Type Systems for Resource Use in Component Software

Dag Hovland

December 12, 2006

Type Systems for Resource Use in Component Software. Thesis for the master degree, Institutt for Informatikk, University of Bergen.

Acknowledgements

My advisor during the work on this thesis has been Marc Bezem. I must thank him for being inspiring and helpful. I want to thank Hoang Truong for interesting discussions and articles. I also want to thank Institutt for Informatikk at University of Bergen and Facultat d'Informàtica de Barcelona for making the exchange to Barcelona during the last year of my master possible.

Contents

Chapter 1

Introduction

1.1 Resource Usage

In many situations a programmer must be concerned with resources which are not accounted and controlled completely by the programming language. These could be external physical resources, like a printer or a screen, it could be more abstract physical resources, like computing time, memory usage, or writing some file to disk or it could be other software components or programs. The resources can be used directly by the program, or indirectly, through the use of libraries or other software. An important property of these resources is their externally, often physically, enforced limits, which are independent of program execution.

Finding maximum and minimum number of active or used instances of these resources at some point during execution can be difficult and demand time from both programmer and computer. But this can also be important for safe execution. As a silly example, a program which every minute allocates, but fails to deallocate, 1 byte of memory, will at some point fail, while runtime testing might not reveal this before it is run for a week. Many of the new mobile and low-cost devices (e.g. the hundred dollar laptop http://laptop.org) would probably also benefit from provable upper limits on the usage of some resources, like writing to the disk or memory.

Developing static systems for finding some of these limits, is the goal in which this thesis hopes to take part. With "static" I mean systems which analyse the source code, not the execution of the compiled program.

Example. Runtime checking is always an alternative to static analysis. For an example of the difficulties that could be involved in this, I will refer the reader to Dave Jones' text "Why Userspace Sucks - (Or, 101 Really Dumb Things Your App Shouldn't Do)" held at Ottawa Linux Symposium 2006 [6]. As users of the GNU/Linux operating system will be aware, the time from switching on a system until it is fully operational is longer than for many other operating systems. One of the reasons for this seems to be that many of the startup scripts and programs use more resources than necessary - the same XML file can be parsed hundred or thousands of times - unnecessary hardware is probed etc. For his analysis Jones had to patch the kernel and connect a serial console to the computer. This is time-consuming and requires a high level of competence.

There seems to be no good tools to analyse this situation statically, which would be possible as the source code of all the programs is readily available.

Existing tools. For languages like C, the static tools that exist mostly look after misuse of functions or interfaces. An error-checking compiler like gcc [4] (with warnings turned on) and splint [8] are some of the very few tools freely available. There is also done research on statically detecting string buffer overruns in C [14].

The alternative to a static checking is of course running the program, or, for some properties, using a "dynamic" tool, which checks for some properties during running. Widely used examples are "Valgrind" [10] and "D.U.M.A" [3].

Resource dependencies. Allocation of one resource can depend on allocation of other resources. Every time an instance of the depending resource is allocated there will also be allocated the necessary instances of the resources it depends on. As an example, starting a printer service requires, among other resources, opening and reading some global configuration files, and for each printer, opening and reading the postscript printer driver. If opening and reading one file is seen as a resource, then the "cups" resource would depend on several instances of this "open file" resource.

The model. The systems in this thesis are concerned with "components" which can be allocated, created or instantiated in some manner, and also be removed, deleted or deinstantiated. These two operations are called new and del. There is a set of component names, and components of the same name are identified. There can be different limits to the maximum number of concurrently existing instances of each component. It is an error trying to deallocate or delete a component when there are no instances of this component left, or trying to instantiate a component, when the maximum limit is reached. There is no exception- or error-handling. The dependency on other components is modelled by letting the declarations of all components be the first part of any program, and every call to new will execute the expression in the declaration of the component. Limited resources would in many cases be modelled as a "primitive component", that is, a component with an empty declaration, while more complex resource usage or libraries (like cups in the example above) will often have non-empty declarations.

The different limits on the number of instantiated components will be inferred as a type of the expression, therefore the name "Typed Resource Usage".

Previous work. Marc Bezem and Hoang Truong have described similar systems in several texts: [2], [11], [12] and [13]. Haakon Nilsen has implemented the type inference with the program "comp" [7].

1.2 New and old

The second chapter, the main part of this thesis, is based on a modification of a system in Hoang Truongs thesis "Type Systems for Guaranteeing Resource Bounds of Component Software" [13]. Many of the lemmas and theorems have

formulations and proofs which are similar, while others are new. I will in this section try to indicate what is new and what is more similar to Hoangs chapter. This section is probably only interesting to those evaluating the work behind this thesis. All proofs are written from scratch, but especially in the case of the typing properties, the proofs are quite similar, although with some subtle, but important differences.

Apart from the changes discussed in the introduction (removal of choice and scope), the language is similar, but the general formulation and the treatment of the empty string is somewhat different. The formulation of the operational semantics is also new, as there is only one global store, and not local stores in each node and leaf. The formal definition of a run (definition 2.2.1) is new. The type system is changed in that σ is moved into the type as X^n. Also, the parallel rule is changed as according to the new semantics.

Valid typing judgement (lemma 2.4.2) is changed to fit a system without choice. Strengthening (lemma 2.4.6) has one added clause, which is new here. Uniqueness of types is somewhat stronger, as the bases do not need to be equal. This is usefule for type inference. The whole section on configuration properties is new. The invariance lemma (lemma 2.4.15) is different, and the sharpness lemma (2.4.20) is new.

As mentioned, there are many similarities in the proofs of typing properties, but especially the proofs of the generation lemma (2.5.3) and of uniqueness of types (2.5.6) is new. The proof of strengthening 2 (2.5.5) and all the proofs of configuration properties are of course new. Most of the soundness properties have also new proofs, as the invariant lemma (2.4.15) is different, although the last three, especially soundness (2.7.5) are similar. The proof of termination (2.9.1) is new.

The last chapters contain new proofs of new lemmas concerning sharpness in some chapters of Truongs thesis. In addition, lemmas 3.1.8, 4.3.2, 5.3.1 and 6.3.1 are new, and in some way an extension of soundness. Except for the repetition of some of the properties of the system, these chapters are new.

Chapter 2

Global Resources

2.1 Introduction

The system described in this text is a modified version of the one found in chapter 4 "Explicit Deallocation and Parallel Composition" in Hoang Truongs thesis [13]. The language does not contain choice (+) and scope ({}), which are present in Truongs chapter. Although I am aiming to make this text self-contained, it is recommended to read at least chapter two of Hoangs thesis before reading this text, as it describes a simpler system. If you have not read it, please skip this section ("Introduction"), as it mainly concerns the differences between the two texts.

The main change from [13] is an altered semantics of parallel composition. The goal is to let components be shared between the threads of parallel execution. This does create some new problems. For instance, $(\mathsf{new}x \cdot ||\mathsf{del}x\cdot)\cdot$ should not be run on empty store, even though one of the possible runs would actually be okay. This is because I want to allow a parallel composition where we cannot know or control which of the two operations will run first. This problem is also known as scheduling.

On the other hand, the expression $\mathsf{new}x \cdot \mathsf{new}x \cdot (\mathsf{del}x \cdot ||\mathsf{del}x\cdot)\cdot$ can be run from an empty store in this system, while it would create an error if it was run in [13], as there each thread has its own store, which starts out being empty.

The model is somewhat closer to the situation seen in shared memory programming. But note that the general problem including controlling the contents and the access to the contents of the memory will not be handled. This is vital for shared memory programming in general, but in this text I am only concerned with the total amount claimed of the given component (e.g. memory), and not that it is accessed properly. Accordingly, there is in this language no way to actually use the components, only to claim and release them.

As mentioned above, scope (push and pop) is not treated. The changes to the semantics of parallel are to give components a more "global" nature, which the scope operator would remove again. The environment has one global store for instances of components. If expression E has type $X = \langle X^n, X^p, X^a \rangle$, then X^n is the highest possible negative change to the store during execution of E, X^p is the highest possible positive change to the store during execution and X^a is the net change to the store measured after E is executed. (While X^n replaces

the store (σ), X^p replaces X^i and X^a replaces X^o and X^l).

While the maximum negative and positive change during a run depend on the exact scheduling, this is not true of the net change after the run, which in this system is the same for any run and independent of the scheduling.

2.2 Language

The language is defined by a context-free grammar, as defined in "Introduction to automata theory, languages and computation" [5]. The language is parameterised over some non-empty set of component names. In the grammar below "x" will indicate some element from this set.

$$\begin{array}{rcl} Prog & \rightarrow & Decls; Expr \\ Decls & \rightarrow & x \prec Expr \\ & | & x \prec Expr, Decls \\ Expr & \rightarrow & Oper \cdot Expr \\ & | & \epsilon \\ Oper & \rightarrow & \mathsf{new}\, x \\ & | & \mathsf{del}\, x \\ & | & (Expr \,||\, Expr) \end{array} \tag{2.1}$$

A program in $L(Prog)$ is a list of declarations from $L(Decls)$ followed by a single expression from $L(Expr)$. This last expression is the expression which starts the execution, while the declarations are called upon when instantiating a component with new during the run. ϵ is here the empty string, not a blank. The "$\cdot$" is an expression separator somewhat akin to the semicolon in C.

The grammar rule for $Expr$ is split in two - one for sequencing and a second rule for each $Oper$ in the expression. This makes the grammar $Expr$ unambiguous. But it is no longer as obvious as in [13] that $L(Expr)$ is closed under concatenation.

2.2.1 $Prog$ is unambiguous

From the first rule in the grammar we see that there is only one possible combination of a word from $L(Expr)$ and $L(Decls)$ creating a word in $L(Prog)$. That $Expr$ is unambiguous will be proved by induction on the derivation of a word $E \in L(Expr)$. The inductive hypothesis is: *for any shorter word E it is the case that there is only one leftmost derivation of E.* The base case is $E = \epsilon$, which has only one derivation $Expr \Rightarrow \epsilon$. The inductive case is $E = O \cdot E'$ for some E' and $O \in L(Oper)$. There are three possibilities for O: new$x$, del$x$ or $(E_1||E_2)$ for some E_1 and E_2. The next step in a leftmost derivation is accordingly one of:

- $Oper \cdot Expr \Rightarrow \mathsf{new}x \cdot Expr$. (If $O = \mathsf{new}x$).
- $Oper \cdot Expr \Rightarrow \mathsf{del}x \cdot Expr$. (If $O = \mathsf{del}x$).
- $Oper \cdot Expr \Rightarrow (Expr||Expr) \cdot Expr$. (If $O = (E_1||E_2)$).

In all cases there is no other possible step at this stage. In the first and second cases, the unique leftmost derivation of E' follows. In the third case, first comes the steps from the derivation of E_1, then from E_2 and last from E'. All three have unique leftmost derivations by the inductive hypothesis, so the rest of the derivation is also unique.

Finally, it should not be difficult to see that $L(Decls)$ is unambiguous: Do an induction on the length of the list of declarations: The base case is the single declaration $x \prec E$ which has a unique leftmost derivation by the unambiguity of $Expr$. The inductive case is a word which is not a single declaration. The first rule used must then be an application of $Decls \to x \prec E, Decls$ and the steps after this are given by the argument given for the base case and the inductive hypothesis on $Decls$. □

2.2.2 $L(Expr)$ is closed under concatenation

Let $w_1, w_2 \in L(Expr)$. I must show that $w = w_1 w_2 \in L(Expr)$. If $w_1 = \epsilon$, we have $w = w_2$ and this word is in $L(Expr)$ by the assumption. I will therefore assume $w_1 \neq \epsilon$. Assume the leftmost derivations of w_1 and w_2 look like this (where $n \geq 1$):

$$E \Rightarrow Oper \cdot Expr \Rightarrow f_1 \cdot Expr \Rightarrow^* f_1 \cdot \ldots \cdot f_n \cdot Expr \Rightarrow f_1 \cdot \ldots f_n \cdot = w_1 \quad (2.2)$$

$$Expr \Rightarrow^* w_2 \quad (2.3)$$

If we remove the last step in the derivation of w_1 (2.2) and instead use the $Expr$ to derive w_2 as in 2.3 we get a derivation of w:

$$\begin{aligned} Expr &\Rightarrow Oper \cdot Expr \\ &\Rightarrow f_1 \cdot Expr \\ &\Rightarrow^* f_1 \cdot \ldots \cdot f_m \cdot Expr \\ &\Rightarrow^* f_1 \cdot \ldots \cdot f_m \cdot w_2 = w_1 w_2 = w \end{aligned}$$

Since we can derive w from $Expr$ we must have $w \in L(Expr)$. □

I will from now on use $Prog$ meaning some word in $L(Prog)$, capital Roman letters from the beginning of the alphabet $(A, B, C, \ldots)$ meaning some word in $L(Expr)$ and $Decls$ some word in $L(Decls)$. I will also use extensively $E\cdot$ for a word in $L(Expr) - \{\epsilon\}$. The intuition is that an expression ending in $\cdot$ cannot be the empty word.

