) \leqslant w(p) < -m(|X|-1)$, we can apply the inductive hypothesis on p'. We therefore derive that p' has a subpath q which is a cycle having strictly positive weight. This cycle q is either entirely in $p'_{0,i}$ or in $p'_{j+1,\ell}$, otherwise q would include the cycle $p_{i,j}$ thus contradicting the maximality of $p_{i,j}$. Hence, q is a cycle in the original path p having a strictly negative weight. □

For the following proof consider the $\min : \mathbb{I} \to \mathbb{Z}$ function, inductively defined as follows:

$$\min(\bot) = +\infty$$
$$\min([a, b]) = a$$

and recall the Lemma 4.6 statement:

Lemma A.2. *Let* $\mathsf{C} \in \mathsf{Imp}$.
For all $\eta \in \dot{\mathbb{I}}$ *and* $\mathtt{y} \in \mathit{Var}$, *if* $\min([\![\mathsf{C}]\!]\eta\mathtt{y}) \neq -\infty$ *and* $\min([\![\mathsf{C}]\!]\eta\mathtt{y}) < -(\mathsf{C})_{\mathsf{b}}$ *then there exist a variable* $\mathtt{z} \in \mathit{Var}$ *and an integer* $h \in \mathbb{Z}$ *s.t.* $|h| \leqslant (\mathsf{C})_{\mathsf{b}}$ *s.t. the following two properties hold:*

(i) $\min([\![\mathsf{C}]\!]\eta\mathtt{y}) = \min(\eta\mathtt{z}) + h$;

(ii) for all $\eta' \in \dot{\mathbb{I}}$, *if* $\eta' \sqsupseteq \eta$ *then* $\min([\![\mathsf{C}]\!]\eta'\mathtt{y}) \leqslant \min(\eta'\mathtt{z}) + h$.

Proof. The proof is by structural induction on the command $\mathsf{C} \in \mathsf{Imp}$. We preliminarly observe that we can safely assume $\eta \neq \bot$. In fact, if $\eta = \bot$ then $[\![\mathsf{C}]\!]\bot = \bot$ and thus $\min([\![\mathsf{C}]\!]\eta\mathtt{y}) = +\infty \geqslant (\mathsf{C})^{\mathsf{b}}$, against the hypothesis $\min([\![\mathsf{C}]\!]\eta\mathtt{y}) < -(\mathsf{C})_{\mathsf{b}}$. Moreover, when quantifying over η' such that $\eta' \sqsupseteq \eta$ in (i), if $\min([\![\mathsf{C}]\!]\eta'\mathtt{y}) = -\infty$ holds, then $\min([\![\mathsf{C}]\!]\eta'\mathtt{y}) \leqslant \min(\eta'\mathtt{z}) + h$ trivially holds, hence we will sometimes silently omit to consider this case.

Case $(\mathtt{x} \in S)$
Take $\eta \in \dot{\mathbb{I}}$ and assume $-\infty \neq \min([\![\mathtt{x} \in S]\!]\eta\mathtt{y}) < -(\mathtt{x} \in S)_{\mathsf{b}}$. Clearly $[\![\mathtt{x} \in S]\!]\eta \neq \bot$, otherwise we would get the contradiction $\min([\![\mathtt{x} \in S]\!]\eta\mathtt{y}) = +\infty \geqslant (\mathtt{x} \in S)_{\mathsf{b}}$. We distinguish two cases:

- If $\mathtt{y} \neq \mathtt{x}$, then for all $\eta' \in \dot{\mathbb{I}}$ such that $\eta \sqsubseteq \eta'$ it holds

  $$\bot \neq [\![\mathtt{x} \in S]\!]\eta' = \eta'[\mathtt{x} \mapsto \alpha_{\mathbb{I}}(\gamma_{\mathbb{I}}(\eta(\mathtt{x})) \cap \gamma_{\mathbb{I}}(S))]$$

  and thus

  $$\min([\![\mathtt{x} \in S]\!]\eta'\mathtt{y}) = \min(\eta'\mathtt{y}) = \min(\eta'\mathtt{y}) + 0$$

  hence the thesis follows with $\mathtt{z} = \mathtt{y}$ and $h = 0$.

- If $\mathtt{y} = \mathtt{x}$ then $\eta(\mathtt{x}) \in \mathbb{I}$ and

  $$\min([\![\mathtt{x} \in S]\!]\eta\mathtt{y}) = \min(\alpha_{\mathbb{I}}(\gamma_{\mathbb{I}}(\eta\mathtt{x}) \cap \gamma_{\mathbb{I}}(S)))$$

  Note that it cannot be $\min(S) \in \mathbb{Z}$. Otherwise, by Definition 4.2, $\min(\alpha_{\mathbb{I}}(\gamma_{\mathbb{I}}(\eta\mathtt{x}) \cap \gamma_{\mathbb{I}}(S))) \geqslant \min(S) = (\mathtt{x} \in S)_{\mathsf{b}}$, violating the assumption $\min([\![\mathtt{x} \in S]\!]\eta\mathtt{y}) < -(\mathtt{x} \in S)_{\mathsf{b}}$. Hence, $\min(S) = -\infty$ must hold and therefore $\min(\alpha_{\mathbb{I}}(\gamma_{\mathbb{I}}(\eta\mathtt{x}) \cap \gamma_{\mathbb{I}}(S))) = \min(\eta(\mathtt{x})) = \min(\eta(\mathtt{x})) + 0$. It is immediate to check that the same holds for all $\eta' \sqsupseteq \eta$, i.e.,

  $$\min(\alpha_{\mathbb{I}}(\gamma_{\mathbb{I}}(\eta'\mathtt{x}) \cap \gamma_{\mathbb{I}}(S))) = \min(\eta'\mathtt{x}) + 0$$

  and thus the thesis follows with $\mathtt{z} = \mathtt{y} = \mathtt{x}$ and $h = 0$.

Case $(\mathtt{x} := k)$ Take $\eta \in \dot{\mathbb{I}}$ and assume $\min([\![\mathtt{x} := k]\!]\eta\mathtt{y}) < -(\mathtt{x} := k)_{\mathsf{b}} = |k|$.
Observe that it cannot be $\mathtt{x} = \mathtt{y}$. In fact, since $[\![\mathtt{x} := k]\!]\eta = \eta[\mathtt{x} \mapsto \alpha_{\mathbb{I}}(\{k\})]$, we would have $[\![\mathtt{x} := k]\!]\eta\mathtt{y} = \alpha_{\mathbb{I}}(\{k\}) = [k, k]$ and thus

$$\min([\![\mathtt{x} := k]\!]\eta\mathtt{y}) = k \geqslant |k| = (\mathtt{x} := k)_{\mathsf{b}}$$

violating the assumption. Therefore, it must be $\mathtt{y} \neq \mathtt{x}$. Now, for all $\eta' \sqsupseteq \eta$, we have $[\![\mathtt{x} := k]\!]\eta'\mathtt{y} = \eta'\mathtt{y}$ and thus

$$\min([\![\mathtt{x} := k]\!]\eta'\mathtt{y}) = \min(\eta'\mathtt{y}) = \min(\eta'\mathtt{y}) + 0,$$

hence the thesis holds with $h = 0 \leqslant |k| = (\mathtt{x} := k)_\mathsf{b}$ and $\mathtt{z} = \mathtt{y}$.

Case $(\mathtt{x} := \mathtt{w} + k)$ Take $\eta \in \dot{\mathbb{I}}$ and assume $\min([\![\mathtt{x} := \mathtt{w} + k]\!]\eta\mathtt{y}) < -(\mathtt{x} := \mathtt{w} + k)_\mathsf{b} = -|k|$. Recall that $[\![\mathtt{x} := \mathtt{w} + k]\!]\eta = \eta[\mathtt{x} \mapsto \eta\mathtt{w} + k]$.

We distinguish two cases:

- If $\mathtt{y} \neq \mathtt{x}$, then for all $\eta' \sqsupseteq \eta$, we have $[\![\mathtt{x} := \mathtt{w} + k]\!]\eta'\mathtt{y} = \eta'\mathtt{y}$ and thus

$$\min([\![\mathtt{x} := \mathtt{w} + k]\!]\eta'\mathtt{y}) = \min(\eta'\mathtt{y}) + 0$$

  hence the thesis follows with $h = 0 \leqslant (\mathtt{x} := \mathtt{w} + k)_\mathsf{b}$ and $\mathtt{z} = \mathtt{y}$.

- If $\mathtt{x} = \mathtt{y}$ then for all $\eta' \sqsupseteq \eta$, we have $[\![\mathtt{x} := \mathtt{w} + k]\!]\eta'\mathtt{y} = \eta'\mathtt{w} + k$ and thus

$$\min([\![\mathtt{x} := \mathtt{w} + k]\!]\eta'\mathtt{y}) = \min(\eta'\mathtt{w}) + k$$

  hence, the thesis follows with $h = k$ (recall that $k \leqslant |k| = (\mathtt{x} := \mathtt{w} + k)_\mathsf{b}$) and $\mathtt{z} = \mathtt{w}$.