2.2.3 Operational semantics

Configurations. Before embarking on the configurations and transition rules, I will introduce the hybrid set, a generalisation of multisets. The name is taken from "Mathematics of Multisets", Apostolos Syropolous [9]. A hybrid set is a mapping from some universe, in this context, the component names, to the integers, $\mathcal{Z}$. If A and B are hybrid sets over the set of component names, call

this set Σ, we have some of the properties below:

$$\begin{aligned} A \subseteq B &\Leftrightarrow \forall x \in \Sigma : A(x) \leq B(x) \\ A = B &\Leftrightarrow A \subseteq B \wedge B \subseteq A \\ (A + B)(x) &= A(x) + B(x) \\ (A - B)(x) &= A(x) - B(x) \\ (A \cup B)(x) &= \max(A(x), B(x)) \\ (A \cap B)(x) &= \min(A(x), B(x)) \\ A(x) = 0 &\Leftrightarrow x \notin A \end{aligned}$$

In words, an element is said to be in a hybrid set if it is not mapped to 0. A union of two hybrid sets maps the elements to the maximum of what the two sets map them to. A sum of two hybrid sets maps the elements to the sum of what they were mapped to in the two hybrid sets. In the other texts, there has been a differentiation between signed and unsigned multisets. I will in this text use hybrid sets for both cases, but argue for or require that the set only maps to a subset of $\mathcal{Z}$ in certain cases. This is meant to simplify the arguments.

I will use a different notation than in [9]. I will write $[x_1 \mapsto c_1, \cdots, x_n \mapsto c_n]$ for a hybrid set where for all i, where $1 \leq i \leq n$, we have x_i is mapped to integer c_i, and all other components are mapped to 0. I will also use two abbreviations: if x is some component name, then the name itself "x" is short for "$x \mapsto 1$" and for $[x \mapsto 1]$, such that $x = [x] = [x \mapsto 1]$ and "$-x$" is short for "$x \mapsto -1$", such that $[-x] = [x \mapsto -1]$. It will be clear from the context when "x" is a component name, and when it is a hybrid set.

The operational semantics is defined by small-step transitions between "configurations". A configuration is a pair $(M, \mathbb{T})$, where M is a hybrid set of component names and $\mathbb{T}$ is a tree of expressions as defined below. Since the only rule that deletes components osDel, has as prerequisite that M contains an instance of the component, we have that M only maps components to non-negative numbers. A configuration models a state of the system.

$\mathbb{T}$	$\rightarrow$		tree
		$\mathsf{Lf}(Expr)$	Leaf
	$\mid$	$\mathsf{Nd}(Expr, \mathbb{T})$	Node with one branch
	$\mid$	$\mathsf{Nd}(Expr, \mathbb{T}, \mathbb{T})$	Node with two branches

- We use $\mathbb{T}, \mathbb{T}', \ldots$ and $\mathbb{R}, \mathbb{R}', \ldots$ as variables for trees.
- A location in the tree is described by a sequence of c, l, r with $\bullet$ for the root. c is used in the case of a node with a single child, while l and r are used for the left and the right child, respectively, in the case of a node with two children.
- By $\mathbb{T}(\alpha)$ I mean the expression in the node or leaf at location α.
- $\mathbb{T}[\mathbb{T}']_\alpha$ means a tree $\mathbb{T}$ with a hole in the position α replaced by $\mathbb{T}'$. For example, in the rules (osNew) and (osDel) below, this means that the rule can be applied to any leaf.
- By $\mathbb{T}_\alpha$ I mean the subtree rooted in α, such that $\mathbb{T}[\mathbb{T}_\alpha]_\alpha = \mathbb{T}$.

Transition rules. The allowed transitions in the operational semantics are given in two lines each. The first line consists of the name in parenthesis and then any conditions. The second line has the start of the transition on the left, an arrow and then the end point of the transition:

$$\begin{array}{l}(\mathsf{osNew}) \quad \text{if } x \prec A \in \mathit{Decls} \text{ and } M(x) < R(x) \\ (M, \mathbb{T}[\mathsf{Lf}(\text{new } x \cdot E)]_\alpha) \longrightarrow (M + x, \mathbb{T}[\mathsf{Lf}(AE)]_\alpha)\end{array}$$

$$\begin{array}{l}(\mathsf{osDel}) \quad x \in M \\ (M, \mathbb{T}[\mathsf{Lf}(\text{del } x \cdot E)]_\alpha) \longrightarrow (M - x, \mathbb{T}[\mathsf{Lf}(E)]_\alpha)\end{array}$$

$$\begin{array}{l}(\mathsf{osParIntr}) \\ (M, \mathbb{T}[\mathsf{Lf}((A \,||\, B) \cdot E)]_\alpha) \longrightarrow (M, \mathbb{T}[\mathsf{Nd}(E, \mathsf{Lf}(A), \mathsf{Lf}(B))]_\alpha)\end{array}$$

$$\begin{array}{l}(\mathsf{osParElimL}) \\ (M, \mathbb{T}[\mathsf{Nd}(E, \mathsf{Lf}(\epsilon), \mathbb{R}))]_\alpha) \longrightarrow (M, \mathbb{T}[\mathsf{Nd}(E, \mathbb{R})]_\alpha)\end{array}$$

$$\begin{array}{l}(\mathsf{osParElimR}) \\ (M, \mathbb{T}[\mathsf{Nd}(E, \mathbb{R}, \mathsf{Lf}(\epsilon))]_\alpha) \longrightarrow (M, \mathbb{T}[\mathsf{Nd}(E, \mathbb{R})]_\alpha)\end{array}$$

$$\begin{array}{l}(\mathsf{osParElim}) \\ (M, \mathbb{T}[\mathsf{Nd}(E, \mathsf{Lf}(\epsilon))]_\alpha) \longrightarrow (M, \mathbb{T}[\mathsf{Lf}(E)]_\alpha)\end{array}$$

Explanation of the rules. The osNew rule is used when instantiating a component. It first adds the component to the store, and then runs the expression in the declaration. Note that since A and E are in $L(Expr)$ by assumption, then the concatenation AE is also in $L(Expr)$. In the case where $A = \epsilon$, x is called a *primitive component*, and we then have $AE = E$. $\mathcal{R}$ is as in chapter 5 in [13] a restriction on the maximal number of a given component - a mapping from component names to $(\mathcal{N} - \{0\}) \cup \infty$. osDel deletes one instance of a component, and does not use the declaration. The remaining four rules control parallel execution. Note that the parallel execution is only parallel between the two newly started threads. The expression remaining in the parent node remains unchanged until the expressions in both leafs are terminated.

I will now give a definition of the "run" of an expression. This is mainly used for the sharpness lemma, 2.4.20, but is included here to give an impression of what a run is. You may skip this now, and return to it when getting to the sharpness lemma.

Definition 2.2.1 (Run of an expression). *A run of an expression E on position α in context $\mathbb{T}$, is a sequence of configurations, where*

- *E is the first part of the expression in a leaf in the tree in the first configuration in the sequence. That is, the first configuration is of the form $(M, \mathbb{T}[\mathsf{Lf}(EE')]_\alpha)$, where M is some store, E' some expression, $\mathbb{T}$ is the context and α the position.*

- *In any pair of two consecutive configurations the last is formed from the first using one of the rules in the operational semantics. Also, only transitions on positions of the form $\alpha\beta$ are allowed, that is, α or any positions below it. This means they have the following form:*

$$(M^i, \mathbb{T}^i) = (M^i, \mathbb{T}^i[\mathbb{R}^i]_{\alpha\beta}) \to (M^{i+1}, \mathbb{T}^i[\mathbb{R}^{i+1}]_{\alpha\beta}) = (M^{i+1}, \mathbb{T}^{i+1})$$

  where $\mathbb{R}^i$ and $\mathbb{R}^{i+1}$ are leaves or nodes depending on which rule is used.

- *The length of the run is the number of configurations minus one, that is, the number of applications of the rules from the operational semantics.*

- *The last configuration is of the form $(M', \mathbb{T}[\mathsf{Lf}(E')]_\alpha)$.*

□

I will often omit the context or the position, writing only "a run of E". This will then express a run in any context and any position within that context.

2.2.4 Example expression

As an example program I will use $x \prec \epsilon\,,\ y \prec \mathsf{new}\,x\cdot; (\mathsf{new}x\cdot\mathsf{del}x\cdot||\mathsf{new}y\cdot)\cdot\mathsf{new}x\cdot$. If we run the "main" expression starting from an empty store, the first transition in a run of it will be an instance of osParIntr:

$$\begin{array}{l}([], \mathsf{Lf}((\mathsf{new}x\cdot\ \mathsf{del}x\cdot||\mathsf{new}y\cdot)\cdot\mathsf{new}x\cdot)\\ \to ([], \mathsf{Nd}(\mathsf{new}x\cdot, \mathsf{Lf}(\mathsf{new}x\cdot\ \mathsf{del}x\cdot), \mathsf{Lf}(\mathsf{new}y\cdot))\end{array}$$

For the next step I can choose to take the left or the right leaf first. I show now one possibility for the rest of the run. The names of the transitions are on the left.

$$\begin{array}{r|l}
 & ([], \mathsf{Nd}(\mathsf{new}x\cdot, \mathsf{Lf}(\mathsf{new}x\cdot\ \mathsf{del}x\cdot), \mathsf{Lf}(\mathsf{new}y\cdot))\\
(\mathsf{osNew}) & \to ([x], \mathsf{Nd}(\mathsf{new}x\cdot, \mathsf{Lf}(\mathsf{del}x\cdot), \mathsf{Lf}(\mathsf{new}y\cdot))\\
(\mathsf{osNew}) & \to ([x,y], \mathsf{Nd}(\mathsf{new}x\cdot, \mathsf{Lf}(\mathsf{del}x\cdot), \mathsf{Lf}(\mathsf{new}x\cdot))\\
(\mathsf{osNew}) & \to ([x\mapsto 2, y], \mathsf{Nd}(\mathsf{new}x\cdot, \mathsf{Lf}(\mathsf{del}x\cdot), \mathsf{Lf}(\epsilon))\\
(\mathsf{osParElimR}) & \to ([x\mapsto 2, y], \mathsf{Nd}(\mathsf{new}x\cdot, \mathsf{Lf}(\mathsf{del}x\cdot))\\
(\mathsf{osDel}) & \to ([x,y], \mathsf{Nd}(\mathsf{new}x\cdot, \mathsf{Lf}(\epsilon))\\
(\mathsf{osParElim}) & \to ([x,y], \mathsf{Lf}(\mathsf{new}x\cdot)\\
(\mathsf{osNew}) & \to ([x\mapsto 2, y], \mathsf{Lf}(\epsilon)
\end{array}$$

I end up with a net increase in x with two and in y with one, and this is also the maximum any of them reach in this run.

Now, if I change the expression by moving the last $\mathsf{new}\,x$ into the right branch of the parallel, I get the following program:

$$x \prec \epsilon\,,\ y \prec \mathsf{new}\,x\cdot\,;\ (\mathsf{new}x\cdot\ \mathsf{del}x\cdot||\mathsf{new}y\cdot\mathsf{new}x\cdot)\cdot$$

It looks almost the same, but this program has a run reaching a maximum of three numbers of the component x in the store. The size of the store after the run is the same for any run of the two programs.

2.3 Type system

A requirement $\mathcal{R}$ is used as in chapter 5 in [13] — a hybrid set with the restriction that only positive values can be mapped to, that is, $\mathcal{R} \supset []$. But because of the global nature of the store, the requirement is not a part of the typing judgement, but of a well-formed configuration.

Types are tuples $X = \langle X^n, X^p, X^a \rangle$ of hybrid sets. X^a represents the net change in the number of instances from before to after execution of the expression. X^n represents the largest negative change to the store. So $X^n(x)$ is the number of components that must be in the store before execution to prevent it to get stuck. X^p represents the largest positive possible change to the store during execution. The number of instances of component x in the store added to $X^p(x)$ must not exceed $\mathcal{R}(x)$ for any component x to prevent the execution from getting stuck because of too many copies of the component being used. In valid typing judgement, lemma 2.4.2 I will show that $X^p \supseteq []$ and $X^n \supseteq []$, that is, these hybrid sets only map to non-negative numbers. A typing judgement is of the form $\Gamma \vdash E : X$, where Γ is a basis, as defined later in definition 2.3.1.

As mentioned after the "language" section, I will use "$A\cdot$" to mean some non-empty expression, and the intuition is that an expression ending in "$\cdot$" cannot be empty.

2.3.1 Typing rules

$$\frac{\Gamma \vdash A : X \qquad x \prec A \in \Gamma}{\Gamma \vdash \mathsf{del}\, x\cdot : \langle [x], [], [-x] \rangle}\ (\textsc{Del}) \qquad \frac{\Gamma \vdash A : X \qquad \Gamma \vdash B : Y \quad x \notin \mathsf{dom}(\Gamma)}{\Gamma, x \prec B \vdash A : X}\ (\textsc{WeakenB})$$

$$\frac{\Gamma \vdash A : X \quad x \notin \mathsf{dom}(\Gamma)}{\Gamma, x \prec A \vdash \mathsf{new}\, x\cdot : \langle X^n, X^p + x, X^a + x \rangle}\ (\textsc{New}) \qquad \frac{\Gamma \vdash A : X \qquad \Gamma \vdash B : Y}{\Gamma \vdash (A \,||\, B)\cdot : X + Y}\ (\textsc{Parallel})$$

$$\frac{}{\oslash \vdash \epsilon : \langle [], [], [] \rangle}\ (\textsc{Axiom}) \qquad \frac{\Gamma \vdash A\cdot : X \qquad \Gamma \vdash B\cdot : Y}{\Gamma \vdash A \cdot B\cdot : \langle X^n \cup (Y^n - X^a), X^p \cup (X^a + Y^p), X^a + Y^a \rangle}\ (\textsc{Seq})$$

An important part of a typing judgement is the "basis". The basis is a reordering of a subset of the declarations in *Decls*.