Case $(\mathsf{C}_1 + \mathsf{C}_2)$ Take $\eta \in \dot{\mathbb{I}}$ and assume $\min([\![\mathsf{C}_1 + \mathsf{C}_2]\!]\eta) < -(\mathsf{C}_1 + \mathsf{C}_2)_\mathsf{b} = -(\mathsf{C}_1)_\mathsf{b} - (\mathsf{C}_2)_\mathsf{b}$. Recall that $[\![\mathsf{C}_1 + \mathsf{C}_2]\!]\eta = [\![\mathsf{C}_1]\!]\eta \sqcup [\![\mathsf{C}_2]\!]\eta$. Hence, since $\min([\![\mathsf{C}_1 + \mathsf{C}_2]\!]\eta\mathtt{y}) \neq -\infty$, we have that $\min([\![\mathsf{C}_1]\!]\eta\mathtt{y}) \neq -\infty \neq \min([\![\mathsf{C}_2]\!]\eta\mathtt{y})$. Moreover

$$\begin{aligned}\min([\![\mathsf{C}_1 + \mathsf{C}_2]\!]\eta\mathtt{y}) &= \min([\![\mathsf{C}_1]\!]\eta\mathtt{y} \sqcup [\![\mathsf{C}_2]\!]\eta\mathtt{y}) \\ &= \min\{\min([\![\mathsf{C}_1]\!]\eta\mathtt{y}), \min([\![\mathsf{C}_2]\!]\eta\mathtt{y})\}\end{aligned}$$

Thus $\min([\![\mathsf{C}_1 + \mathsf{C}_2]\!]\eta\mathtt{y}) = \min([\![\mathsf{C}_i]\!]\eta\mathtt{y})$ for some $i \in \{1, 2\}$. We can assume, without loss of generality, that the maximum is realized by the first component, i.e., $\min([\![\mathsf{C}_1 + \mathsf{C}_2]\!]\eta\mathtt{y}) = \min([\![\mathsf{C}_1]\!]\eta\mathtt{y}) < -(\mathsf{C}_1 + \mathsf{C}_2)_\mathsf{b}$. Hence we can use the inductive hypothesis on C_1 and state that there exists $h \in \mathbb{Z}$ with $|h| \leqslant (\mathsf{C}_1)_\mathsf{b}$ and $\mathtt{z} \in \mathit{Var}$ such that $\min([\![\mathsf{C}_1]\!]\eta\mathtt{y}) = \min(\eta\mathtt{z}) + h$ and for all $\eta' \in \dot{\mathbb{I}}$, $\eta \sqsubseteq \eta'$,

$$\min([\![\mathsf{C}_1]\!]\eta'\mathtt{y}) \leqslant \min(\eta'\mathtt{z}) + h$$

Therefore

$$\min([\![\mathsf{C}_1 + \mathsf{C}_2]\!]\eta\mathtt{y}) = \min([\![\mathsf{C}_1]\!]\eta\mathtt{y}) = \min(\eta\mathtt{z}) + h$$

and and for all $\eta' \in \dot{\mathbb{I}}$, $\eta \sqsubseteq \eta'$,

$$\begin{aligned}\min([\![\mathsf{C}_1 + \mathsf{C}_2]\!]\eta'\mathtt{y}) &= \min\{\min([\![\mathsf{C}_1]\!]\eta'\mathtt{y}), \min([\![\mathsf{C}_2]\!]\eta'\mathtt{y})\} \\ &\leqslant \min([\![\mathsf{C}_1]\!]\eta'\mathtt{y}) \\ &\leqslant \min(\eta'\mathtt{z}) + h\end{aligned}$$

with $|h| \leqslant (\mathsf{C}_1)_\mathsf{b} \leqslant (\mathsf{C}_1 + \mathsf{C}_2)_\mathsf{b}$, as desired.

Case $(\mathsf{C}_1; \mathsf{C}_2)$ Take $\eta \in \dot{\mathbb{I}}$ and assume $\min([\![\mathsf{C}_1; \mathsf{C}_2]\!]\eta\mathtt{y}) < -(\mathsf{C}_1; \mathsf{C}_2)_\mathsf{b} = -(\mathsf{C}_1)_\mathsf{b} - (\mathsf{C}_2)_\mathsf{b}$.

Recall that $[\![\mathsf{C}_1; \mathsf{C}_2]\!]\eta = [\![\mathsf{C}_2]\!]([\![\mathsf{C}_1]\!]\eta)$. If we define

$$[\![\mathsf{C}_1]\!]\eta = \eta_1$$

since $\min([\![\mathsf{C}_2]\!]\eta_1\mathtt{y}) \neq -\infty$ and $\min([\![\mathsf{C}_2]\!]\eta_1\mathtt{y}) < -(\mathsf{C}_1; \mathsf{C}_2)_\mathsf{b} \leqslant (\mathsf{C}_2)_\mathsf{b}$, by inductive hypothesis on C_2, there are $|h_2| \leqslant (\mathsf{C}_2)_\mathsf{b}$ and $\mathtt{w} \in \mathit{Var}$ such that $\min([\![\mathsf{C}_2]\!]\eta_1\mathtt{y}) = \min(\eta_1\mathtt{w}) + h_2$ and for all $\eta_1' \in \dot{\mathbb{I}}$ with $\eta_1 \sqsubseteq \eta_1'$

$$\min([\![\mathsf{C}_2]\!]\eta_1'\mathtt{y}) \leqslant \min(\eta_1'\mathtt{w}) + h_2 \tag{A.1}$$

Now observe that $\min([\![\mathsf{C}_1]\!]\eta\mathtt{w}) = \min(\eta_1\mathtt{w}) < -(\mathsf{C}_1)_\mathsf{b}$. Otherwise, if it were $\min(\eta_1\mathtt{w}) \geqslant -(\mathsf{C}_1)_\mathsf{b}$ we would have

$$\min([\![\mathsf{C}_2]\!]\eta_1\mathtt{y}) = \min(\eta_1\mathtt{w}) + h_2 \geqslant -(\mathsf{C}_1)_\mathsf{b} - (\mathsf{C}_2)_\mathsf{b} = -(\mathsf{C}_1; \mathsf{C}_2)_\mathsf{b},$$

violating the hypotheses. Moreover, $\min([\![\mathsf{C}_1]\!]\eta\mathtt{w}) \neq -\infty$, otherwise we would have $\min([\![\mathsf{C}_2]\!]\eta_1\mathtt{y}) = \min(\eta_1\mathtt{w}) + h_2 = -\infty$, contradicting the hypotheses. Therefore we can apply the inductive hypothesis also to C_1 and deduce that there are $|h_1| \leqslant (\mathsf{C}_1)_\mathsf{b}$ and $\mathtt{w}' \in \mathit{Var}$ such that $\min([\![\mathsf{C}_1]\!]\eta\mathtt{w}) = \min(\eta\mathtt{w}') + h_1$ and for all $\eta' \in \dot{\mathbb{I}}$ with $\eta \sqsubseteq \eta'$

$$\min([\![\mathsf{C}_1]\!]\eta'\mathtt{w}) \leqslant \min(\eta'\mathtt{w}') + h_1 \tag{A.2}$$

Now, for all $\eta' \in \dot{\mathbb{I}}$ with $\eta \sqsubseteq \eta'$ we have that:

$$\begin{aligned}\min([\![\mathsf{C}_1;\mathsf{C}_2]\!]\eta\mathtt{y}) &= \min([\![\mathsf{C}_2]\!]([\![\mathsf{C}_1]\!]\eta)\mathtt{y}) \\ &= \min([\![\mathsf{C}_2]\!]\eta_1\mathtt{y}) \\ &= \min(\eta_1\mathtt{w}) + h_2 \\ &= \min([\![\mathsf{C}_1]\!]\eta\mathtt{w}) + h_2 \\ &= \min(\eta\mathtt{w}') + h_1 + h_2\end{aligned}$$

and

$$\begin{aligned}\min([\![\mathsf{C}_1;\mathsf{C}_2]\!]\eta'\mathtt{y}) &= \\ \min([\![\mathsf{C}_2]\!]([\![\mathsf{C}_1]\!]\eta')\mathtt{y}) &\leqslant \\ \min([\![\mathsf{C}_1]\!]\eta'\mathtt{w}) + h_2 &\leqslant && \text{by (A.1), since } \eta_1 = [\![\mathsf{C}_1]\!]\eta \sqsubseteq [\![\mathsf{C}_1]\!]\eta' \\ (\min(\eta'\mathtt{w}') + h_1) + h_2 & && \text{by (A.2)}\end{aligned}$$

Thus, the thesis holds with $h = h_1 + h_2$, as $|h| = |h_1 + h_2| \leqslant |h_1| + |h_2| \leqslant (\mathsf{C}_1)_\mathsf{b} + (\mathsf{C}_2)_\mathsf{b} = (\mathsf{C}_1;\mathsf{C}_2)_\mathsf{b}$, as needed.

Case ($\mathsf{fix}(\mathsf{C})$) Let $\eta \in \dot{\mathbb{I}}$ such that $\min([\![\mathsf{fix}(\mathsf{C})]\!]\eta\mathtt{y}) \neq -\infty$. Recall that $[\![\mathsf{fix}(\mathsf{C})]\!]\eta = \mathrm{lfp}\lambda\mu.([\![\mathsf{C}]\!]\mu \sqcup \eta)$. Observe that the least fixpoint of $\lambda\mu.([\![\mathsf{C}]\!]\mu \sqcup \eta)$ coincides with the least fixpoint of $\lambda\mu.([\![\mathsf{C}]\!]\mu \sqcup \mu) = \lambda\mu.[\![\mathsf{C} + \mathsf{true}]\!]\mu$ above η. Hence, if

- $\eta_0 \triangleq \eta$,
- for all $i \in \mathbb{N}$, $\eta_{i+1} \triangleq [\![\mathsf{C}]\!]\eta_i \sqcup \eta_i = [\![\mathsf{C} + \mathsf{true}]\!]\eta_i \sqsupseteq \eta_i$,

then we define an increasing chain $\{\eta_i\}_{i\in\mathbb{N}} \subseteq \dot{\mathbb{I}}$ such that

$$[\![\mathsf{fix}(\mathsf{C})]\!]\eta = \bigsqcup_{i\in\mathbb{N}} \eta_i.$$

Since $\min([\![\mathsf{fix}(\mathsf{C})]\!])\eta\mathtt{y} \neq -\infty$, we have that for all $i \in \mathbb{N}$, $\min(\eta_i\mathtt{y}) \neq -\infty$. Moreover, $\bigsqcup_{i\in\mathbb{N}} \eta_i$ on $\mathtt{y}$ is finitely reached in the chain $\{\eta_i\}_{i\in\mathbb{N}}$, i.e., there exists $m \in \mathbb{N}$ such that for all $i \geqslant m + 1$

$$[\![\mathsf{fix}(\mathsf{C})]\!]\eta\mathtt{y} = \eta_i\mathtt{y}.$$

The inductive hypothesis holds for C and true, hence for $\mathsf{C} + \mathsf{true}$, therefore for all $\mathtt{x} \in \mathit{Var}$ and $j \in \{0, 1, \ldots, m\}$, if $\min(\eta_{j+1}\mathtt{x}) < -(\mathsf{C} + \mathsf{true})_\mathsf{b} = -(\mathsf{C})_\mathsf{b}$ then there exist $\mathtt{z} \in \mathit{Var}$ and $h \in \mathbb{Z}$ such that $|h| \leqslant (\mathsf{C})_\mathsf{b}$ and

(a) $-\infty \neq \min(\eta_{j+1}\mathtt{x}) = \min(\eta_j\mathtt{z}) + h$,

(b) $\forall\eta' \sqsupseteq \eta_j.\, \min([\![\mathsf{C} + \mathsf{true}]\!]\eta'\mathtt{x}) \leqslant \min(\eta'\mathtt{z}) + h$.

To shortly denote that the two conditions (a) and (b) hold, we write

$$(\mathtt{z}, j) \to_h (\mathtt{x}, j + 1)$$

Now, assume that for some variable $\mathtt{y} \in \mathit{Var}$

$$\min([\![\mathsf{fix}(\mathsf{C})]\!]\eta\mathtt{y}) = \min(\eta_{m+1}\mathtt{y}) < -(\mathsf{fix}(\mathsf{C}))_\mathsf{b} = -(n + 1)(\mathsf{C})_\mathsf{b}$$

where $n = |vars(\mathsf{C})|$. We want to show that the thesis holds, i.e., that there exist $\mathtt{z} \in Var$ and $h \in \mathbb{Z}$ with $|h| \leqslant (\mathsf{fix}(\mathsf{C}))_{\mathsf{b}}$ such that:

$$\min([\![\mathsf{fix}(\mathsf{C})]\!]\eta\mathtt{y}) = \min(\eta\mathtt{z}) + h \tag{A.3}$$

and for all $\eta' \sqsupseteq \eta$,

$$\min([\![\mathsf{fix}(\mathsf{C})]\!]\eta'\mathtt{y}) \leqslant \min(\eta'\mathtt{z}) + h \tag{A.4}$$

Let us consider (i). We first observe that we can define a path

$$\sigma \triangleq (\mathtt{y}_0, 0) \rightarrow_{h_0} (\mathtt{y}_1, 1) \rightarrow_{h_1} \ldots \rightarrow_{h_m} (\mathtt{y}_{m+1}, m+1) \tag{A.5}$$

such that $\mathtt{y}_{m+1} = \mathtt{y}$ and for all $j \in \{0, \ldots, m+1\}$, $\mathtt{y}_j \in Var$ and $\min(\eta_j\mathtt{y}_j) < -(\mathsf{C})_{\mathsf{b}}$. In fact, if, by contradiction, this is not the case, there would exist an index $i \in \{0, \ldots, m\}$ (as

$$\min(\eta_{m+1}\mathtt{y}_{m+1}) < -(\mathsf{C})_{\mathsf{b}}$$

already holds) such that $\min(\eta_i\mathtt{y}_i) \geqslant -(\mathsf{C})_{\mathsf{b}}$, while for all $j \in \{i+1, \ldots, m+1\}$, $\min(\eta_j\mathtt{y}_j) < -(\mathsf{C})_{\mathsf{b}}$. Thus, in such a case, we consider the nonempty path:

$$\pi \triangleq (\mathtt{y}_i, i) \rightarrow_{h_i} (\mathtt{y}_{i+1}, i+1) \rightarrow_{h_{i+1}} \ldots \rightarrow_{h_m} (\mathtt{y}_{m+1}, m+1)$$

and we have that:

$$\begin{array}{l}
\Sigma_{j=i}^{m} h_j = \\
\Sigma_{j=i}^{m} \min(\eta_{j+1}\mathtt{y}_{j+1}) - \min(\eta_j\mathtt{y}_j) = \\
\min(\eta_{m+1}\mathtt{y}_{m+1}) - \min(\eta_i\mathtt{y}_i) = \\
\min(\eta_{m+1}\mathtt{y}) - \min(\eta_i\mathtt{y}_i) < \\
-(n+1)(\mathsf{C})_{\mathsf{b}} + (\mathsf{C})_{\mathsf{b}} = -n(\mathsf{C})_{\mathsf{b}}
\end{array}$$

with $|h_j| \leqslant (\mathsf{C})_{\mathsf{b}}$ for $j \in \{i, \ldots, m\}$. Hence we can apply Lemma A.1 to the projection π_p of the nodes of this path π to the variable component to deduce that π_p has a subpath which is a cycle with a strictly negative weight. More precisely, there exist $i \leqslant k_1 < k_2 \leqslant m+1$ such that $\mathtt{y}_{k_1} = \mathtt{y}_{k_2}$ and $h = \Sigma_{j=k_1}^{k_2-1} h_j < 0$. If we denote $\mathtt{w} = \mathtt{y}_{k_1} = \mathtt{y}_{k_2}$, then we have that

$$\begin{array}{lll}
\min(\eta_{k_2}\mathtt{w}) = h_{k_2-1} + \min(\eta_{k_2-1}\mathtt{w}) & & \\
= h_{k_2-1} + h_{k_2-2} + \min(\eta_{k_2-2}\mathtt{w}) & & \\
= \Sigma_{j=k_1}^{k_2-1} h_j + \min(\eta_{k_1}\mathtt{w}) & & \\
= \min(\eta_{k_1}\mathtt{w}) + h & & \text{recall } h = \Sigma_{j=k_1}^{k_2-1} h_j < 0
\end{array}$$

Thus,

$$\min([\![\mathsf{C} + \mathsf{true}]\!]^{k_2-k_1}\eta_{k_1}\mathtt{w}) = \min(\eta_{k_1}\mathtt{w}) + h$$

Observe that for all $\eta' \sqsupseteq \eta_{k_1}$

$$\min([\![\mathsf{C} + \mathsf{true}]\!]^{k_2-k_1}\eta'\mathtt{w}) \leqslant \min(\eta'\mathtt{w}) + h \tag{A.6}$$

This property (A.6) can be shown by induction on $k_2 - k_1 \geqslant 1$.
Then, an inductive argument allows us to show that for all $r \in \mathbb{N}$:

$$\min([\![\mathsf{C} + \mathsf{true}]\!]^{r(k_2-k_1)}\eta_{k_1}\mathtt{w}) \leqslant \min(\eta_{k_1}\mathtt{w}) + rh \tag{A.7}$$

In fact, for $r = 0$ the claim trivially holds. Assuming the validity for $r \geqslant 0$ then we have that

$$\begin{array}{lll}
\min([\![\mathsf{C} + \mathsf{true}]\!]^{(r+1)(k_2-k_1)}\eta_{k_1}\mathtt{w}) = & & \\
\min([\![\mathsf{C} + \mathsf{true}]\!]^{k_2-k_1}([\![\mathsf{C} + \mathsf{true}]\!]^{r(k_2-k_1)}\eta_{k_1})\mathtt{w}) \leqslant & \text{by (A.6) as } \eta_{k_1} \sqsubseteq [\![\mathsf{C} + \mathsf{true}]\!]^{r(k_2-k_1)}\eta_{k_1} & \\
\min([\![\mathsf{C} + \mathsf{true}]\!]^{r(k_2-k_1)}\eta_{k_1}\mathtt{w}) + h \leqslant & & \text{by inductive hypothesis} \\
\min(\eta_{k_1}\mathtt{w}) + rh + h \leqslant \min(\eta_{k_1}\mathtt{w}) + (r+1)h & &
\end{array}$$

However, This would contradict the hypothesis $[\![\mathsf{fix}(\mathsf{C})]\!]\eta\mathtt{y} \neq -\infty$. In fact the inequality (A.7) would imply

$$\begin{aligned}\min\left([\![\mathsf{fix}(\mathsf{C})]\!]\eta\mathtt{w}\right) &= \min\left(\bigsqcup_{i\in\mathbb{N}} [\![\mathsf{C}+\mathsf{true}]\!]^i\eta\mathtt{w}\right)\\ &= \min\left(\bigsqcup_{i\in\mathbb{N}} [\![\mathsf{C}+\mathsf{true}]\!]^i\eta_{k_1}\mathtt{w}\right)\\ &= \min\left(\bigsqcup_{r\in\mathbb{N}} [\![\mathsf{C}+\mathsf{true}]\!]^{r(k_2-k_1)}\eta_{k_1}\mathtt{w}\right)\\ &= -\infty\end{aligned}$$

Now, from (A.5) we deduce that for all $\eta' \sqsupseteq \eta_{k_1}$, for $j \in \{k_1,\dots,m\}$, if we let $\mu_{k_1} = \eta'$ and $\mu_{j+1} = [\![\mathsf{C}+\mathsf{true}]\!]\mu_j$, we have that $\min(\mu_{j+1}\mathtt{y}_{j+1}) \leqslant \min(\mu_{j+1}\mathtt{y}_j) + h_j$ and thus

$$[\![\mathsf{C}+\mathsf{true}]\!]^{m-k_1+1}\eta'\mathtt{y} = \mu_{m+1}\mathtt{y}_{m+1} \leqslant \min(\mathtt{y}_{k_1}) + \Sigma_{i=k_1}^m h_i = \min(\eta'\mathtt{w}) + \Sigma_{i=k_1}^m h_i$$

Since $\eta' = [\![\mathsf{fix}(\mathsf{C})]\!]\eta \sqsupseteq \eta_{k_1}$ we conclude

$$\begin{aligned}\min([\![\mathsf{fix}(\mathsf{C})]\!]\eta\mathtt{y}) &= \min\left([\![\mathsf{C}+\mathsf{true}]\!]^{m-k_1+1}[\![\mathsf{fix}(\mathsf{C})]\!]\eta\mathtt{y}\right)\\ &\leqslant -\infty + \Sigma_{i=k_1}^m h_i = -\infty\end{aligned}$$

contradicting the assumption. Therefore, the path σ of (A.5) must exist, and consequently

$$\min([\![\mathsf{fix}(\mathsf{C})]\!]\eta\mathtt{y}) = \min(\eta_{m+1}\mathtt{y}) = \min(\eta\mathtt{y}_0) + \Sigma_{i=0}^m h_i$$

and $|\Sigma_{i=0}^m h_i| \leqslant (\mathsf{fix}(\mathsf{C}))_{\mathsf{b}} = (n+1)(\mathsf{C})_{\mathsf{b}}$, otherwise we could use the same argument above for inferring the contradiction $\min([\![\mathsf{fix}(\mathsf{C})]\!]\eta\mathtt{y}) = -\infty$.