Definition 2.3.1 (Basis). *Let $\Gamma = x_1 \prec A_1, ..., x_n \prec A_n$ be a basis*

- *Γ is called legal if $\Gamma \vdash A : X$ for some expression A and type X.*
- *A declaration $x \prec A$ is in Γ, notation $x \prec A \in \Gamma$, if $x = x_i$ and $A = A_i$ for some i*
- *Δ is an initial segment of Γ, if $\Delta = x_1 \prec A_1, ..., x_j \prec A_j$ for some $1 \leq j \leq n$.*
- *The domain of Γ, notation $\mathsf{dom}(\Gamma)$, is the set $\{x_1, \ldots, x_n\}$.*

A typing judgement is in itself not a guarantee that the expression can run without errors. Since expressions are local in each node, while the store is global, there must be a global comparison between all types and the store. An

expression E with type $\langle Z^n, Z^p, Z^a \rangle$ is safe to execute (starting from an empty store) if

$$\oslash \subseteq -Z^n \subseteq Z^p \subseteq \mathcal{R}$$

Since $Z^n \supseteq []$, the leftmost inclusion means that Z^n must be empty ($Z^n = []$). It is written in this way for elegance.

The typing system is modelled after the system in [13]. The differences are, as mentioned before, that there is only one global store, that PARALLEL does not require that the subexpressions can be typed with $X^n = []$ and finally that what is called the store, σ in the typing rules in [13], is here moved into the proper type and called X^n.

2.3.2 Example

To return to the example, $x \prec \epsilon, y \prec \mathsf{new}\, x\cdot; (\mathsf{new}x \cdot \mathsf{del}x \cdot ||\mathsf{new}y\cdot) \cdot \mathsf{new}x\cdot$. I will first type $\mathsf{new}x \cdot \mathsf{del}x\cdot$. Since we have $\oslash \vdash \epsilon : \langle [], [], [] \rangle$ from the axiom, we get

$$\frac{\oslash \vdash \epsilon : \langle [], [], [] \rangle \quad x \notin \mathsf{dom}(\oslash)}{x \prec \epsilon \vdash \mathsf{new}\, x\cdot : \langle [], [x], [x] \rangle} \text{(NEW)} \tag{2.4}$$

From WEAKENB applied to the axiom I now get

$$\frac{\oslash \vdash \epsilon : \langle [], [], [] \rangle \qquad \oslash \vdash \epsilon : \langle [], [], [] \rangle \quad x \notin \mathsf{dom}(\oslash)}{x \prec \epsilon \vdash \epsilon : \langle [], [], [] \rangle} \text{(WEAKENB)}$$

And further from DEL

$$\frac{x \prec \epsilon \vdash \epsilon : \langle [], [], [] \rangle \qquad x \prec \epsilon \in \{x \prec \epsilon\}}{x \prec \epsilon \vdash \mathsf{del}x\cdot : \langle [x], [], [-x] \rangle} \text{(DEL)}$$

So, I can now sequence them:

$$\frac{x \prec \epsilon \vdash \mathsf{new}\, x\cdot : \langle [], [x], [x] \rangle \qquad x \prec \epsilon \vdash \mathsf{del}\, x\cdot : \langle [x], [], [-x] \rangle}{x \prec \epsilon \vdash \mathsf{new}\, x \cdot \mathsf{del}\, x\cdot : \langle [], [x], [] \rangle} \text{(SEQ)} \tag{2.5}$$

I will now continue to type $(\mathsf{new}\, x \cdot \mathsf{del}\, x \cdot ||\mathsf{new}\, y\cdot)\cdot$. First, I need a type for $\mathsf{new}\, y\cdot$. To do that, I can use NEW on the conclusion (2.4) from above:

$$\frac{x \prec \epsilon \vdash \mathsf{new}\, x\cdot : \langle [], [x], [x] \rangle \quad y \notin \mathsf{dom}(x \prec \epsilon)}{x \prec \epsilon, y \prec \mathsf{new}\, x\cdot \vdash \mathsf{new}\, y\cdot : \langle [], [x, y], [x, y] \rangle} \text{(NEW)}$$

To be able to use PARALLEL on the two expressions, I must first weaken the base of the left expression (2.5) to get the same basis:

$$\frac{x \prec \epsilon \vdash \mathsf{new}\, x \cdot \mathsf{del}\, x\cdot : \langle [], [x], [] \rangle \qquad x \prec \epsilon \vdash \mathsf{new}\, x\cdot : \langle [], [x], [x] \rangle \quad y \notin \mathsf{dom}(x \prec \epsilon)}{x \prec \epsilon\,,\ y \prec \mathsf{new}\, x\cdot \vdash \mathsf{new}\, x \cdot \mathsf{del}\, x\cdot : \langle [], [x], [] \rangle} \text{(WEAKENB)}$$

(The second premise comes from (2.4)). An application of Parallel then gives

$$\frac{x \prec \epsilon, y \prec \mathsf{new}\, x\cdot \vdash \mathsf{new}\, x \cdot \mathsf{del}\, x\cdot : \langle [], [x], [] \rangle \qquad x \prec \epsilon, y \prec \mathsf{new}\, x\cdot \vdash \mathsf{new}\, y\cdot : \langle [], [x,y], [x,y] \rangle}{x \prec \epsilon, y \prec \mathsf{new}\, x\cdot \vdash (\mathsf{new}\, x \cdot \mathsf{del}\, x \cdot ||\mathsf{new}\, y\cdot)\cdot : \langle [], [[x \mapsto 2], y], [x,y] \rangle} \text{(Parallel)}$$

Now I want to sequence this with $\mathsf{new}\, x\cdot$, for which I have a type (2.4), but first I need to weaken the basis.

$$\frac{x \prec \epsilon \vdash \mathsf{new}\, x\cdot : \langle [], [x], [x] \rangle \qquad x \prec \epsilon \vdash \mathsf{new}\, x\cdot : \langle [], [x], [x] \rangle \quad y \notin \mathsf{dom}(x \prec \epsilon)}{x \prec \epsilon\,,\; y \prec \mathsf{new}\, x\cdot \vdash \mathsf{new}\, x\cdot : \langle [], [x], [x] \rangle} \text{(WeakenB)}$$

And finally, from Seq

$$\frac{\begin{array}{l} x \prec \epsilon, y \prec \mathsf{new}\, x\cdot \vdash (\mathsf{new}\, x \cdot \mathsf{del}\, x \cdot ||\mathsf{new}\, y\cdot)\cdot : \langle [], [x \mapsto 2, y], [x,y] \rangle \\ x \prec \epsilon\,,\; y \prec \mathsf{new}\, x\cdot \vdash \mathsf{new}\, x\cdot : \langle [], [x], [x] \rangle \end{array}}{\begin{array}{l} x \prec \epsilon\,,\; y \prec \mathsf{new}\, x\cdot \vdash (\mathsf{new}\, x \cdot \mathsf{del}\, x \cdot ||\mathsf{new}\, y\cdot) \cdot \mathsf{new}\, x\cdot : \\ \langle [] \cup ([] - [x,y]), [x \mapsto 2, y] \cup ([x,y] + [x]), [x,y] + [x] \rangle \\ \langle [] \cup [-x, -y], [x \mapsto 2, y] \cup [x \mapsto 2, y], [x \mapsto 2, y] \rangle \\ \langle [], [x \mapsto 2, y], [x \mapsto 2, y] \rangle \end{array}} \text{(Seq)} \tag{2.6}$$

This means that the expression is safe to execute on an empty store ($X^n = []$) if $\mathcal{R}(x) \geq 2$ and $\mathcal{R}(y) \geq 1$, since the maximum increase during the run will be two of x and one of y. This also will be the amount left after the run of the expression. This was also what we saw in the example run above. Note that it is not generally the case that X^a and X^p coincide like this.

If we now look at the modified version of the example,

$$x \prec \epsilon\,,\; y \prec \mathsf{new}\, x\cdot; (\mathsf{new} x \cdot \mathsf{del} x \cdot ||\mathsf{new} y \cdot \mathsf{new} x\cdot)\cdot$$

First see that $\mathsf{new}\, y \cdot \mathsf{new}\, x\cdot$ has type $\langle [], [x \mapsto 2, y], [x \mapsto 2, y] \rangle$. By applying Parallel we then get that

$$x \prec \epsilon, y \prec \mathsf{new}\, x\cdot \vdash (\mathsf{new} x \cdot \mathsf{del} x \cdot ||\mathsf{new} y \cdot \mathsf{new} x\cdot)\cdot : \langle [], [x \mapsto 3, y], [x \mapsto 2, y] \rangle$$

This fits with our observation earlier, that there is a run which achieves three x during the run, but the number of components in the store after the run is the same as in the original example expression.

2.4 Properties

2.4.1 Typing properties

Before defining a valid typing judgement I have to define what $\mathsf{dom}(X^*)$ means for any of the hybrid sets X^n, X^p or X^a in some type X. I have already used the notation $\mathsf{dom}(\Gamma)$ for domain of a base, but while a base can be undefined for the components it does not contain, this is not the case of the hybrid sets - they map the remaining components to 0. To be of any use to us dom of a hybrid set must usually be smaller than the domain of the mapping they represent.

Definition 2.4.1 ($\mathsf{dom}(X^*)$)**.**

$$\mathsf{dom}(X^*) = \{x | X(x) \neq 0\}$$

Note that a consequence of this is that we can in some situations have $\mathsf{dom}(A + B) \subset \mathsf{dom}(A) \cup \mathsf{dom}(B)$, as we could have $A(x) = -B(x)$ for some component x.

Lemma 2.4.2 (Valid Typing Judgement). *For all typing derivations* $\Gamma \vdash A : X$ *this holds:*

1. $\mathsf{var}(A) \subseteq \mathsf{dom}(\Gamma), \mathsf{dom}(X^*) \subseteq \mathsf{dom}(\Gamma)$.
2. *Every variable in* $\mathsf{dom}(\Gamma)$ *is declared only once in* Γ.
3. $X^p \supseteq X^a \supseteq -X^n$.
4. $X^p \supseteq []$ *and* $X^n \supseteq []$.

Lemma 2.4.3 (Associativity). *Assume* $\Gamma \vdash A_i \cdot : X_i$ *for* $i \in \{1, 2, 3\}$*, and let* $\Gamma \vdash A_1 \cdot A_2 \cdot : X_{12}$ *and* $\Gamma \vdash A_2 \cdot A_3 \cdot : X_{23}$ *be inferred by* Seq*. The two different ways to apply* Seq *to infer a type for* $A_1 \cdot A_2 \cdot A_3 \cdot$*, namely,*

$$\dfrac{\dfrac{\Gamma \vdash A_1 \cdot A_2 \cdot : X_{12} \qquad \Gamma \vdash A_3 \cdot : X_3}{\Gamma \vdash A_1 \cdot A_2 \cdot A_3 \cdot : X}\,(\textsc{Seq})}{}$$

and

$$\dfrac{\dfrac{\Gamma \vdash A_1 \cdot : X_1 \qquad \Gamma \vdash A_2 \cdot A_3 \cdot : X_{23}}{\Gamma \vdash A_1 \cdot A_2 \cdot A_3 \cdot : Y}\,(\textsc{Seq})}{}$$

lead to equal types, that is, $X = Y$ *in the above inferences.*

Proof on page 22

Lemma 2.4.4 (Generation lemma). *For all typing derivations* $\Gamma \vdash E : X$

1. *If* $E = \epsilon$*, then* $X = \langle [], [], [] \rangle$.
2. *If* $E = \mathsf{new}\, x \cdot$*, then there exist* Δ, Δ', A *and* Y *such that*

$$\begin{aligned} &\Gamma = \Delta, x \prec A, \Delta' \\ &\Delta \vdash A : Y \\ &X = \langle Y^n, Y^p + x, Y^a + x \rangle \end{aligned}$$

3. *If* $E = \mathsf{del}\, x \cdot$*, then*

$$\begin{aligned} &x \in \mathsf{dom}(\Gamma) \\ &X = \langle [x], [], [-x] \rangle \end{aligned}$$

4. *If* $E = (A \,||\, B) \cdot$ *for some* A, B*, then there exist* Y *and* Z *such that*

$$\begin{aligned} &\Gamma \vdash A : Y \\ &\Gamma \vdash B : Z \\ &X = Y + Z \end{aligned}$$

5. *If* $E = A \cdot B\cdot$ *for some expressions* $A\cdot$ *and* $B\cdot$ *, then there exist* Y *and* Z *such that*

$$\begin{array}{l}\Gamma \vdash A\cdot : Y\\ \Gamma \vdash B\cdot : Z\\ X = \langle Y^n \cup (Z^n - Y^a), Y^p \cup (Y^a + Z^p), Y^a + Z^a\rangle\end{array}$$

Proof on page 23.

Lemma 2.4.5 (Weakening). *1. If* $\Gamma = \Delta, x \prec E, \Delta'$ *is legal, then* $\Delta \vdash E : X$ *for some* X*.*

2. If $\Gamma \vdash E : X$ *and* Γ *is an initial segment of a legal basis* Γ'*, then* $\Gamma' \vdash E : X$*.*

Proof on page 26.