Let us now show (ii). Given $\eta' \sqsupseteq \eta$ from (A.5) we deduce that for all $j \in \{0,\dots,m\}$, if we let $\mu_0 = \eta'$ and $\mu_{j+1} = [\![\mathsf{C}+\mathsf{true}]\!]\mu_j$, we have that

$$\min(\mu_{j+1}\mathtt{y}_{j+1}) \leqslant \min(\mu_{j+1}\mathtt{y}_j) + h_j.$$

Therefore, since $[\![\mathsf{fix}(\mathsf{C})]\!]\eta' \sqsupseteq \mu_{m+1}$ (observe that the convergence of $[\![\mathsf{fix}(\mathsf{C})]\!]\eta'$ could be at an index greater than $m+1$), we conclude that:

$$\min([\![\mathsf{fix}(\mathsf{C})]\!]\eta'\mathtt{y}) \leqslant \min(\mu_{m+1}\mathtt{y}) = \min(\mu_{m+1}\mathtt{y}_{m+1}) \leqslant \min(\eta'\mathtt{y}_0) + \Sigma_{i=0}^m h_i$$

as desired. □

A.2 Lemma 4.17 proof

Lemma A.3. *Let* $\mathsf{C} \in \mathsf{Imp}$. *For all* $\eta \in \mathbb{C}$ *and* $\mathtt{y} \in \mathit{Var}$, *if* $\max(\langle\!\langle \mathsf{C} \rangle\!\rangle \eta\mathtt{y}) \neq +\infty$ *and* $\max(\langle\!\langle \mathsf{C} \rangle\!\rangle \eta\mathtt{y}) > (\mathsf{C})_{\mathsf{b}}$ *then there exist a variable* $\mathtt{z} \in \mathit{Var}$ *and an integer* $h \in \mathbb{Z}$ *such that* $|h| \leqslant (\mathsf{C})_{\mathsf{b}}$ *and the following two properties hold:*

(i) $\max(\langle\!\langle \mathsf{C} \rangle\!\rangle \eta\mathtt{y}) = \max(\eta\mathtt{z}) + h$;

(ii) for all $\eta' \in \mathbb{C}$, *if* $\eta' \dot{\sqsupseteq} \eta$ *then* $\max(\langle\!\langle \mathsf{C} \rangle\!\rangle \eta'\mathtt{y}) \geqslant \max(\eta'\mathtt{z}) + h$.

Proof. The proof is by structural induction on the command $\mathsf{C} \in \mathsf{Imp}$. We preliminarily observe that we can safely assume $\eta \neq \bot$. In fact, if $\eta = \bot$ then $\langle\!\langle \mathsf{C} \rangle\!\rangle \bot = \bot$ and thus $\max(\langle\!\langle \mathsf{C} \rangle\!\rangle \eta\mathtt{y}) = -\infty \leqslant (\mathsf{C})_{\mathsf{b}}$, against the hypothesis $\max(\langle\!\langle \mathsf{C} \rangle\!\rangle \eta\mathtt{y}) > (\mathsf{C})_{\mathsf{b}}$. Moreover, when quantifying over η' such that $\eta' \dot{\sqsupseteq} \eta$ in (ii), if $\max(\langle\!\langle \mathsf{C} \rangle\!\rangle \eta'\mathtt{y}) = +\infty$ holds, then $\max(\langle\!\langle \mathsf{C} \rangle\!\rangle \eta'\mathtt{y}) \geqslant \max(\eta'\mathtt{z}) + h$ trivially holds, hence we will sometimes silently omit to consider this case.

Case $(\mathtt{x} \in I)$. Take $\eta \in \mathbb{C}$ and assume $+\infty \neq \max(\langle\!\langle \mathtt{x} \in I \rangle\!\rangle \eta \mathtt{y}) > (\mathtt{x} \in I)^{\mathsf{b}}$. Recall that $I \in \mathbb{I}$. Clearly $\langle\!\langle \mathtt{x} \in I \rangle\!\rangle \eta \neq \bot$, otherwise we would get the contradiction $\max(\langle\!\langle \mathtt{x} \in I \rangle\!\rangle \eta \mathtt{y}) = -\infty \leqslant (\mathtt{x} \in I)^{\mathsf{b}}$. We distinguish two cases:

- If $\mathtt{y} \neq \mathtt{x}$, then for all $\eta' \in \mathbb{C}$ such that $\eta \dot{\subseteq} \eta'$ it holds
$$\bot \neq \langle\!\langle \mathtt{x} \in I \rangle\!\rangle \eta' = \eta'[\mathtt{x} \mapsto \eta' \mathtt{x} \cap \gamma_{\mathbb{I}}(I)]$$
and thus
$$\max(\langle\!\langle \mathtt{x} \in I \rangle\!\rangle \eta' \mathtt{y}) = \max(\eta' \mathtt{y}) = \max(\eta' \mathtt{y}) + 0$$
hence the thesis follows with $\mathtt{z} = \mathtt{y}$ and $h = 0$.
- If $\mathtt{y} = \mathtt{x}$ then
$$\max(\langle\!\langle \mathtt{x} \in I \rangle\!\rangle \eta \mathtt{y}) = \max(\eta \mathtt{x} \cap \gamma_{\mathbb{I}}(I))$$
Note that it cannot be $\max(I) \in \mathbb{Z}$. Otherwise, by Definition 4.2, $\max(\eta \mathtt{x} \cap \gamma_{\mathbb{I}}(I)) \leqslant \max(I) = (\mathtt{x} \in I)^{\mathsf{b}}$, violating the assumption $\max(\langle\!\langle \mathtt{x} \in I \rangle\!\rangle \eta \mathtt{y}) > (\mathtt{x} \in I)^{\mathsf{b}}$. Hence, $\max(I) = +\infty$ must hold and therefore $\max(\eta \mathtt{x} \cap \gamma_{\mathbb{I}}(I)) = \max(\eta(\mathtt{x})) = \max(\eta(\mathtt{x})) + 0$. It is immediate to check that the same holds for all $\eta' \dot{\supseteq} \eta$, i.e.,
$$\max(\eta' \mathtt{x} \cap \gamma_{\mathbb{I}}(I)) = \max(\eta' \mathtt{x}) + 0$$
and thus the thesis follows with $\mathtt{z} = \mathtt{y} = \mathtt{x}$ and $h = 0$.

Case $(\mathtt{x} := k)$. Take $\eta \in \mathbb{C}$ and assume $\max(\langle\!\langle \mathtt{x} := k \rangle\!\rangle \eta \mathtt{y}) > (\mathtt{x} := k)^{\mathsf{b}} = |k|$.

Observe that it cannot be $\mathtt{x} = \mathtt{y}$. In fact, since $\langle\!\langle \mathtt{x} := k \rangle\!\rangle \eta = \eta[\mathtt{x} \mapsto \{k\}]$, we would have $\langle\!\langle \mathtt{x} := k \rangle\!\rangle \eta \mathtt{y} = \{k\}$ and thus
$$\max(\langle\!\langle \mathtt{x} := k \rangle\!\rangle \eta \mathtt{y}) = k \leqslant (\mathtt{x} := k)^{\mathsf{b}}$$
violating the assumption. Therefore, it must be $\mathtt{y} \neq \mathtt{x}$. Now, for all $\eta' \dot{\supseteq} \eta$, we have $\langle\!\langle \mathtt{x} := k \rangle\!\rangle \eta' \mathtt{y} = \eta' \mathtt{y}$ and thus
$$\max(\langle\!\langle \mathtt{x} := k \rangle\!\rangle \eta' \mathtt{y}) = \max(\eta' \mathtt{y}) = \max(\eta' \mathtt{y}) + 0,$$
hence the thesis holds with $h = 0 \leqslant (\mathtt{x} := k)^{\mathsf{b}}$ and $\mathtt{z} = \mathtt{y}$.

Case $(\mathtt{x} := \mathtt{w} + k)$. Take $\eta \in \mathbb{C}$ and assume $\max(\langle\!\langle \mathtt{x} := \mathtt{w} + k \rangle\!\rangle \eta \mathtt{y}) > (\mathtt{x} := \mathtt{w} + k)^{\mathsf{b}} = |k|$. Recall that $\langle\!\langle \mathtt{x} := \mathtt{w} + k \rangle\!\rangle \eta = \eta[\mathtt{x} \mapsto \eta \mathtt{w} + k]$.

We distinguish two cases:

- If $\mathtt{y} \neq \mathtt{x}$, then for all $\eta' \dot{\supseteq} \eta$, we have $\langle\!\langle \mathtt{x} := \mathtt{w} + k \rangle\!\rangle \eta' \mathtt{y} = \eta' \mathtt{y}$ and thus
$$\max(\langle\!\langle \mathtt{x} := \mathtt{w} + k \rangle\!\rangle \eta' \mathtt{y}) = \max(\eta' \mathtt{y})$$
hence the thesis follows with $h = 0 \leqslant (\mathtt{x} := \mathtt{w} + k)^{\mathsf{b}}$ and $\mathtt{z} = \mathtt{y}$.
- If $\mathtt{x} = \mathtt{y}$ then for all $\eta' \dot{\supseteq} \eta$, we have $\langle\!\langle \mathtt{x} := \mathtt{w} + k \rangle\!\rangle \eta' \mathtt{y} = \eta' \mathtt{w} + k$ and thus
$$\max(\langle\!\langle \mathtt{x} := \mathtt{w} + k \rangle\!\rangle \eta' \mathtt{y}) = \max(\eta' \mathtt{w}) + k$$
hence, the thesis follows with $h = k$ (recall that $k \leqslant |k| = (\mathtt{x} := \mathtt{w} + k)^{\mathsf{b}}$) and $\mathtt{z} = \mathtt{w}$.

Case $(\mathsf{C}_1 + \mathsf{C}_2)$. Take $\eta \in \mathbb{C}$ and assume $\max(\langle\!\langle \mathsf{C}_1 + \mathsf{C}_2 \rangle\!\rangle \eta) > (\mathsf{C}_1 + \mathsf{C}_2)^{\mathsf{b}} = (\mathsf{C}_1)^{\mathsf{b}} + (\mathsf{C}_2)^{\mathsf{b}}$. Recall that $\langle\!\langle \mathsf{C}_1 + \mathsf{C}_2 \rangle\!\rangle \eta = \langle\!\langle \mathsf{C}_1 \rangle\!\rangle \eta \dot{\cup} \langle\!\langle \mathsf{C}_2 \rangle\!\rangle \eta$. Hence, since $\max(\langle\!\langle \mathsf{C}_1 + \mathsf{C}_2 \rangle\!\rangle \eta \mathtt{y}) \neq +\infty$, we have that $\max(\langle\!\langle \mathsf{C}_1 \rangle\!\rangle \eta \mathtt{y}) \neq +\infty \neq \max(\langle\!\langle \mathsf{C}_2 \rangle\!\rangle \eta \mathtt{y})$. Moreover
$$\begin{aligned} \max(\langle\!\langle \mathsf{C}_1 + \mathsf{C}_2 \rangle\!\rangle \eta \mathtt{y}) &= \max(\langle\!\langle \mathsf{C}_1 \rangle\!\rangle \eta \mathtt{y} \cup \langle\!\langle \mathsf{C}_2 \rangle\!\rangle \eta \mathtt{y}) \\ &= \max\{\max(\langle\!\langle \mathsf{C}_1 \rangle\!\rangle \eta \mathtt{y}), \max(\langle\!\langle \mathsf{C}_2 \rangle\!\rangle \eta \mathtt{y})\} \end{aligned}$$

Thus $\max(\langle\!\langle \mathsf{C}_1 + \mathsf{C}_2 \rangle\!\rangle \eta \mathtt{y}) = \max(\langle\!\langle \mathsf{C}_i \rangle\!\rangle \eta \mathtt{y})$ for some $i \in \{1, 2\}$. We can assume, without loss of generality, that the maximum is realized by the first component, i.e., $\max(\langle\!\langle \mathsf{C}_1 + \mathsf{C}_2 \rangle\!\rangle \eta \mathtt{y}) = \max(\langle\!\langle \mathsf{C}_1 \rangle\!\rangle \eta \mathtt{y}) > (\mathsf{C}_1 + \mathsf{C}_2)^{\mathsf{b}}$. Hence we can use the inductive hypothesis on C_1 and state that there exists $h \in \mathbb{Z}$ with $|h| \leqslant (\mathsf{C}_1)^{\mathsf{b}}$ and $\mathtt{z} \in \mathit{Var}$ such that $\max(\langle\!\langle \mathsf{C}_1 \rangle\!\rangle \eta \mathtt{y}) = \max(\eta \mathtt{z}) + h$ and for all $\eta' \in \mathbb{C}$, $\eta \dot{\subseteq} \eta'$,

$$\max(\langle\!\langle \mathsf{C}_1 \rangle\!\rangle \eta' \mathtt{y}) \geqslant \max(\eta' \mathtt{z}) + h$$

Therefore

$$\max(\langle\!\langle \mathsf{C}_1 + \mathsf{C}_2 \rangle\!\rangle \eta \mathtt{y}) = \max(\langle\!\langle \mathsf{C}_1 \rangle\!\rangle \eta \mathtt{y}) = \max(\eta \mathtt{z}) + h$$

and and for all $\eta' \in \mathbb{C}$, $\eta \dot{\subseteq} \eta'$,

$$\begin{aligned} \max(\langle\!\langle \mathsf{C}_1 + \mathsf{C}_2 \rangle\!\rangle \eta' \mathtt{y}) &= \max\{\max(\langle\!\langle \mathsf{C}_1 \rangle\!\rangle \eta' \mathtt{y}), \max(\langle\!\langle \mathsf{C}_2 \rangle\!\rangle \eta' \mathtt{y})\} \\ &\geqslant \max(\langle\!\langle \mathsf{C}_1 \rangle\!\rangle \eta' \mathtt{y}) \\ &\geqslant \max(\eta' \mathtt{z}) + h \end{aligned}$$

with $|h| \leqslant (\mathsf{C}_1)^{\mathsf{b}} \leqslant (\mathsf{C}_1 + \mathsf{C}_2)^{\mathsf{b}}$, as desired.

Case $(\mathsf{C}_1; \mathsf{C}_2)$. Take $\eta \in \mathbb{C}$ and assume $\max(\langle\!\langle \mathsf{C}_1; \mathsf{C}_2 \rangle\!\rangle \eta \mathtt{y}) > (\mathsf{C}_1; \mathsf{C}_2)^{\mathsf{b}} = (\mathsf{C}_1)^{\mathsf{b}} + (\mathsf{C}_2)^{\mathsf{b}}$. Recall that $\langle\!\langle \mathsf{C}_1; \mathsf{C}_2 \rangle\!\rangle \eta = \langle\!\langle \mathsf{C}_2 \rangle\!\rangle (\langle\!\langle \mathsf{C}_1 \rangle\!\rangle \eta)$. If we define

$$\langle\!\langle \mathsf{C}_1 \rangle\!\rangle \eta = \eta_1$$

since $\max(\langle\!\langle \mathsf{C}_2 \rangle\!\rangle \eta_1 \mathtt{y}) \neq +\infty$ and $\max(\langle\!\langle \mathsf{C}_2 \rangle\!\rangle \eta_1 \mathtt{y}) > (\mathsf{C}_1; \mathsf{C}_2)^{\mathsf{b}} \geqslant (\mathsf{C}_2)^{\mathsf{b}}$, by inductive hypothesis on C_2, there are $|h_2| \leqslant (\mathsf{C}_2)^{\mathsf{b}}$ and $\mathtt{w} \in \mathit{Var}$ such that $\max(\langle\!\langle \mathsf{C}_2 \rangle\!\rangle \eta_1 \mathtt{y}) = \max(\eta_1 \mathtt{w}) + h_2$ and for all $\eta_1' \in \mathbb{C}$ with $\eta_1 \dot{\subseteq} \eta_1'$

$$\max(\langle\!\langle \mathsf{C}_2 \rangle\!\rangle \eta_1' \mathtt{y}) \geqslant \max(\eta_1' \mathtt{w}) + h_2 \tag{A.8}$$

Now observe that $\max(\langle\!\langle \mathsf{C}_1 \rangle\!\rangle \eta \mathtt{w}) = \max(\eta_1 \mathtt{w}) > (\mathsf{C}_1)^{\mathsf{b}}$. Otherwise, if it were $\max(\eta_1 \mathtt{w}) \leqslant (\mathsf{C}_1)^{\mathsf{b}}$ we would have

$$\max(\langle\!\langle \mathsf{C}_2 \rangle\!\rangle \eta_1 \mathtt{y}) = \max(\eta_1 \mathtt{w}) + h_2 \leqslant (\mathsf{C}_1)^{\mathsf{b}} + (\mathsf{C}_2)^{\mathsf{b}} = (\mathsf{C}_1; \mathsf{C}_2)^{\mathsf{b}},$$

violating the hypotheses. Moreover, $\max(\langle\!\langle \mathsf{C}_1 \rangle\!\rangle \eta \mathtt{w}) \neq +\infty$, otherwise we would have $\max(\langle\!\langle \mathsf{C}_2 \rangle\!\rangle \eta_1 \mathtt{y}) = \max(\eta_1 \mathtt{w}) + h_2 = +\infty$, contradicting the hypotheses. Therefore we can apply the inductive hypothesis also to C_1 and deduce that there are $|h_1| \leqslant (\mathsf{C}_1)^{\mathsf{b}}$ and $\mathtt{w}' \in \mathit{Var}$ such that $\max(\langle\!\langle \mathsf{C}_1 \rangle\!\rangle \eta \mathtt{w}) = \max(\eta \mathtt{w}') + h_1$ and for all $\eta' \in \mathbb{C}$ with $\eta \dot{\subseteq} \eta'$

$$\max(\langle\!\langle \mathsf{C}_1 \rangle\!\rangle \eta' \mathtt{w}) \geqslant \max(\eta' \mathtt{w}') + h_1 \tag{A.9}$$