Lemma 2.4.6 (Strengthening). *1. If* $\Gamma, x \prec A \vdash B : Y$ *and* $x \notin \mathsf{var}(B)$*, then* $\Gamma \vdash B : Y$*.*

2. If $\Gamma = x_1 \prec A_1, \ldots, x_n \prec A_n$ *is a legal basis and* $x \notin \mathsf{dom}(\Gamma)$*, then for all* i*, where* $1 \leq i \leq n$*, we have that* $x \notin \mathsf{var}(A_i)$*.*

Proofs on page 27. Before expressing the next lemma, uniqueness, I will define a "valid" set of declarations as those with only one declaration of each component.

Definition 2.4.7 (Valid set of declarations). *A set of declarations* $\{x_1 \prec A_1, \ldots, x_n \prec A_n\}$ *will be called "valid" iff we have that for all* i, j *where* $1 \leq i, j \leq n$ *and* $i \neq j$ *also* $x_i \neq x_j$*.*

Note that valid typing judgement (lemma 2.4.2), clause 2, guarantees this property for any basis in a valid typing judgement.

Lemma 2.4.8 (Uniqueness of type). *Let* Γ *and* Γ' *be reorderings of subsets of the same valid set of declarations. If* $\Gamma \vdash A : X$ *and* $\Gamma' \vdash A : Y$*, then* $X = Y$*.*

Proof on page 29.

2.4.2 Configuration properties

To be able to get more type information from a tree, I need a notion of "the expression of a tree". Since all two parallel branches can be expressed by parallel composition in the language, this is not difficult.

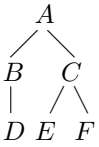
Definition 2.4.9 (Expression of a tree). *The expression of a tree,* $\mathsf{expr}(\mathbb{T})$ *is defined inductively by writing parallel branches as parallel and sequencing parent nodes after their children.*

$$\begin{array}{l}\mathsf{expr}(\mathsf{Lf}(E)) = E\\ \mathsf{expr}(\mathsf{Nd}(E, \mathbb{T})) = (\epsilon||\mathsf{expr}(\mathbb{T})) \cdot E\\ \mathsf{expr}(\mathsf{Nd}(E, \mathbb{T}, \mathbb{T}')) = (\mathsf{expr}(\mathbb{T})||\mathsf{expr}(\mathbb{T}')) \cdot E\end{array}$$

As an example, I will use this tree

$$\mathbb{T} = \mathsf{Nd}(A, \mathsf{Nd}(B, \mathsf{Lf}(D)), \mathsf{Nd}(C, \mathsf{Lf}(E), \mathsf{Lf}(F))),$$

where A, B, C, D, E and F are some expressions. If we only include the expressions at each node, the tree could be visualised like this



And the expression of the tree is:

$$\mathsf{expr}(\mathbb{T}) = ((\epsilon||D) \cdot B||(E||F) \cdot C) \cdot A.$$

The following lemma expresses a property we get using this definition of the expression of a tree.

Lemma 2.4.10 (Property of $\mathsf{expr}(\mathbb{T})$). *If $E = \mathsf{expr}(\mathbb{T})$, then there is a run of E in context $([], E)$ where after only applying rules* osParIntr *and* osParElim$*$ *we get a configuration of the form $([], \mathbb{T})$.*

Proof on page 31.

Definition 2.4.11 (Type of a tree). *If Γ is such that for every α in the tree $\mathbb{T}$ there is an X such that $\Gamma \vdash \mathbb{T}(\alpha) : X$, then there exist Y such that*

$$\Gamma \vdash \mathsf{expr}(\mathbb{T}) : Y$$

This Y is unique and we define $\tau(\mathbb{T}) = Y$, and say that $\mathbb{T}$ is well-typed with respect to Γ.

I will sometimes drop the Γ and just write that $\mathbb{T}$ is well-typed, meaning with respect to some unspecified Γ.

Note that the previous paragraph (2.4.11), in addition to defining $\tau(\mathbb{T})$, also states the existence of this type given a type for the expression in every node and leaf under the same basis. This property must be proved. To clearly separate the definition from the existence property I will state this separately in the next lemma.

Lemma 2.4.12 (Typability of a tree). *If the expression at every node and leaf in a tree has a type under the same basis, then the expression of the whole tree also has a type under the same basis. In other words:*

$$\forall \Gamma : ((\forall \alpha \in \mathbb{T} : \exists X : (\Gamma \vdash \mathbb{T}(\alpha) : X)) \Rightarrow \exists \tau(\mathbb{T}) : (\Gamma \vdash \mathsf{expr}(\mathbb{T}) : \tau(\mathbb{T})))$$

In addition, since for all positions α in $\mathbb{T}$, we have that for some $\tau(\mathbb{T}(\alpha))$, $\Gamma \vdash \mathbb{T}(\alpha) : \tau(\mathbb{T}(\alpha))$ we get:

$$\tau(\mathbb{T})^a = \sum_{\alpha \in \mathbb{T}} \tau(\mathbb{T}(\alpha)) \tag{2.7}$$

Proof on page 31. $\tau(\mathbb{T}(\alpha))$ will here and later express the type of the expression at position α in the tree $\mathbb{T}$.

It should also be easy to see that any subtree of a well-typed tree also is well-typed, as follows. That the expression at each position has a type follows from it being a subtree of a well-typed tree, and then I can again use Lemma 2.4.12 to get the existence of a type for the expression of the subtree.

Definition 2.4.13 (Well-formed configuration). *Configuration* $(M, \mathbb{T})$ *is well-formed with respect to a basis* Γ *and a restriction* $\mathcal{R}$*, notation* $\Gamma \models_{\mathcal{R}} (M, \mathbb{T})$*, iff* $\mathbb{T}$ *is well-typed with respect to* Γ *and we have:*

$$[] \subseteq M - \tau(\mathbb{T})^n \subseteq M + \tau(\mathbb{T})^p \subseteq \mathcal{R}$$

I will omit the subscript $\mathcal{R}$ when no confusion can arise.

We see from this that the conditions stated in section 2.3.1 for an expression being safe to execute on an empty store:

$$[] \subseteq -Z^n \subseteq Z^p \subseteq \mathcal{R},$$

gives a well-formed configuration. Remember that if $\Gamma \vdash E : Z$ for some reordering Γ and type Z, then $\tau(\mathsf{Lf}(E)) = Z$, so we get that if $([], \mathsf{Lf}(E))$ is well-formed then

$$[] \subseteq [] - Z^n \subseteq [] + Z^p \subseteq R,$$

that is, $[] \subseteq -Z^n \subseteq Z^p \subseteq \mathcal{R}$.

Definition 2.4.14 (Terminal configurations). *A configuration* $\mathbb{T}$ *is terminal if it has the form* $(M, \mathsf{Lf}(\epsilon))$*, where* M *is any store.*

2.4.3 Soundness properties

Lemma 2.4.15 (Invariance of $M - \tau(\mathbb{T})^n$ and $M + \tau(\mathbb{T})^p$). *If* $\Gamma \models (M, \mathbb{T})$ *and* $(M, \mathbb{T}) \longrightarrow (M', \mathbb{T}')$*, then*

1. $\mathsf{expr}(\mathbb{T}')$ *has a type under the same basis - there exists* $\tau(\mathbb{T}')$ *such that* $\Gamma \vdash \mathsf{expr}(\mathbb{T}') : \tau(\mathbb{T}')$*.*

2. $$\begin{aligned} M - \tau(\mathbb{T})^n &\subseteq M' - \tau(\mathbb{T}')^n \\ M + \tau(\mathbb{T})^p &\supseteq M' + \tau(\mathbb{T}')^p \\ M + \tau(\mathbb{T})^a &= M' + \tau(\mathbb{T}')^a \end{aligned}$$

Proof on page 37. The invariance lemma is important for understanding the system, and both preservation (2.4.16) and soundness (2.4.19) make extensive use of it.

Lemma 2.4.16 (Preservation). *If* $\Gamma \models (M, \mathbb{T})$ *and* $(M, \mathbb{T}) \longrightarrow (M', \mathbb{T}')$ *then* $\Gamma \models (M', \mathbb{T}')$

Proof on page 43.

Lemma 2.4.17 (Progress). *If* $\Gamma \models (M, \mathbb{T})$ *then either* $(M, \mathbb{T})$ *is terminal or there exists a configuration* $(M', \mathbb{T}')$ *such that* $(M, \mathbb{T}) \longrightarrow (M', \mathbb{T}')$

Proof on page 44.

Definition 2.4.18 (Stuck states). *A configuration $(M, \mathbb{T})$ is stuck if no transition rule applies and $(M, \mathbb{T})$ is not terminal.*

This means in practice that no side condition of any applicable rule from the operational semantics holds for $(M, \mathbb{T})$.

Lemma 2.4.19 (Soundness). *Let Prog = Decls;E be such that $\Gamma \models_{\mathcal{R}} ([], E)$ for some reordering Γ of Decls and restriction $\mathcal{R}$. Then for any $(M, \mathbb{T})$ such that $([], \mathsf{Lf}(E)) \longrightarrow^* (M, \mathbb{T})$ we have that $(M, \mathbb{T})$ is not stuck and $M \subseteq X^p$.*

Proof on page 45.

Lemma 2.4.20 (Sharpness). *If $\Gamma \vdash E : X$ then, for every component x, for every restriction $\mathcal{R}$ and every well-formed configuration $(M, \mathbb{T}[\mathsf{Lf}(E)]_\alpha) = (M_0, \mathbb{T}_0)$ with respect to the given $\mathcal{R}$, there exists a run*

$$(M_0, \mathbb{T}_0) \to \cdots \to (M_n, \mathbb{T}_n) = (M_n, \mathbb{T}[\mathsf{Lf}(\epsilon)]_\alpha)$$

of E where there is a k, $0 \leq k \leq n$, such that $M_k(x) = M_0(x) + X^p(x)$, and there exists a run

$$(M_0, \mathbb{T}_0) \to \cdots \to (M_m, \mathbb{T}_m) = (M_m, \mathbb{T}[\mathsf{Lf}(\epsilon)]_\alpha)$$

of E where there is a j, $0 \leq j \leq m$, such that $M_j(x) = M_0(x) - X^n(x)$, and for all runs

$$(M_0, \mathbb{T}_0) \to \cdots \to (M_q, \mathbb{T}_q) = (M_q, \mathbb{T}[\mathsf{Lf}(\epsilon)]_\alpha)$$

of E we have $M_q(x) = M_0(x) + X^a(x)$.

The next corollary is a special case of the previous lemma (2.4.20), only using $M_0 = []$ and $\alpha = \bullet$.

Corollary 2.4.21 (Sharpness of programs). *For any program Prog = Decls; E such that for some reordering Γ of Decls we have $\Gamma \vdash E : X$ and $\Gamma \models_{\mathcal{R}} ([], \mathsf{Lf}(E))$, for some restriction $\mathcal{R}$, then, for every component x, there is a run*

$$([], \mathsf{Lf}(E)) = ([], \mathbb{T}_0) \to \cdots \to (M_n, \mathbb{T}_n) = (M_n, \mathsf{Lf}(\epsilon))$$

where there is a k, $0 \leq k \leq n$ such that $M_k(x) = M_0(x) + X^p(x)$, and there exists a run

$$([], \mathbb{T}_0) \to \cdots \to (M_m, \mathbb{T}_m) = (M_m, \mathsf{Lf}(\epsilon))$$

of E where there is a j, $0 \leq j \leq m$ such that $M_j(x) = M_0(x) - X^n(x)$, and for all runs

$$([], \mathbb{T}_0) \to \cdots \to (M_q, \mathbb{T}_q) = (M_q, \mathsf{Lf}(\epsilon))$$

of E we have $M_q(x) = X^a(x) + M_0(x)$.

Proofs on pages 46 to 54.

Example. We have that

$$\mathsf{expr}(\mathsf{Nd}(\mathsf{new}x, \mathsf{Lf}(\,\mathsf{new}\,x\,\mathsf{del}x), \mathsf{Lf}(\mathsf{new}y))) = (\,\mathsf{new}\,x\mathsf{del}\,x||\mathsf{new}\,y)\mathsf{new}\,x$$

In the previous section (2.6) we saw that

$$x \prec \epsilon, y \prec \mathsf{new}\,x \vdash (\mathsf{new}\,x\,\mathsf{del}\,x||\mathsf{new}\,y)\mathsf{new}\,x : \langle [], [x \mapsto 2, y], [x \mapsto 2, y] \rangle$$

This implies that

$$\tau(\mathsf{Nd}(\mathsf{new}x, \mathsf{Lf}(\,\mathsf{new}\,x\,\mathsf{del}x), \mathsf{Lf}(\mathsf{new}y))) = \langle [], [x \mapsto 2, y], [x \mapsto 2, y] \rangle$$

2.4.4 Termination

As a last theorem, we have termination:

Theorem 2.4.22 (Termination). *If $\Gamma \vdash E : X$ for some Γ, E and X, then for any $\mathbb{T}$, $\mathcal{R}$, α and M such that $\Gamma \models_{\mathcal{R}} (M, \mathbb{T}[\mathsf{Lf}(E)]_\alpha)$ we have that any run of E in context $\mathbb{T}$, on position α and starting with store M has finite length.*

Prof on page 54.

2.5 Proofs of typing properties

> Truth. Truth is all I want. And a little dignity.
>
> Charles Chaplin.

2.5.1 Valid typing judgement (Lemma 2.4.2)

The lemma states that: *For all typing derivations $\Gamma \vdash A : X$ this holds:*

1. $\mathsf{var}(A) \subseteq \mathsf{dom}(\Gamma), \mathsf{dom}(X^*) \subseteq \mathsf{dom}(\Gamma)$.
2. *Every variable in $\mathsf{dom}(\Gamma)$ is declared only once in Γ.*
3. $X^p \supseteq X^a \supseteq -X^n$.
4. $X^p \supseteq []$ *and* $X^n \supseteq []$.