Summing up:

$$\begin{aligned} \max(\langle\!\langle \mathsf{C}_1; \mathsf{C}_2 \rangle\!\rangle \eta \mathtt{y}) &= \max(\langle\!\langle \mathsf{C}_2 \rangle\!\rangle (\langle\!\langle \mathsf{C}_1 \rangle\!\rangle \eta) \mathtt{y}) \\ &= \max(\langle\!\langle \mathsf{C}_2 \rangle\!\rangle \eta_1 \mathtt{y}) \\ &= \max(\eta_1 \mathtt{w}) + h_2 \\ &= \max(\langle\!\langle \mathsf{C}_1 \rangle\!\rangle \eta \mathtt{w}) + h_2 \\ &= \max(\eta \mathtt{w}') + h_1 + h_2. \end{aligned}$$

Now, for all $\eta' \in \mathbb{C}$ with $\eta \dot{\subseteq} \eta'$ we have that:

$$\begin{aligned} &\max(\langle\!\langle \mathsf{C}_1; \mathsf{C}_2 \rangle\!\rangle \eta' \mathtt{y}) = \\ &\max(\langle\!\langle \mathsf{C}_2 \rangle\!\rangle (\langle\!\langle \mathsf{C}_1 \rangle\!\rangle \eta') \mathtt{y}) \geqslant \\ &\max(\langle\!\langle \mathsf{C}_1 \rangle\!\rangle \eta' \mathtt{w}) + h_2 \geqslant && \text{by (A.8), since } \eta_1 = \langle\!\langle \mathsf{C}_1 \rangle\!\rangle \eta \dot{\subseteq} \langle\!\langle \mathsf{C}_1 \rangle\!\rangle \eta' \text{ and monotonicity} \\ &(\max(\eta' \mathtt{w}') + h_1) + h_2 && \text{by (A.9)} \end{aligned}$$

Thus, the thesis holds with $h = h_1 + h_2$, as $|h| = |h_1 + h_2| \leqslant |h_1| + |h_2| \leqslant (\mathsf{C}_1)^{\mathsf{b}} + (\mathsf{C}_2)^{\mathsf{b}} = (\mathsf{C}_1; \mathsf{C}_2)^{\mathsf{b}}$, as needed.

Case ($\mathsf{fix}(\mathsf{C})$). Let $\eta \in \mathbb{C}$ such that $\max(\langle\!\langle \mathsf{fix}(\mathsf{C}) \rangle\!\rangle \eta \mathtt{y}) \neq +\infty$. Recall that $\langle\!\langle \mathsf{fix}(\mathsf{C}) \rangle\!\rangle \eta = \mathrm{lfp}\left(\lambda\mu.(\langle\!\langle \mathsf{C} \rangle\!\rangle \mu \mathbin{\dot\cup} \eta)\right)$. Observe that the least fixpoint of $\lambda\mu.(\langle\!\langle \mathsf{C} \rangle\!\rangle \mu \dot\cup \eta)$ coincides with the least fixpoint of $\lambda\mu.(\langle\!\langle \mathsf{C} \rangle\!\rangle \mu \dot\cup \mu) = \lambda\mu.\langle\!\langle \mathsf{C} + \mathsf{true} \rangle\!\rangle \mu$ above η. Hence, if

$$\eta_0 \triangleq \eta$$
$$\text{for all } i \in \mathbb{N} \quad \eta_{i+1} \triangleq \langle\!\langle \mathsf{C} \rangle\!\rangle \eta_i \mathbin{\dot\cup} \eta_i = \langle\!\langle \mathsf{C} + \mathsf{true} \rangle\!\rangle \eta_i \mathbin{\dot\supseteq} \eta_i$$

then we define an increasing chain $\{\eta_i\}_{i\in\mathbb{N}} \subseteq \mathbb{C}$ such that

$$\langle\!\langle \mathsf{fix}(\mathsf{C}) \rangle\!\rangle \eta = \dot\bigcup_{i\in\mathbb{N}} \eta_i.$$

Since $\max(\langle\!\langle \mathsf{fix}(\mathsf{C}) \rangle\!\rangle)\eta \mathtt{y} \neq +\infty$, we have that for all $i \in \mathbb{N}$, $\max(\eta_i \mathtt{y}) \neq +\infty$. Moreover, $\dot\bigcup_{i\in\mathbb{N}} \eta_i$ on $\mathtt{y}$ is finitely reached in the chain $\{\eta_i\}_{i\in\mathbb{N}}$, i.e., there exists $m \in \mathbb{N}$ such that for all $i \geqslant m+1$

$$\max(\langle\!\langle \mathsf{fix}(\mathsf{C}) \rangle\!\rangle \eta \mathtt{y}) = \max(\eta_i \mathtt{y}).$$

The inductive hypothesis holds for C and true, hence for $\mathsf{C} + \mathsf{true}$, therefore for all $\mathtt{x} \in \mathit{Var}$ and $j \in \{0, 1, \ldots, m\}$, if $\max(\eta_{j+1}\mathtt{x}) > (\mathsf{C} + \mathsf{true})^{\mathsf{b}} = (\mathsf{C})^{\mathsf{b}}$ then there exist $\mathtt{z} \in \mathit{Var}$ and $h \in \mathbb{Z}$ such that $|h| \leqslant (\mathsf{C})^{\mathsf{b}}$ and

(a) $+\infty \neq \max(\eta_{j+1}\mathtt{x}) = \max(\eta_j \mathtt{z}) + h$,

(b) $\forall \eta' \mathbin{\dot\supseteq} \eta_j . \max(\langle\!\langle \mathsf{C} + \mathsf{true} \rangle\!\rangle \eta' \mathtt{x}) \geqslant \max(\eta' \mathtt{z}) + h$.

To shortly denote that the two conditions (a) and (b) hold, we write

$$(\mathtt{z}, j) \to_h (\mathtt{x}, j+1)$$

Now, assume that for some variable $\mathtt{y} \in \mathit{Var}$

$$\max(\langle\!\langle \mathsf{fix}(\mathsf{C}) \rangle\!\rangle \eta \mathtt{y}) = \max(\eta_{m+1}\mathtt{y}) > (\mathsf{fix}(\mathsf{C}))^{\mathsf{b}} = (n+1)(\mathsf{C})^{\mathsf{b}}$$

where $n = |\mathit{vars}(\mathsf{C})|$. We want to show that the thesis holds, i.e., that there exist $\mathtt{z} \in \mathit{Var}$ and $h \in \mathbb{Z}$ with $|h| \leqslant (\mathsf{fix}(\mathsf{C}))^{\mathsf{b}}$ such that:

$$\max(\langle\!\langle \mathsf{fix}(\mathsf{C}) \rangle\!\rangle \eta \mathtt{y}) = \max(\eta \mathtt{z}) + h \tag{A.10}$$

and for all $\eta' \mathbin{\dot\supseteq} \eta$,

$$\max(\langle\!\langle \mathsf{fix}(\mathsf{C}) \rangle\!\rangle \eta' \mathtt{y}) \geqslant \max(\eta' \mathtt{z}) + h \tag{A.11}$$

Let us consider (A.10). We first observe that we can define a path

$$\sigma \triangleq (\mathtt{y}_0, 0) \to_{h_0} (\mathtt{y}_1, 1) \to_{h_1} \ldots \to_{h_m} (\mathtt{y}_{m+1}, m+1) \tag{A.12}$$

such that $\mathtt{y}_{m+1} = \mathtt{y}$ and for all $j \in \{0, \ldots, m+1\}$, $\mathtt{y}_j \in \mathit{Var}$ and $\max(\eta_j \mathtt{y}_j) > (\mathsf{C})^{\mathsf{b}}$. In fact, if, by contradiction, this were not the case, there would exist an index $i \in \{0, \ldots, m\}$ (as $\max(\eta_{m+1}\mathtt{y}_{m+1}) > (\mathsf{C})^{\mathsf{b}}$ already holds) such that $\max(\eta_i \mathtt{y}_i) \leqslant (\mathsf{C})^{\mathsf{b}}$, while for all $j \in \{i+1, \ldots, m+1\}$, $\max(\eta_j \mathtt{y}_j) > (\mathsf{C})^{\mathsf{b}}$. Thus, in such a case, we consider the nonempty path:

$$\pi \triangleq (\mathtt{y}_i, i) \to_{h_i} (\mathtt{y}_{i+1}, i+1) \to_{h_{i+1}} \ldots \to_{h_m} (\mathtt{y}_{m+1}, m+1) \tag{A.13}$$

and we have that:

$$\begin{aligned}
&\Sigma_{j=i}^{m} h_j = \\
&\Sigma_{j=i}^{m} \max(\eta_{j+1}\mathtt{y}_{j+1}) - \max(\eta_j \mathtt{y}_j) = \\
&\max(\eta_{m+1}\mathtt{y}_{m+1}) - \max(\eta_i \mathtt{y}_i) = \\
&\max(\eta_{m+1}\mathtt{y}) - \max(\eta_i \mathtt{y}_i) > \\
&(n+1)(\mathsf{C})^{\mathsf{b}} - (\mathsf{C})^{\mathsf{b}} = n(\mathsf{C})^{\mathsf{b}}
\end{aligned}$$

with $|h_j| \leqslant (\mathsf{C})^{\mathsf{b}}$ for $j \in \{i, \ldots, m\}$. Hence we can apply Lemma 4.3 to the projection π_p of the nodes of this path π to the variable component to deduce that π_p has a subpath which is a cycle with a strictly positive weight. More precisely, there exist $i \leqslant k_1 < k_2 \leqslant m+1$ such that $\mathtt{y}_{k_1} = \mathtt{y}_{k_2}$ and $h = \Sigma_{j=k_1}^{k_2-1} h_j > 0$. If we denote $\mathtt{w} = \mathtt{y}_{k_1} = \mathtt{y}_{k_2}$, then we have that

$$\begin{aligned}\max(\eta_{k_2}\mathtt{w}) &= h_{k_2-1} + \max(\eta_{k_2-1}\mathtt{w}) \\ &= h_{k_2-1} + h_{k_2-2} + \max(\eta_{k_2-2}\mathtt{w}) \\ &= \Sigma_{j=k_1}^{k_2-1} h_j + \max(\eta_{k_1}\mathtt{w}) \\ &= h + \max(\eta_{k_1}\mathtt{w})\end{aligned}$$

Thus,

$$\max(\langle\!\langle \mathsf{C} + \mathsf{true} \rangle\!\rangle^{k_2-k_1} \eta_{k_1}\mathtt{w}) = \max(\eta_{k_1}\mathtt{w}) + h$$

Observe that for all $\eta' \mathrel{\dot\supseteq} \eta_{k_1}$

$$\max\left(\langle\!\langle \mathsf{C} + \mathsf{true} \rangle\!\rangle^{k_2-k_1} \eta'\mathtt{w}\right) \geqslant \max(\eta'\mathtt{w}) + h \tag{A.14}$$

Let us show that Equation (A.14) holds. We do so by induction on $\ell = k_2 - k_1 \geqslant 1$.