Proof By induction on the length of typing derivations of $\Gamma \vdash A : X$. The base case is Axiom

Base case Let $\Gamma \vdash A : X$ be inferred by Axiom:

$$\frac{}{\oslash \vdash \epsilon : \langle [], [], [] \rangle}$$

We now have $A = \epsilon$ and $\Gamma = \oslash$ and $X = \langle [], [], [] \rangle$. Then $\mathsf{var}(\epsilon) = \mathsf{dom}(X^*) = \mathsf{dom}(\oslash)$ and $[] \supseteq [] \supseteq -[]$ and all the clauses hold.

Inductive Cases The inductive cases concern the other typing derivations:

- Let $\Gamma \vdash A : X$ be inferred by WeakenB:

$$\frac{\Gamma' \vdash A : X \qquad \Gamma' \vdash B : Y \quad x \notin \mathsf{dom}(\Gamma')}{\Gamma', x \prec B \vdash A : X}$$

  We have $\Gamma = \Gamma', x \prec B$ and A and X the same as in the hypothesis.

  1. By the inductive hypothesis $\mathsf{var}(A) \subseteq \mathsf{dom}(\Gamma')$ and $\mathsf{dom}(X^*) \subseteq \mathsf{dom}(\Gamma')$ so the clause follows by $\mathsf{dom}(\Gamma') \subset \mathsf{dom}(\Gamma', x \prec B) = \mathsf{dom}(\Gamma)$.
  2. By the inductive hypothesis on the shorter typing derivation $\Gamma' \vdash A : X$ all variables in Γ' are declared only once. By the side condition this does not include x, so the new declaration of x is unique in $\Gamma = \Gamma', x \prec B$.

3. I need to know that $X^p \supseteq X^a \supseteq -X^n$. But we have this already by the inductive hypothesis on $\Gamma' \vdash A : X$, which has a shorter typing derivation.
4. I need to know that $X^p \supseteq []$ and $X^n \supseteq []$. But we have this already by the inductive hypothesis on $\Gamma' \vdash A : X$, which has a shorter typing derivation.

- Let $\Gamma \vdash A : X$ be inferred by New:

$$\frac{\Gamma' \vdash B : Y \quad x \notin \mathsf{dom}(\Gamma)}{\Gamma', x \prec B \vdash \mathsf{new}\, x\cdot : \langle Y^n, Y^p + x, Y^a + x\rangle}$$

We have $A = \mathsf{new}\, x\cdot$, $X = \langle Y^n, Y^p + x, Y^a + x\rangle$ and $\Gamma = \Gamma', x \prec B$.

1. For the first condition: $\mathsf{var}(\mathsf{new}\, x\cdot) = \{x\} \subseteq \mathsf{dom}(\Gamma', x \prec B)$. For the second condition: by the inductive hypothesis $\mathsf{dom}(Y^*) \subseteq \mathsf{dom}(\Gamma')$. Adding x on both sides (because of the side condition) keeps the subset relation.
2. By the inductive hypothesis on the shorter typing derivation $\Gamma' \vdash B : Y$ all variables in Γ' are declared only once. By the side condition this does not include x, so the new declaration of x is unique in $\Gamma = \Gamma', x \prec B$.
3. By the induction hypothesis I have $Y^p \supseteq Y^a \supseteq -Y^n$. This implies $Y^p + x \supseteq Y^a + x \supseteq -Y^n$, which is all we need.
4. By the induction hypothesis I have $Y^p \supseteq []$ and $Y^n \supseteq []$. This implies $Y^p + x = X^p \supseteq []$ and $Y^n = X^n \supseteq []$, which is all we need.

- Let $\Gamma \vdash A : X$ be inferred by Del:

$$\frac{\Gamma \vdash B : Y \qquad x \prec B \in \Gamma}{\Gamma \vdash \mathsf{del}\, x\cdot : \langle [x], [], [-x]\rangle}$$

Then $A = \mathsf{del} x\cdot$, $X = \langle [x], [], [-x]\rangle$ and Γ the same as in the premise.

1. Holds by side condition: $\mathsf{dom}(X^n) = \mathsf{dom}(X^a) = \{x\} = \mathsf{var}(\mathsf{del}\, x\cdot) = \{x\} \subseteq \mathsf{dom}(\Gamma)$ and $\mathsf{dom}(X^p) = []$.
2. By the induction hypothesis all variables in $\mathsf{dom}(\Gamma)$ are declared exactly once in Γ, and this is all we need.
3. Holds by $[] \supseteq [-x] \supseteq -[x]$.
4. Holds by $[x] \supseteq []$ and $[] \supseteq []$.

- Let $\Gamma \vdash A : X$ be inferred by Parallel:

$$\frac{\Gamma \vdash B : Y \qquad \Gamma \vdash C : Z}{\Gamma \vdash (B \,||\, C)\cdot : \langle Y^n + Z^n, Y^p + Z^p, Y^a + Z^a\rangle}$$

We then have $A = (B \,||\, C)\cdot$, $X = \langle Y^n + Z^n, Y^p + Z^p, Y^a + Z^a\rangle$ and Γ as in the hypothesis. By the inductive hypothesis we have $\mathsf{var}(B) \subseteq \mathsf{dom}(\Gamma)$, $\mathsf{dom}(Y^*) \subseteq \mathsf{dom}(\Gamma)$, $\mathsf{var}(C) \subseteq \mathsf{dom}(\Gamma)$ and $\mathsf{dom}(Z^*) \subseteq \mathsf{dom}(\Gamma)$

1.

$$\begin{array}{l}\mathsf{var}(A) = \mathsf{var}((B \,||\, C)\cdot) = \mathsf{var}(B) \cup \mathsf{var}(C) \subseteq \mathsf{dom}(\Gamma)\\ \mathsf{dom}(X^*) = \mathsf{dom}(Y^* + Z^*) \subseteq \mathsf{dom}(Y^*) \cup \mathsf{dom}(Z^*) \subseteq \mathsf{dom}(\Gamma)\end{array}$$

2. Since Γ is the same in the premises and the conclusion, this holds by the inductive hypothesis.
3. I have $Y^p \supseteq Y^a \supseteq -Y^n$ and $Z^p \supseteq Z^a \supseteq -Z^n$. This implies

$$Y^p + Z^p \supseteq Y^a + Z^a \supseteq -(Y^n + Z^n),$$

which is all we need.

4. I have $Y^p \supseteq []$ and $Y^n \supseteq []$ and $Z^p \supseteq []$ and $Z^n \supseteq []$. This implies $Y^p + Z^p \supseteq []$ and $Y^n + Z^n \supseteq []$ which is all we need.

- Let $\Gamma \vdash A : X$ be inferred by (SEQ):

$$\frac{\Gamma \vdash B\cdot : Y \qquad \Gamma \vdash C\cdot : Z}{\Gamma \vdash B \cdot C\cdot : \langle Y^n \cup (Z^n - Y^a), Y^p \cup (Y^a + Z^p), Y^a + Z^a\rangle}$$

Then $A = B \cdot C\cdot$, $X = \langle Y^n \cup (Z^n - Y^a), Y^p \cup (Y^a + Z^p), Y^a + Z^a\rangle$ and Γ the same as in the hypothesis.

1. holds by the inductive hypothesis and $\mathsf{var}(B \cdot C\cdot) = \mathsf{var}(B\cdot) \cup \mathsf{var}(C\cdot)$ and

$$\begin{array}{r}\mathsf{dom}(X^p) = \mathsf{dom}(Y^p \cup (Y^a + Z^p)) \subseteq \mathsf{dom}(Y^p) \cup \mathsf{dom}(Y^a) \cup \mathsf{dom}(Z^p) \subseteq \mathsf{dom}(\Gamma)\\ \mathsf{dom}(X^n) = \mathsf{dom}(Y^n \cup (Z^n - Y^a)) \subseteq \mathsf{dom}(Y^n) \cup \mathsf{dom}(Y^a) \cup \mathsf{dom}(Z^n) \subseteq \mathsf{dom}(\Gamma)\\ \mathsf{dom}(X^a) = \mathsf{dom}(Y^a + Z^a) \subseteq \mathsf{dom}(Y^a) \cup \mathsf{dom}(Z^a) \subseteq \mathsf{dom}(\Gamma)\end{array}$$

2. Since Γ is the same in the premises, which have a shorter typing derivation, and the conclusion, this holds by the inductive hypothesis.
3. I do this in the parts; first I show that $X^p \supseteq X^a$. Remember I have $Z^p \supseteq Z^a$ from inductive hypothesis on the shorter typing derivation $\Gamma \vdash C\cdot : Z$, and this implies $Y^a + Z^p \supseteq Y^a + Z^a$.

$$\begin{array}{rcl}X^p & = & Y^p \cup (Y^a + Z^p)\\ & \supseteq & (Y^a + Z^p)\\ & \supseteq & Y^a + Z^a\\ & = & X^a\end{array}$$

Secondly I must prove that $X^a \supseteq -X^n$. I use that from the inductive hypothesis $Z^a \supseteq -Z^n$ and $Y^a \supseteq -Y^n$.

$$\begin{array}{rcll}X^a & = & Y^a + Z^a & \\ & \supseteq & Y^a - Z^n & Z^a \supseteq -Z^n\\ & = & ((-Y^n) \cup Y^a) - Z^n & Y^a \supseteq -Y^n\\ & = & (-Y^n - Z^n) \cup (Y^a - Z^n) & \text{distributivity of } - \text{ over } \cup\\ & \supseteq & (-Y^n) \cup (Y^a - Z^n) & Z^n \supseteq []\\ & = & -(Y^n \cup (Z^n - Y^a)) & \text{distributivity of } - \text{ over } \cup\\ & = & -X^n & \end{array}$$

4. From the inductive hypothesis I have $Y^n \supseteq []$ and $Y^p \supseteq []$. By the properties of union of hybrid sets, this implies that $Y^n \cup (Z^n - Y^a) \supseteq []$ and $Y^p \cup (Y^a + Z^p) \supseteq []$, which is what I need to prove.

□

2.5.2 Associativity (Lemma 2.4.3)

Assume $\Gamma \vdash A_i\cdot : X_i$ *for* $i \in \{1,2,3\}$*, and let* $\Gamma \vdash A_1 \cdot A_2\cdot : X_{12}$ *and* $\Gamma \vdash A_2 \cdot A_3\cdot : X_{23}$ *be inferred by* Seq*. The two different ways to apply* Seq *to infer a type for* $A_1 \cdot A_2 \cdot A_3\cdot$*, namely,*

$$\frac{\Gamma \vdash A_1 \cdot A_2\cdot : X_{12} \qquad \Gamma \vdash A_3\cdot : X_3}{\Gamma \vdash A_1 \cdot A_2 \cdot A_3\cdot : X} \text{(Seq)}$$

and

$$\frac{\Gamma \vdash A_1\cdot : X_1 \qquad \Gamma \vdash A_2 \cdot A_3\cdot : X_{23}}{\Gamma \vdash A_1 \cdot A_2 \cdot A_3\cdot : Y} \text{(Seq)}$$

lead to equal types, that is, $X = Y$ *in the above inferences.*

Proof I have $\Gamma \vdash A_i\cdot : X_i$ for $i \in \{1,2,3\}$. First I will find the types X_{12} and X_{23}.

Apply first Seq to $A_1\cdot$ and $A_2\cdot$:

$$\frac{\Gamma \vdash A_1\cdot : X_1 \qquad \Gamma \vdash A_2\cdot : X_2}{\Gamma \vdash A_1 \cdot A_2\cdot : \langle X_1^n \cup (X_2^n - X_1^a), X_1^p \cup (X_1^a + X_2^p), X_1^a + X_2^a\rangle} \text{(Seq)}$$

Using the same kind of application, I also get $\Gamma \vdash A_2 \cdot A_3\cdot : \langle X_2^n \cup (X_3^n - X_2^a), X_2^p \cup (X_2^a + X_3^p), X_2^a + X_3^a\rangle$. Now, sequence $A_1 \cdot A_2\cdot$ with $A_3\cdot$:

$$\frac{\begin{array}{l}\Gamma \vdash A_1 \cdot A_2\cdot : \langle X_1^n \cup (X_2^n - X_1^a), X_1^p \cup (X_1^a + X_2^p), X_1^a + X_2^a\rangle \\ \Gamma \vdash A_3\cdot : X_3\end{array}}{\begin{array}{ll}\Gamma \vdash A_1 \cdot A_2 \cdot A_3\cdot : & \langle (X_1^n \cup (X_2^n - X_1^a)) \cup (X_3^n - X_1^a - X_2^a), \\ & (X_1^p \cup (X_1^a + X_2^p)) \cup (X_1^a + X_2^a + X_3^p), \\ & X_1^a + X_2^a + X_3^a\rangle\end{array}} \text{(Seq)}$$

and to $A_1\cdot$ with $A_2 \cdot A_3\cdot$:

$$\frac{\begin{array}{l}\Gamma \vdash A_1\cdot : X_1 \\ \Gamma \vdash A_2 \cdot A_3\cdot : \langle X_2^n \cup (X_3^n - X_2^a), X_2^p \cup (X_2^a + X_3^p), X_2^a + X_3^a\rangle\end{array}}{\begin{array}{ll}\Gamma \vdash A_1 \cdot A_2 \cdot A_3\cdot : & \langle X_1^n \cup (X_2^n \cup (X_3^n - X_2^a) - X_1^a), \\ & X_1^p \cup (X_1^a + X_2^p \cup (X_2^a + X_3^p)), \\ & X_1^a + X_2^a + X_3^a\rangle\end{array}} \text{(Seq)}$$