Case ($\ell = 1$). Notice that by (b) used to build π in (A.13) it holds that $\forall \eta' \mathrel{\dot\supseteq} \eta_{k_1} \mathrel{\dot\supseteq} \eta$

$$\max\left(\langle\!\langle \mathsf{C} + \mathsf{true} \rangle\!\rangle \eta'\mathtt{w}\right) \geqslant \max(\eta'\mathtt{w}) + h$$

hence the thesis holds.

Case ($\ell \Rightarrow \ell + 1$). Recall that

$$\left(\langle\!\langle \mathsf{C} + \mathsf{true} \rangle\!\rangle\right)^{\ell+1} \eta' = \left(\langle\!\langle \mathsf{C} + \mathsf{true} \rangle\!\rangle\right) \left(\left(\left(\langle\!\langle \mathsf{C} + \mathsf{true} \rangle\!\rangle\right)^{\ell}\right) \eta'\right)$$

and by inductive hypothesis $\max\left(\left(\langle\!\langle \mathsf{C} + \mathsf{true} \rangle\!\rangle\right)^{\ell} \eta'\mathtt{w}\right) \geqslant \max\left(\eta'\mathtt{w}\right) + h$. Recall that for all $\eta'' \in \mathbb{C}$ we know that $\langle\!\langle \mathsf{C} + \mathsf{true} \rangle\!\rangle \eta'' = \eta'' \mathbin{\dot\cup} \langle\!\langle \mathsf{C} \rangle\!\rangle \eta''$. Hence we can notice that $\max(\langle\!\langle \mathsf{C} + \mathsf{true} \rangle\!\rangle \eta''\mathtt{x}) \geqslant \max(\eta''\mathtt{x})$ for all $\mathtt{x} \in \mathit{Var}$. Therefore

$$\max\left(\langle\!\langle \mathsf{C} + \mathsf{true} \rangle\!\rangle \left(\left(\langle\!\langle \mathsf{C} + \mathsf{true} \rangle\!\rangle\right)^{\ell} \eta'\right) \mathtt{w}\right) \geqslant \max\left(\left(\langle\!\langle \mathsf{C} + \mathsf{true} \rangle\!\rangle\right)^{\ell} \eta'\mathtt{w}\right) \geqslant \max(\eta'\mathtt{w}) + h$$

which is our thesis for Property (A.14).

Then, an inductive argument allows us to show that for all $r \in \mathbb{N}$:

$$\max(\langle\!\langle \mathsf{C} + \mathsf{true} \rangle\!\rangle^{r(k_2-k_1)} \eta_{k_1}\mathtt{w}) \geqslant \max(\eta_{k_1}\mathtt{w}) + rh \tag{A.15}$$

In fact, for $r = 0$ the claim trivially holds. Assuming the validity for $r \geqslant 0$ then we have that

$$\begin{aligned}&\max(\langle\!\langle \mathsf{C} + \mathsf{true} \rangle\!\rangle^{(r+1)(k_2-k_1)} \eta_{k_1}\mathtt{w}) = \\ &\max(\langle\!\langle \mathsf{C} + \mathsf{true} \rangle\!\rangle^{k_2-k_1} (\langle\!\langle \mathsf{C} + \mathsf{true} \rangle\!\rangle^{r(k_2-k_1)} \eta_{k_1})\mathtt{w}) \geqslant \quad \text{by (A.14) as } \eta_{k_1} \mathrel{\dot\subseteq} \langle\!\langle \mathsf{C} + \mathsf{true} \rangle\!\rangle^{r(k_2-k_1)} \eta_{k_1} \\ &\max(\langle\!\langle \mathsf{C} + \mathsf{true} \rangle\!\rangle^{r(k_2-k_1)} \eta_{k_1}\mathtt{w}) + h \geqslant \quad \text{by inductive hypothesis} \\ &\max(\eta_{k_1}\mathtt{w}) + rh + h \geqslant \max(\eta_{k_1}\mathtt{w}) + (r+1)h\end{aligned}$$

However, this would contradict the hypothesis $\langle\!\langle \mathsf{fix}(\mathsf{C}) \rangle\!\rangle \eta\mathtt{y} \neq \infty$. In fact the Inequality (A.15) would imply

$$\begin{aligned}\langle\!\langle \mathsf{fix}(\mathsf{C}) \rangle\!\rangle \eta\mathtt{w} &= \dot{\bigcup}_{i \in \mathbb{N}} \langle\!\langle \mathsf{C} + \mathsf{true} \rangle\!\rangle^{i} \eta\mathtt{w} = \\ &= \dot{\bigcup}_{i \in \mathbb{N}} \langle\!\langle \mathsf{C} + \mathsf{true} \rangle\!\rangle^{i} \eta_{k_1}\mathtt{w} \\ &= \dot{\bigcup}_{r \in \mathbb{N}} \langle\!\langle \mathsf{C} + \mathsf{true} \rangle\!\rangle^{r(k_2-k_1)} \eta_{k_1}\mathtt{w} \\ &= +\infty\end{aligned}$$

Now, from (A.12) we deduce that for all $\eta' \dot{\supseteq} \eta_{k_1}$, for $j \in \{k_1, \dots, m\}$, if we let $\mu_{k_1} = \eta'$ and $\mu_{j+1} = \langle\!\langle \mathsf{C} + \mathsf{true} \rangle\!\rangle \mu_j$, by the choice of the subsequence, since $k_1 \geqslant i$, we have that

$$\max(\mu_{j+1}\mathtt{y}_{j+1}) \geqslant \max(\mu_{j+1}\mathtt{y}_j) + h_j$$

and thus

$$\langle\!\langle \mathsf{C} + \mathsf{true} \rangle\!\rangle^{m-k_1+1} \eta'\mathtt{y} = \mu_{m+1}\mathtt{y}_{m+1} \geqslant \max(\mathtt{y}_{k_1}) + \Sigma_{i=k_1}^{m} h_i = \max(\eta'\mathtt{w}) + \Sigma_{i=k_1}^{m} h_i$$

Since $\eta' = \langle\!\langle \mathsf{fix}(\mathsf{C}) \rangle\!\rangle \eta \dot{\supseteq} \eta_{k_1}$ we conclude

$$\begin{aligned} \max\left(\langle\!\langle \mathsf{fix}(\mathsf{C}) \rangle\!\rangle \eta\mathtt{y}\right) &= \max\left(\langle\!\langle \mathsf{C} + \mathsf{true} \rangle\!\rangle^{m-k_1+1} \langle\!\langle \mathsf{fix}(\mathsf{C}) \rangle\!\rangle \eta\mathtt{w}\right) \\ &= \max\left(\langle\!\langle \mathsf{fix}(\mathsf{C}) \rangle\!\rangle \eta\mathtt{w}\right) + \Sigma_{i=k_1}{}^{m} h_i \\ &\geqslant +\infty + \Sigma_{i=k_1}^{m} h_i = +\infty \end{aligned}$$

contradicting the assumption.

Therefore, the path σ of (A.12) must exist, and consequently

$$\max(\langle\!\langle \mathsf{fix}(\mathsf{C}) \rangle\!\rangle \eta\mathtt{y}) = \max(\eta_{m+1}\mathtt{y}) = \max(\eta\mathtt{y}_0) + \Sigma_{i=0}^{m} h_i$$

and $\Sigma_{i=0}^{m} h_i \leqslant (\mathsf{fix}(\mathsf{C}))^{\mathsf{b}} = (n+1)(\mathsf{C})^{\mathsf{b}}$, otherwise we could use the same argument above for inferring the contradiction $\max(\langle\!\langle \mathsf{fix}(\mathsf{C}) \rangle\!\rangle \eta\mathtt{y}) = +\infty$.

Let us now show (A.11). Given $\eta' \dot{\supseteq} \eta$ from (A.12) we deduce that for all $j \in \{0, \dots, m\}$, if we let $\mu_0 = \eta'$ and $\mu_{j+1} = \langle\!\langle \mathsf{C} + \mathsf{true} \rangle\!\rangle \mu_j$, we have that

$$\max(\mu_{j+1}\mathtt{y}_{j+1}) \geqslant \max(\mu_{j+1}\mathtt{y}_j) + h_j.$$

Therefore, since $\langle\!\langle \mathsf{fix}(\mathsf{C}) \rangle\!\rangle \eta' \dot{\supseteq} \mu_{m+1}$ (observe that the convergence of $\langle\!\langle \mathsf{fix}(\mathsf{C}) \rangle\!\rangle \eta'$ could be at an index greater than $m+1$), we conclude that:

$$\max(\langle\!\langle \mathsf{fix}(\mathsf{C}) \rangle\!\rangle \eta'\mathtt{y}) \geqslant \max(\mu_{m+1}\mathtt{y}) = \max(\mu_{m+1}\mathtt{y}_{m+1}) \geqslant \max(\eta'\mathtt{y}_0) + \Sigma_{i=0}^{m} h_i$$

as desired.