To show they are equal, note first that the last part X^a is the same. For X^n:

$$\begin{array}{l}X_1^n \cup (X_2^n \cup (X_3^n - X_2^a) - X_1^a) = \\ X_1^n \cup ((X_2^n - X_1^a) \cup (X_3^n - X_2^a - X_1^a)) = \\ (X_1^n \cup (X_2^n - X_1^a)) \cup (X_3^n - X_2^a - X_1^a)\end{array}$$

And finally, X^p:

$$X_1^p \cup (X_1^a + X_2^p \cup (X_2^a + X_3^p)) =$$
$$X_1^p \cup ((X_1^a + X_2^p) \cup (X_1^a + X_2^a + X_3^p)) =$$
$$(X_1^p \cup (X_1^a + X_2^p)) \cup (X_1^a + X_2^a + X_3^p) =$$

□

2.5.3 Generation (Lemma 2.4.4)

The proof is by structural induction on the typing derivations. The inductive hypothesis is: *For any shorter type derivation with conclusion* $\Gamma \vdash E : X$*: if* $E = \epsilon$*, then* $X = \langle [], [], [] \rangle$*, if* $E = \mathsf{new}\, x\cdot$*, then there exist* Δ, Δ', A *and* Y *such that* $\Gamma = \Delta, x \prec A, \Delta'$ *and* $\Delta \vdash A : Y$ *and* $X = \langle Y^n, Y^p + x, Y^a + x \rangle$*, if* $E = \mathsf{del}\, x\cdot$*, then* $x \in \mathsf{dom}(\Gamma)$ *and* $X = \langle [x], [], [-x] \rangle$*, if* $E = (A \,||\, B)\cdot$ *for some* A, B*, then there exist* Y *and* Z *such that* $\Gamma \vdash A : Y$*,* $\Gamma \vdash B : Z$ *and* $X = Y + Z$*, and finally, if* $E = A \cdot B\cdot$ *, then there exist* Y *and* Z *such that* $\Gamma \vdash A\cdot : Y$*,* $\Gamma \vdash B\cdot : Z$ *and* $X = \langle Y^n \cup (Z^n - Y^a), Y^p \cup (Y^a + Z^p), Y^a + Z^a \rangle$.

The base case is the derivation of shortest length: $\oslash \vdash \epsilon : \langle [], [], [] \rangle$, which can only be derived by Axiom. This only fits the pattern $E = \epsilon$, and we have the result $X = \langle [], [], [] \rangle$ directly from the type rule.

The inductive cases are the following:

- New. Using any shorter type derivation $\Delta \vdash A : Y$ where $x \notin \mathsf{dom}(\Delta)$, we can apply New, and the application will follow this pattern:

$$\frac{\Delta \vdash A : Y \quad x \notin \mathsf{dom}(\Delta)}{\Delta, x \prec A \vdash \mathsf{new}\, x\cdot : \langle Y^n, Y^p + x, Y^a + x \rangle} \text{(New)}$$

  The conclusion is of a form where $E = \mathsf{new}\, x\cdot$. This means that I must show that there exist Δ, Δ', A and Y such that $\Gamma = \Delta, x \prec A, \Delta'$ and $\Delta \vdash A : Y$ and $X = \langle Y^n, Y^p + x, Y^a + x \rangle$. Now, let Δ be the same as in the rule application, let $\Delta' = \oslash$ and the properties should hold.

- Del. Using any shorter type derivation $\Gamma \vdash A : X$ where $x \prec A \in \Gamma$, I can get a longer one with this application:

$$\frac{\Gamma \vdash A : X \qquad x \prec A \in \Gamma}{\Gamma \vdash \mathsf{del}\, x\cdot : \langle [x], [], [-x] \rangle} \text{(Del)}$$

  This fits the pattern where $E = \mathsf{del}\, x\cdot$, and we must have $x \in \mathsf{dom}(\Gamma)$ and $X = \langle [x], [], [-x] \rangle$. Both hold immediately from the rule application.

- Seq. Take any two type derivations $\Gamma \vdash A_1\cdot : Y_1$ and $\Gamma \vdash B_1\cdot : Z_1$. I can get a longer derivation with the following application:

$$\frac{\Gamma \vdash A_1\cdot : Y_1 \qquad \Gamma \vdash B_1\cdot : Z_1}{\Gamma \vdash A_1 \cdot B_1\cdot : \langle Y_1^n \cup (Z_1^n - Y_1^a), Y_1^p \cup (Y_1^a + Z_1^p), Y_1^a + Z_1^a \rangle} \text{(Seq)}$$

  We see that we are in the case where $E = A \cdot B\cdot$ and X is the type in the last inference, so we need to prove that there exist Y and Z, such that

$\Gamma \vdash A\cdot : Y, \Gamma \vdash B\cdot : Z$ and $X = \langle Y^n \cup (Z^n - Y^a), Y^p \cup (Z^p + Y^a), Y^a + Z^a \rangle$. But even though $A \cdot B\cdot = A_1 \cdot B_1\cdot$, it is not necessarily the case that $A\cdot = A_1\cdot$ and $B\cdot = B_1\cdot$. There are actually three different possibilities:

We can have (1) : $A\cdot = A_1\cdot$ and $B\cdot = B_1\cdot$, or, if $A\cdot \neq A_1\cdot$ and $B\cdot \neq B_1\cdot$ we can have: (2) $A\cdot = A_1 \cdot A_2\cdot$ and $B_1\cdot = A_2 \cdot B\cdot$ or finally (3) we can have $B\cdot = A_2 \cdot B_1\cdot$ and $A_1\cdot = A \cdot A_2\cdot$. I treat each of the three cases separately below:

1. $A\cdot = A_1\cdot$ and $B\cdot = B_1\cdot$: This one is not difficult, as the wanted properties follows from the application of Seq above, just removing the subscripts and you have the wanted types Y and Z:

$$\text{(Seq)}\quad \frac{\Gamma \vdash A\cdot : Y \qquad \Gamma \vdash B\cdot : Z}{\Gamma \vdash A \cdot B\cdot : \langle Y^n \cup (Z^n - Y^a), Y^p \cup (Y^a + Z^p), Y^a + Z^a \rangle}$$

2. $A\cdot = A_1 \cdot A_2\cdot$ and $B_1\cdot = A_2 \cdot B\cdot$. Note that $\Gamma \vdash B_1\cdot : Z_1$ is derived by a shorter type derivation, so by the inductive hypothesis used on $B_1\cdot = A_2 \cdot B\cdot$ there are Y_2 and Z, such that $\Gamma \vdash A_2\cdot : Y_2$, $\Gamma \vdash B\cdot : Z$ and $Z_1 = \langle Y_2^n \cup (Z^n - Y_2^a), Y_2^p \cup (Y_2^a + Z^p), Y_2^a + Z^a \rangle$. Now apply Seq to $A\cdot = A_1 \cdot A_2\cdot$:

$$\text{(Seq)}\quad \frac{\Gamma \vdash A_1\cdot : Y_1 \qquad \Gamma \vdash A_2\cdot : Y_2}{\Gamma \vdash A_1 \cdot A_2\cdot : \langle Y_1^n \cup (Y_2^n - Y_1^a), Y_1^p \cup (Y_1^a + Y_2^p), Y_1^a + Y_2^a \rangle}$$

Since $A_1 \cdot A_2\cdot = A\cdot$, we now have $\Gamma \vdash A\cdot : Y$, where $Y = \langle Y_1^n \cup (Y_2^n - Y_1^a), Y_1^p \cup (Y_1^a + Y_2^p), Y_1^a + Y_2^a \rangle$. Now again apply Seq, this time to $A\cdot$ and $B\cdot$:

$$\text{(Seq)}\quad \frac{\Gamma \vdash A\cdot : Y \qquad \Gamma \vdash B\cdot : Z}{\Gamma \vdash A \cdot B\cdot : \langle Y^n \cup (Z^n - Y^a), Y^p \cup (Y^a + Z^p), Y^a + Z^a \rangle}$$

Since $A \cdot B\cdot = A_1 \cdot A_2 \cdot B\cdot$ and $A_1 \cdot B_1\cdot = A_1 \cdot A_2 \cdot B\cdot$, we now have equality of X and the type of $A \cdot B\cdot$ by associativity (2.4.3).

3. $B\cdot = A_2 \cdot B_1\cdot$ and $A_1\cdot = A \cdot A_2\cdot$. I will proceed as in the previous case, just renaming as necessary: note that $\Gamma \vdash A_1\cdot : Y_1$ is derived by a shorter type derivation, so by the inductive hypothesis used on $A_1\cdot = A \cdot A_2\cdot$ there are Y and Y_2, such that $\Gamma \vdash A\cdot : Y$, $\Gamma \vdash A_2\cdot : Y_2$ and $Y_1 = \langle Y^n \cup (Y_2^n - Y^a), Y^p \cup (Y^a + Y_2^p), Y^a + Y_2^a \rangle$. Now apply Seq to $B\cdot = A_2 \cdot B_1\cdot$:

$$\text{(Seq)}\quad \frac{\Gamma \vdash A_2\cdot : Y_2 \qquad \Gamma \vdash B_1\cdot : Z_1}{\Gamma \vdash A_1 \cdot A_2\cdot : \langle Y_2^n \cup (Z_1^n - Y_2^a), Y_2^p \cup (Y_2^a + Z_1^p), Y_2^a + Z_1^a \rangle}$$

Since $A_2 \cdot B_1\cdot = B\cdot$, we now have $\Gamma \vdash B\cdot : Z$, where $Z = \langle Y_2^n \cup (Z_1^n - Y_2^a), Y_2^p \cup (Y_2^a + Z_1^p), Y_2^a + Z_1^a \rangle$. Now again apply Seq, this time to $A\cdot$ and $B\cdot$:

$$\text{(Seq)}\quad \frac{\Gamma \vdash A\cdot : Y \qquad \Gamma \vdash B\cdot : Z}{\Gamma \vdash A \cdot B\cdot : \langle Y^n \cup (Z^n - Y^a), Y^p \cup (Y^a + Z^p), Y^a + Z^a \rangle}$$

Since $A \cdot B\cdot = A \cdot A_2 \cdot B_1\cdot$ and $A_1 \cdot B_1\cdot = A \cdot A_2 \cdot B_1\cdot$, we now have equality of X and the type of $A \cdot B\cdot$ by associativity (2.4.3).

- Parallel.

$$\frac{\Gamma \vdash A : Y \qquad \Gamma \vdash B : Z}{\Gamma \vdash (A \,||\, B)\cdot : \langle Y^n + Z^n, Y^p + Z^p, Y^a + Z^a\rangle}\ (\textsc{Parallel})$$

We have $E = (A \,||\, B)\cdot$ and have to show that there are Y and Z such that $\Gamma \vdash A : Y$ and $\Gamma \vdash B : Z$ and $X = Y + Z$. All three properties follow from the rule application as shown above.

- WeakenB.

$$\frac{\Gamma' \vdash E : X \qquad \Gamma' \vdash C : V \quad y \notin \mathsf{dom}(\Gamma')}{\Gamma', y \prec C \vdash E : X}\ (\textsc{WeakenB})$$

I have $\Gamma = \Gamma', y \prec C$. I must now do a case distinction on E, according to the case distinction in the inductive hypothesis:

  - $E = \epsilon$:

$$\frac{\Gamma' \vdash \epsilon : X \qquad \Gamma' \vdash C : V \quad y \notin \mathsf{dom}(\Gamma')}{\Gamma', y \prec C \vdash \epsilon : X}\ (\textsc{WeakenB})$$

    In this case, $E = \epsilon$ and I must prove that $X = \langle [], [], []\rangle$. This follows from the inductive hypothesis applied to $\Gamma' \vdash \epsilon : X$.

  - $E = \mathsf{new}\, x\cdot$

    The application of WeakenB would then follow this pattern:

$$\frac{\Gamma' \vdash \mathsf{new}\, x\cdot : X \qquad \Gamma' \vdash C : V \quad y \notin \mathsf{dom}(\Gamma')}{\Gamma', y \prec C \vdash \mathsf{new}\, x\cdot : X}\ (\textsc{WeakenB})$$

    Since $\Gamma' \vdash \mathsf{new}\, x\cdot : X$ must have been derived by a shorter derivation, I can apply the inductive hypothesis and get the existence of Δ_1, Δ_2, A and Y, such that $\Delta_1 \vdash A : Y$ and $\Gamma' = \Delta_1, x \prec A, \Delta_2$ and $X = \langle Y^n, Y^p + x, Y^a + x\rangle$. If we let $\Delta = \Delta_1$ and $\Delta' = \Delta_2, y \prec C$, we have all the needed properties.

  - $E = \mathsf{del}\, x\cdot$ The type was then derived by an application of WeakenB of this form:

$$\frac{\Gamma' \vdash \mathsf{del}\, x\cdot : X \qquad \Gamma' \vdash C : V \quad y \notin \mathsf{dom}(\Gamma')}{\Gamma', y \prec C \vdash \mathsf{del}\, x\cdot : X}\ (\textsc{WeakenB})$$

    Since the premise of this rule has a shorter derivation, I can use the inductive hypothesis, and get that $X = \langle [x], [], [-x]\rangle$ and $x \in \mathsf{dom}(\Gamma')$. Since the latter also implies $x \in \mathsf{dom}(\Gamma', y \prec B) = \mathsf{dom}(\Gamma)$, I am done.

– $E = A \cdot B\cdot$.

It was then derived with WeakenB like this:

$$\frac{\Gamma' \vdash A \cdot B\cdot : X \qquad \Gamma' \vdash C : V \quad y \notin \mathsf{dom}(\Gamma')}{\Gamma', y \prec C \vdash A \cdot B\cdot : X} \text{(WeakenB)}$$

Since it is the conclusion of a shorter type derivation, I can apply the inductive hypothesis on $\Gamma' \vdash A \cdot B\cdot : X$ and get the existence of Y and Z, such that $\Gamma' \vdash A\cdot : Y$ and $\Gamma' \vdash B\cdot : Z$ and $X = \langle Y^n \cup (Z^n - Y^a), Y^p \cup (Z^p + Y^a), Y^a + Z^a \rangle$. Now I can apply WeakenB to the type judgements for $A\cdot$ and $B\cdot$:

$$\frac{\Gamma' \vdash A\cdot : Y \qquad \Gamma' \vdash C : V \quad y \notin \mathsf{dom}(\Gamma')}{\Gamma', y \prec C \vdash A\cdot : Y} \text{(WeakenB)}$$

$$\frac{\Gamma' \vdash B\cdot : Z \qquad \Gamma' \vdash C : V \quad y \notin \mathsf{dom}(\Gamma')}{\Gamma', y \prec C \vdash B\cdot : Z} \text{(WeakenB)}$$

and I get $\Gamma \vdash A\cdot : Y$ and $\Gamma \vdash B\cdot : Z$ as needed.

– $E = (A||B)\cdot$. Assume $\Gamma \vdash (A \,||\, B)\cdot : X$ is inferred by:

$$\frac{\Gamma' \vdash (A \,||\, B)\cdot : X \qquad \Gamma' \vdash C : V \quad y \notin \mathsf{dom}(\Gamma')}{\Gamma', y \prec C \vdash (A \,||\, B)\cdot : X} \text{(WeakenB)}$$

We can apply the induction hypothesis to $\Gamma' \vdash (A \,||\, B)\cdot : X$ and get

$$\begin{gathered} \Gamma' \vdash A : Y \\ \Gamma' \vdash B : Z \\ X = \langle Y^n + Z^n, Y^p + Z^p, Y^a + Z^a \rangle \end{gathered}$$

Now I apply WeakenB to the premises, first for A:

$$\frac{\Gamma' \vdash A : Y \qquad \Gamma' \vdash C : V \quad y \notin \mathsf{dom}(\Gamma')}{\Gamma', y \prec C \vdash A : Y} \text{(WeakenB)}$$

and then for B:

$$\frac{\Gamma' \vdash B : Z \qquad \Gamma' \vdash C : V \quad y \notin \mathsf{dom}(\Gamma')}{\Gamma', y \prec C \vdash B : Z} \text{(WeakenB)}$$

□

2.5.4 Weakening (Lemma 2.4.5)

1 *If* $\Gamma = \Delta, x \prec E, \Delta'$ *is legal, then* $\Delta \vdash E : X$ *for some* X.

Proof. Since $\Gamma = \Delta, x \prec E, \Delta'$ is legal, then by the definition of bases (2.3.1) there exist B and Y such that $\Gamma \vdash B : Y$. In the typing derivation tree for B, the only way to extend Δ to $\Delta, x \prec E$ is by applying the rule New or WeakenB

$$\frac{\Delta \vdash E : Z \quad x \notin \mathsf{dom}(\Delta)}{\Delta, x \prec E \vdash \mathsf{new}\, x\cdot : \langle Z^n, Z^p + x, Z^a + x\rangle} \text{(New)}$$

$$\frac{\Delta \vdash A : X \qquad \Delta \vdash E : Z \quad x \notin \mathsf{dom}(\Delta)}{\Delta, x \prec E \vdash A : X} \text{(WeakenB)}$$

Each of these rules have $\Delta \vdash E : Z$ as a premise. □

2 *If* $\Gamma \vdash E : X$ *and* Γ *is an initial segment of a legal basis* Γ'*, then* $\Gamma' \vdash E : X$*.*

Proof Since Γ is an initial sequence of Γ', assume $\Gamma' = \Gamma, x_1 \prec A_1, \ldots, x_n \prec A_n$. From the previous item, we have that for every k, $1 \leq k \leq n$, there is X_k such that:

$$\Gamma, x_1 \prec A_1, \ldots, x_{k-1} \prec A_{k-1} \vdash A_k : X_k$$

So we can apply WeakenB repeatedly, for $k = 1$, etc. up to $k = n$:

$$\frac{\begin{array}{l}\Gamma, x_1 \prec A_1, \ldots, x_{k-1} \prec A_{k-1} \vdash E : Z \\ \Gamma, x_1 \prec A_1, \ldots, x_{k-1} \prec A_{k-1} \vdash A_k : X_k \\ x_k \notin \mathsf{dom}(\Gamma, x_1 \prec A_1, \ldots, x_{k-1} \prec A_{k-1})\end{array}}{\Gamma, x_1 \prec A_1, \ldots, x_k \prec A_k \vdash E : Z}$$

□

2.5.5 Strengthening (Lemma 2.4.6)

1 The lemma is: *if* $\Gamma, x \prec A \vdash B : Y$ *and* $x \notin \mathsf{var}(B)$*, then* $\Gamma \vdash B : Y$*.*

The proof is by induction on typing derivations. The inductive hypothesis is: *for any shorter type derivation* $\Gamma \vdash B : Y$*, if* $\Gamma = \Gamma', x \prec A$ *for some* Γ', x *and* A*, and where* $x \notin \mathsf{var}(B)$*, then also* $\Gamma' \vdash B : Y$*.*

Base case. The base case is the rule axiom. Since here $\Gamma = \oslash$, it does not fit the condition $\Gamma = \Gamma', x \prec A$, and accordingly the lemma holds vacuously.

Inductive cases

- New.

  If $\Gamma', x \prec A \vdash B : Y$ is inferred by an application New, then we would have $B = \mathsf{new}\, x\cdot$ for some x, and also $\Gamma = \Gamma', x \prec A$ for some Γ' and A, and the same x. This does not fit the conditions in the lemma, so the lemma holds.

- Del.

  Assume the last step in the derivation of $\Gamma', x \prec A \vdash B : Y$ is

$$\frac{\Gamma', x \prec A \vdash C : Z \qquad y \prec C \in \Gamma', x \prec A}{\Gamma', x \prec A \vdash \mathsf{del}\, y\cdot : \langle [y], [], [-y] \rangle} \text{(Del)}$$

This means we would have $B = \mathsf{del}\, y\cdot$ for some y. $y \neq x$ follows from the condition that $x \notin \mathsf{var}(B)$. Since $x \neq y$, we must have that $\Gamma' = \Delta, y \prec C, \Delta'$ for some Δ and Δ'. From weakening (lemma 2.4.5), clause 1, we then get $\Delta \vdash C : W$ for some type W. From valid typing (lemma 2.4.2) we then further get that $x \notin \mathsf{var}(C)$. This means we can use the inductive hypothesis to get $\Gamma' \vdash C : Z$. Now use this in a new application of Del:

$$\frac{\Gamma' \vdash C : Z \qquad y \prec C \in \Gamma'}{\Gamma' \vdash \mathsf{del}\, y\cdot : \langle [y], [], [-y] \rangle} \text{(Del)}$$

- WeakenB.

  Assume the last step in the derivation of $\Gamma', x \prec A \vdash B : Y$ is

  $$\frac{\Gamma' \vdash B : Y \qquad \Gamma' \vdash A : X \quad x \notin \mathsf{dom}(\Gamma')}{\Gamma', x \prec A \vdash B : Y} \text{(WeakenB)}$$

  with $x \notin \mathsf{var}(B)$. In this case, $\Gamma' \vdash B : Y$ is a premise, so the lemma holds directly by the inductive hypothesis.

- Parallel.

  Assume the last step in the derivation of $\Gamma', x \prec A \vdash B : Y$ is:

  $$\frac{\Gamma', x \prec A \vdash C : V \qquad \Gamma', x \prec A \vdash D : W}{\Gamma', x \prec A \vdash (C \,||\, D)\cdot : V + W} \text{(Parallel)}$$

  Since $x \notin \mathsf{var}((C||D)\cdot)$ implies $x \notin \mathsf{var}(C)$ and $x \notin \mathsf{var}(D)$, I can by induction hypothesis on the premises assume that $\Gamma' \vdash C : V$ and $\Gamma' \vdash D : W$. Apply Parallel to this:

  $$\frac{\Gamma' \vdash C : V \qquad \Gamma' \vdash D : W}{\Gamma' \vdash (C \,||\, D)\cdot : V + W} \text{(Parallel)}$$

- Seq.

  Assume the last step in the derivation of $\Gamma \vdash B : Y$ is:

  $$\frac{\Gamma', x \prec A \vdash C\cdot : V \qquad \Gamma', x \prec A \vdash D\cdot : W}{\Gamma', x \prec A \vdash C \cdot D\cdot : \langle V^n \cup (W^n - V^a), V^p \cup (V^a + W^p), V^a + W^a \rangle} \text{(Seq)}$$

  Here, Γ', x and A are the same as in the induction hypothesis and $X = \langle V^n \cup (W^n - V^a), V^p \cup (V^a + W^p), V^a + W^a \rangle$. Since the premises have shorter typing derivations and cannot contain more variables than the

conclusion, I can apply the induction hypothesis and get that $\Gamma' \vdash C\cdot : V$ and $\Gamma' \vdash D\cdot : W$. Apply SEQ to this to get:

$$\text{(SEQ)}\quad \frac{\Gamma' \vdash C\cdot : V \qquad \Gamma' \vdash D\cdot : W}{\Gamma' \vdash C \cdot D\cdot : \langle V^n \cup (W^n - V^a), V^p \cup (V^a + W^p), V^a + W^a\rangle}$$

□

2 The lemma is: *if* $\Gamma = x_1 \prec A_1, \ldots, x_n \prec A_n$ *is a legal basis and* $x \notin \mathsf{dom}(\Gamma)$*, then for all* i*, where* $1 \leq i \leq n$*, we have that* $x \notin \mathsf{var}(A_i)$*.*

Proof. For any i, where $1 \leq i \leq n$, we have that $\Gamma = \Delta, x_i \prec A_i, \Delta'$ for some possibly empty sequences of declarations Δ and Δ'. From Γ a legal basis we know that for some expression E and type X we have $\Delta, x_i \prec A_i, \Delta' \vdash E : X$. From this we can use weakening, lemma 2.4.5, clause 1, to get that $\Delta \vdash A_i : X_i$ for some X_i. Since Δ is an initial sequence of Γ, we must have $\mathsf{dom}(\Delta) \subseteq \mathsf{dom}(\Gamma)$ and therefore $x \notin \mathsf{dom}(\Delta)$. From valid typing, lemma 2.4.2, and $\Delta \vdash A_i : X_i$ we have that $\mathsf{var}(A_i) \subseteq \mathsf{dom}(\Delta)$, which implies $x \notin \mathsf{var}(A_i)$. □

2.5.6 Uniqueness (Lemma 2.4.8)

Let Γ *and* Γ' *be reorderings of subsets of the same valid set of declarations. If* $\Gamma \vdash A : X$ *and* $\Gamma' \vdash A : Y$*, then* $X = Y$*.*

Proof. Note that a valid set of declarations (defined on page 15) implies there is at most one declaration for each component. Let S be a valid set of declarations containing all declarations in Γ and Γ'. The proof is by induction on the typing derivation of $\Gamma \vdash A : X$.

The inductive hypothesis is: *for any shorter typing derivations* $\Gamma \vdash A : X$*, if for some* $\Gamma' \vdash A : Y$*, where* Γ *and* Γ' *are reorderings of subsets of* S*, then we have that* $X = Y$*.*

- The base case is AXIOM: $\oslash \vdash \epsilon : \langle [], [], []\rangle$. This means that $\Gamma = \oslash$ and $A = \epsilon$. Now, this means the other derivation is $\Gamma' \vdash \epsilon : Y$, and then we have by generation lemma (2.4.4) for ϵ that $Y = \langle [], [], []\rangle = X$.

  The inductive cases are the following:

- Assume $\Gamma \vdash A : X$ is inferred by:

  $$\text{(NEW)}\quad \frac{\Delta \vdash B : Z \quad x \notin \mathsf{dom}(\Delta)}{\Delta, x \prec B \vdash \mathsf{new}\, x\cdot : \langle Z^n, Z^p + x, Z^a + x\rangle}$$

  Now, this means the other derivation is $\Gamma' \vdash \mathsf{new}\, x\cdot : Y$. From the generation lemma (2.4.4) for new I have the existence of Δ_1, Δ_2, C and V such that $\Gamma' = \Delta_1, x \prec C, \Delta_2$ and $\Delta_1 \vdash C : V$ and $Y = \langle V^n, V^p + x, V^a + x\rangle$. Now, since Γ and Γ' are reorderings of subsets of S and there cannot be more than one declaration of x in a valid set of declarations, we must have $C = B$, and we must also have that Δ and Δ_1 are reorderings of subsets of S. This implies by the inductive hypothesis applied to $\Delta \vdash B : Z$ that $Z = V$, so I get $Y = \langle Z^n, Z^p + x, Z^a + x\rangle = X$.