□

Bibliography

[CC77] Patrick Cousot and Radhia Cousot. "Abstract Interpretation: A Unified Lattice Model for Static Analysis of Programs by Construction or Approximation of Fixpoints". In: *Proceedings of the 4th ACM SIGACT-SIGPLAN Symposium on Principles of Programming Languages*. POPL '77. Los Angeles, California: Association for Computing Machinery, 1977, pp. 238–252. ISBN: 9781450373500. DOI: 10.1145/512950.512973. URL: https://doi.org/10.1145/512950.512973 (cit. on pp. iii, 2, 7, 8, 11).

[CC79] Patrick Cousot and Radhia Cousot. "Systematic Design of Program Analysis Frameworks". In: *Proceedings of the 6th ACM SIGACT-SIGPLAN Symposium on Principles of Programming Languages*. POPL '79. San Antonio, Texas: Association for Computing Machinery, 1979, pp. 269–282. ISBN: 9781450373579. DOI: 10.1145/567752.567778. URL: https://doi.org/10.1145/567752.567778 (cit. on pp. 2, 7).

[CC92] Patrick Cousot and Radhia Cousot. "Comparing the Galois connection and widening/-narrowing approaches to abstract interpretation". In: *Programming Language Implementation and Logic Programming*. Ed. by Maurice Bruynooghe and Martin Wirsing. Berlin, Heidelberg: Springer Berlin Heidelberg, 1992, pp. 269–295. ISBN: 978-3-540-47297-1 (cit. on p. 3).

[Cou+05] Patrick Cousot et al. "The ASTREÉ Analyzer". In: *Programming Languages and Systems*. Ed. by Mooly Sagiv. Berlin, Heidelberg: Springer Berlin Heidelberg, 2005, pp. 21–30. ISBN: 978-3-540-31987-0 (cit. on p. 2).

[Cut80] Nigel Cutland. *Computability: An introduction to recursive function theory*. Cambridge university press, 1980 (cit. on pp. 5, 22, 23).

[Dis+19] Dino Distefano et al. "Scaling static analyses at Facebook". In: *Commun. ACM* 62.8 (July 2019), pp. 62–70. ISSN: 0001-0782. DOI: 10.1145/3338112. URL: https://doi.org/10.1145/3338112 (cit. on p. 1).

[Dow97] Mark Dowson. "The Ariane 5 software failure". In: *SIGSOFT Softw. Eng. Notes* 22.2 (Mar. 1997), p. 84. ISSN: 0163-5948. DOI: 10.1145/251880.251992. URL: https://doi.org/10.1145/251880.251992 (cit. on p. 1).

[Eis+89] T. Eisenberg et al. "The Cornell commission: on Morris and the worm". In: *Commun. ACM* 32.6 (June 1989), pp. 706–709. ISSN: 0001-0782. DOI: 10.1145/63526.63530. URL: https://doi.org/10.1145/63526.63530 (cit. on p. 1).

[Gaw+09] Thomas Gawlitza et al. *Polynomial Precise Interval Analysis Revisited*. Ed. by Susanne Albers, Helmut Alt, and Stefan Näher. Berlin, Heidelberg: Springer Berlin Heidelberg, 2009, pp. 422–437. ISBN: 978-3-642-03456-5. DOI: 10.1007/978-3-642-03456-5_28. URL: https://doi.org/10.1007/978-3-642-03456-5_28 (cit. on pp. 3, 55, 65).

[GR22] Roberto Giacobazzi and Francesco Ranzato. "History of Abstract Interpretation". In: *IEEE Annals of the History of Computing* 44.2 (2022), pp. 33–43. DOI: 10.1109/MAHC.2021.3133136 (cit. on p. 7).

[HM08] Tony Hoare and Jay Misra. "Verified Software: Theories, Tools, Experiments Vision of a Grand Challenge Project". In: *Verified Software: Theories, Tools, Experiments: First IFIP TC 2/WG 2.3 Conference, VSTTE 2005, Zurich, Switzerland, October 10-13, 2005, Revised Selected Papers and Discussions*. Ed. by Bertrand Meyer and Jim Woodcock. Berlin, Heidelberg: Springer Berlin Heidelberg, 2008, pp. 1–18. ISBN: 978-3-540-69149-5. DOI: 10.1007/978-3-540-69149-5_1. URL: https://doi.org/10.1007/978-3-540-69149-5_1 (cit. on p. 1).

[JOW06] C. Jones, P. O'Hearn, and J. Woodcock. "Verified software: a grand challenge". In: *Computer* 39.4 (2006), pp. 93–95. DOI: 10.1109/MC.2006.145 (cit. on p. 1).

[Koc+19] Paul Kocher et al. "Spectre Attacks: Exploiting Speculative Execution". In: *40th IEEE Symposium on Security and Privacy*. 2019 (cit. on p. 1).

[Kön26] Dénes König. "Sur les correspondances multivoques des ensembles". In: *Fundamenta Mathematicae* 8 (1926), pp. 114–134. DOI: 10.4064/fm-8-1-114-134 (cit. on p. 27).

[Koz97] Dexter Kozen. "Kleene Algebra with Tests". In: *ACM Trans. Program. Lang. Syst.* 19.3 (May 1997), pp. 427–443. ISSN: 0164-0925. DOI: 10.1145/256167.256195. URL: https://doi.org/10.1145/256167.256195 (cit. on p. 13).

[Lac+98] Ph. Lacan et al. "ARIANE 5 - The Software Reliability Verification Process". In: *DASIA 98 - Data Systems in Aerospace*. Ed. by B. Kaldeich-Schürmann. Vol. 422. ESA Special Publication. July 1998, p. 201 (cit. on p. 1).

[Le 97] G. Le Lann. "An analysis of the Ariane 5 flight 501 failure-a system engineering perspective". In: *Proceedings International Conference and Workshop on Engineering of Computer-Based Systems*. 1997, pp. 339–346. DOI: 10.1109/ECBS.1997.581900 (cit. on p. 1).

[Lef+24] Engel Lefaucheux et al. "Porous invariants for linear systems". In: *Formal Methods in System Design* (Feb. 2024). ISSN: 1572-8102. DOI: 10.1007/s10703-024-00444-3. URL: https://doi.org/10.1007/s10703-024-00444-3 (cit. on p. 58).

[Lip+18] Moritz Lipp et al. "Meltdown: Reading Kernel Memory from User Space". In: *27th USENIX Security Symposium (USENIX Security 18)*. 2018 (cit. on p. 1).

[Min18] Antonie Miné. *Static Inference of Numeric Invariants by Abstract Interpretation*. Université Pierre et Marie Curie, Paris, France, 2018 (cit. on pp. 6, 7).

[MOM23] Raphaël Monat, Abdelraouf Ouadjaout, and Antoine Miné. "Mopsa-C: Modular Domains and Relational Abstract Interpretation for C Programs (Competition Contribution)". In: *Tools and Algorithms for the Construction and Analysis of Systems*. Ed. by Sriram Sankaranarayanan and Natasha Sharygina. Cham: Springer Nature Switzerland, 2023, pp. 565–570. ISBN: 978-3-031-30820-8 (cit. on p. 2).

[OHe19] Peter W. O'Hearn. "Incorrectness logic". In: *Proc. ACM Program. Lang.* 4.POPL (Dec. 2019). DOI: 10.1145/3371078. URL: https://doi.org/10.1145/3371078 (cit. on p. 1).

[Orm03] H. Orman. "The Morris worm: a fifteen-year perspective". In: *IEEE Security & Privacy* 1.5 (2003), pp. 35–43. DOI: 10.1109/MSECP.2003.1236233 (cit. on p. 1).

[Ric53] Henry Gordon Rice. "Classes of recursively enumerable sets and their decision problems". In: *Transactions of the American Mathematical society* 74.2 (1953), pp. 358–366 (cit. on pp. 1, 25).

[See89] Donn Seeley. "A Tour of the Worm". In: *Proceedings of 1989 Winter USENIX Conference, Usenix Association, San Diego, CA, February*. 1989 (cit. on p. 1).

[Spa89] Eugene H. Spafford. "The internet worm program: an analysis". In: *SIGCOMM Comput. Commun. Rev.* 19.1 (Jan. 1989), pp. 17–57. ISSN: 0146-4833. DOI: 10.1145/66093.66095. URL: https://doi.org/10.1145/66093.66095 (cit. on p. 1).

[SW05] Zhendong Su and David Wagner. "A class of polynomially solvable range constraints for interval analysis without widenings". In: *Theoretical Computer Science* 345.1 (2005). Tools and Algorithms for the Construction and Analysis of Systems (TACAS 2004), pp. 122–138. ISSN: 0304-3975. DOI: https://doi.org/10.1016/j.tcs.2005.07.035. URL: https://www.sciencedirect.com/science/article/pii/S0304397505003889 (cit. on p. 3).

[Tar55] Alfred Tarski. "A lattice-theoretical fixpoint theorem and its applications." In: (1955) (cit. on p. 7).

[Tur21] Alan Mathison Turing. "On Computable Numbers, with an Application to the Entscheidungsproblem (1936)". In: *Ideas That Created the Future: Classic Papers of Computer Science*. The MIT Press, Feb. 2021. ISBN: 9780262363174. DOI: 10.7551/mitpress/12274.003.0008. eprint: https://direct.mit.edu/book/chapter-pdf/2248314/9780262363174_c000500.pdf. URL: https://doi.org/10.7551/mitpress/12274.003.0008 (cit. on p. 1).

[Woo06] J. Woodcock. "First Steps in the Verified Software Grand Challenge". In: *Computer* 39.10 (2006), pp. 57–64. DOI: 10.1109/MC.2006.340 (cit. on p. 1).