- Assume $\Gamma \vdash A : X$ is inferred by:

$$\frac{\begin{array}{l}(\textsc{Del})\\ \Gamma \vdash B : Z \qquad x \prec B \in \Gamma\end{array}}{\Gamma \vdash \mathsf{del}\, x\cdot : \langle [x], [], [-x] \rangle}$$

  This means the other derivation is $\Gamma' \vdash \mathsf{del}\, x\cdot : Y$. We then have from the generation lemma (2.4.4) for del that $Y = \langle [x], [], [-x] \rangle = X$.

- Assume $\Gamma \vdash A : X$ is inferred by:

$$\frac{\begin{array}{l}(\textsc{Parallel})\\ \Gamma \vdash B : Z \qquad \Gamma \vdash C : V\end{array}}{\Gamma \vdash (B \,||\, C)\cdot : Z + V}$$

  Now, the other typing judgement is $\Gamma' \vdash (B \,||\, C)\cdot : Y$. I have from the generation lemma (2.4.4) for parallel that there are Z' and V' such that $\Gamma' \vdash B : Z'$, $\Gamma' \vdash C : V'$ and $Y = Z' + V'$. I can use the inductive hypothesis on $\Gamma \vdash B : Z$ to get $Z' = Z$ and on $\Gamma \vdash C : V$ to get $V' = V$. This means $Y = Z' + V' = Z + V = X$.

- Assume $\Gamma \vdash A : X$ is inferred by:

$$\frac{\begin{array}{l}(\textsc{Seq})\\ \qquad\qquad \Gamma \vdash B\cdot : Z \qquad \Gamma \vdash C\cdot : V\end{array}}{\Gamma \vdash B \cdot C\cdot : \langle Z^n \cup (V^n - Z^a), Z^p \cup (V^p + Z^a), Z^a + V^a \rangle}$$

  Now the other typing judgement is $\Gamma' \vdash B \cdot C\cdot : Y$. I have from the generation lemma (2.4.4) for sequencing that there are Z' and V' such that $\Gamma' \vdash B\cdot : Z'$, $\Gamma' \vdash C\cdot : V'$ and $Y = \langle Z'^n \cup (V'^n - Z'^a), Z'^p \cup (V'^p + Z'^a), Z'^a + V'^a \rangle$. I can use the inductive hypothesis on $\Gamma \vdash B\cdot : Z$ to get $Z' = Z$ and on $\Gamma \vdash C\cdot : V$ to get $V' = V$. This means $\langle Z'^n \cup (V'^n - Z'^a), Z'^p \cup (V'^p + Z'^a), Z'^a + V'^a \rangle = \langle Z^n \cup (V^n - Z^a), Z^p \cup (V^p + Z^a), Z^a + V^a \rangle$ which implies $Y = X$.

- Assume $\Gamma \vdash A : X$ is inferred by:

$$\frac{\begin{array}{l}(\textsc{WeakenB})\\ \Delta \vdash A : X \quad \Delta \vdash B : Z \quad x \notin \mathsf{dom}(\Delta)\end{array}}{\Delta, x \prec B \vdash A : X}$$

  Now the other typing judgement is $\Gamma' \vdash A : Y$ for Γ' some other reordering of some subset of S. We have $X = Y$ directly from the inductive hypothesis.

□

2.6 Proofs of configuration properties

2.6.1 Proof of property of $\mathsf{expr}(\mathbb{T})$ (Lemma 2.4.10)

The lemma is: *if* $E = \mathsf{expr}(\mathbb{T})$*, then there is a run of* E *in context* $([], E)$ *where after only applying rules* osParIntr *and* osParElim$*$ *we get a configuration of the form* $([], \mathbb{T})$.

Proof. By induction on the tree $\mathbb{T}$. The inductive hypothesis is somewhat stronger. To get the lemma from the hypothesis, use $\alpha = \bullet$. The induction hypothesis is: *for any smaller tree* $\mathbb{T}$*, is is the case that if* $E = \mathsf{expr}(\mathbb{T})$*,* $\mathbb{R}$ *some tree and* α *some position in it, then there is a run of* E *in context* $\mathbb{R}$*, position* α *and starting with store* M *where after only applying rules* osParIntr *and* osParElim$*$ *we get a configuration of the form* $(M, \mathbb{R}[\mathbb{T}]_\alpha)$*.*

- Base case. This is the case when $\mathbb{T} = \mathsf{Lf}(E')$. Then we have $E = \mathsf{expr}(\mathsf{Lf}(E')) = E'$. This means that this first configuration in any run of E has the properties needed.
- $\mathbb{T} = \mathsf{Nd}(E', \mathbb{T}')$. Then we have $E = \mathsf{expr}(\mathbb{T}) = (\epsilon||\mathsf{expr}(\mathbb{T}'))E'$. The first two transitions in a run of E could be

$$\begin{array}{l}(M, \mathbb{R}[\mathsf{Lf}((\epsilon||\mathsf{expr}(\mathbb{T}'))E')]_\alpha) \to (M, \mathbb{R}[\mathsf{Nd}(E', \mathsf{Lf}(\epsilon), \mathsf{Lf}(\mathsf{expr}(\mathbb{T}')))]_\alpha) \\ \to (M, \mathbb{R}[\mathsf{Nd}(E', \mathsf{Lf}(\mathsf{expr}(\mathbb{T}')))]_\alpha)\end{array} \tag{2.8}$$

  Since $\mathbb{T}'$ is smaller than $\mathbb{T}$, we have from inductive hypothesis that there is a run of $\mathsf{expr}(\mathbb{T}')$ in context $(M, \mathbb{R}[\mathsf{Nd}(E', \mathsf{Lf}(\mathsf{expr}(\mathbb{T}')))]_\alpha)$ and position αc where after only using the allowed transitions we get a configuration:

$$\cdots \to (M, \mathbb{R}[\mathsf{Nd}(E', \mathbb{T}')]_\alpha) = (M, \mathbb{R}[\mathbb{T}]_\alpha)$$

  By appending these with the two transitions from (2.8) above we get the needed transitions and configuration.

- $\mathbb{T} = \mathsf{Nd}(E', \mathbb{T}', \mathbb{T}'')$. Then we have $E = \mathsf{expr}(\mathbb{T}) = (\mathsf{expr}(\mathbb{T}')||\mathsf{expr}(\mathbb{T}''))E'$. The first transition in a run of E could be

$$\begin{array}{l}(M, \mathbb{R}[\mathsf{Lf}((\mathsf{expr}(\mathbb{T}')||\mathsf{expr}(\mathbb{T}''))E')]_\alpha) \\ \to (M, \mathbb{R}[\mathsf{Nd}(E', \mathsf{Lf}(\mathsf{expr}(\mathbb{T}')), \mathsf{Lf}(\mathsf{expr}(\mathbb{T}'')))]_\alpha)\end{array}$$

  Since both $\mathbb{T}'$ and $\mathbb{T}''$ are smaller than $\mathbb{T}$, we have from inductive hypothesis that there is a run of $\mathsf{expr}(\mathbb{T}')$ in the context above and position αl where we reach configuration

$$(M, \mathbb{R}[\mathsf{Nd}(E', \mathbb{T}', \mathsf{Lf}(\mathsf{expr}(\mathbb{T}'')))]_\alpha) \tag{2.9}$$

  after only using the allowed transitions. And we have that there is a run of $\mathsf{expr}(\mathbb{T}'')$ in this new context (2.9) and position αr where we reach a configuration

$$(M, \mathbb{R}[\mathsf{Nd}(E', \mathbb{T}', \mathbb{T}'')]_\alpha) = (M, \mathbb{R}[\mathbb{T}]_\alpha)$$

  By appending these two sequences of configurations and the first osParIntr above, we get the needed transitions and configuration.

□

2.6.2 Typability of trees (Lemma 2.4.12)

I have a Γ, such that for every position α in the tree $\mathbb{T}$, there exists a type $\tau(\mathbb{T}(\alpha))$ such that $\Gamma \vdash \mathbb{T}(\alpha) : \tau(\mathbb{T}(\alpha))$. I want to show that

1. There exist $\tau(\mathbb{T})$, such that $\Gamma \vdash \mathsf{expr}(\mathbb{T}) : \tau(\mathbb{T})$.

2.
$$\tau(\mathbb{T})^a = \sum_{\alpha \in \mathbb{T}} \tau(\mathbb{T}(\alpha))^a$$

I will use induction on the structure of a tree.

- The base case is only one leaf: $\mathbb{T} = \mathsf{Lf}(E)$. In this case it is easy, as the expression of this tree is exactly the expression in the root: $\mathsf{expr}(\mathbb{T}) = E$, which we know from the assumptions has a type. Secondly, the only possible value for α is the root $\bullet$, and we have $\tau(\mathbb{T}) = \tau(\mathbb{T}(\bullet))$.

- The first inductive case is where there are two branches from the root: $\mathbb{T} = \mathsf{Nd}(E_\bullet, \mathbb{T}_l, \mathbb{T}_r)$.

  1. From the inductive hypothesis I know that $\Gamma \vdash \mathsf{expr}(\mathbb{T}_l) : \tau(\mathbb{T}_l)$ and $\Gamma \vdash \mathsf{expr}(\mathbb{T}_r) : \tau(\mathbb{T}_r)$. We have $\mathsf{expr}(\mathbb{T}) = (\mathsf{expr}(\mathbb{T}_l)||\mathsf{expr}(\mathbb{T}_r)) \cdot E_\bullet$. Then from an application of $\mathsf{Parallel}$ I get:

  $$\frac{\Gamma \vdash \mathsf{expr}(\mathbb{T}_l) : \tau(\mathbb{T}_l) \quad \Gamma \vdash \mathsf{expr}(\mathbb{T}_r) : \tau(\mathbb{T}_r)}{\Gamma \vdash (\mathsf{expr}(\mathbb{T}_l)||\mathsf{expr}(\mathbb{T}_r))\cdot : \tau(\mathbb{T}_l) + \tau(\mathbb{T}_r)}$$

  Further I have from assumptions that $\Gamma \vdash E_\bullet : X_\bullet$ and by applying Seq I will get:

  $$\Gamma \vdash (\mathsf{expr}(\mathbb{T}_l)||\mathsf{expr}(\mathbb{T}_r)) \cdot E_\bullet : \quad \begin{array}{l} \langle (\tau(\mathbb{T}_l)^n + \tau(\mathbb{T}_r)^n) \cup (X_\bullet^n - \tau(\mathbb{T}_l)^a - \tau(\mathbb{T}_r)^a), \\ (\tau(\mathbb{T}_l)^p + \tau(\mathbb{T}_r)^p) \cup (\tau(\mathbb{T}_l)^a + \tau(\mathbb{T}_r)^a + X_\bullet^p), \\ \tau(\mathbb{T}_l)^a + \tau(\mathbb{T}_r)^a + X_\bullet^a \rangle \end{array}$$

  2. From the inductive hypothesis I know that

  $$\sum_{\alpha \in \mathbb{T}_l} \tau(\mathbb{T}_l(\alpha))^a = \tau(\mathbb{T}_l)^a$$
  $$\sum_{\alpha \in \mathbb{T}_r} \tau(\mathbb{T}_r(\alpha))^a = \tau(\mathbb{T}_r)^a$$

  Further I have from item 1 that $\tau(\mathbb{T})^a = \tau(\mathbb{T}_l)^a + \tau(\mathbb{T}_r)^a + X_\bullet^a$ for $X_\bullet = \tau(\mathbb{T}(\bullet))$ and from the structure of the tree that

  $$\sum_{\alpha \in \mathbb{T}} \tau(\mathbb{T}(\alpha))^a = X_\bullet^a + \sum_{\alpha \in \mathbb{T}_l} \tau(\mathbb{T}_l(\alpha))^a + \sum_{\alpha \in \mathbb{T}_r} \tau(\mathbb{T}_r(\alpha))^a$$

  All in all this gives me

  $$\begin{aligned} \sum_{\alpha \in \mathbb{T}} \tau(\mathbb{T}(\alpha))^a = \\ X_\bullet^a + \sum_{\alpha \in \mathbb{T}_l} \tau(\mathbb{T}_l(\alpha))^a + \sum_{\alpha \in \mathbb{T}_r} \tau(\mathbb{T}_r(\alpha))^a = \\ X_\bullet^a + \tau(\mathbb{T}_l)^a + \tau(\mathbb{T}_r)^a = \\ \tau(\mathbb{T})^a \end{aligned}$$

- The other inductive case is where there is one branch from the root: $\mathbb{T} = \mathsf{Nd}(E_\bullet, \mathbb{T}_c)$.

  1. From the inductive hypothesis I know that $\Gamma \vdash \mathsf{expr}(\mathbb{T}_c) : \tau(\mathbb{T}_c)$. We have $\mathsf{expr}(\mathbb{T}) = (\mathsf{expr}(\mathbb{T}_c)||\epsilon)\cdot E_\bullet$. Then from an application of Parallel I get:
  $$\frac{\Gamma \vdash \mathsf{expr}(\mathbb{T}_c) : \tau(\mathbb{T}_c) \quad \Gamma \vdash \epsilon : \langle [], [], [] \rangle}{\Gamma \vdash (\mathsf{expr}(\mathbb{T}_c)||\epsilon)\cdot : \tau(\mathbb{T}_c)}$$
  Further I have from assumptions that $\Gamma \vdash E_\bullet : X_\bullet$ and by applying Seq I will get:
  $$\Gamma \vdash (\mathsf{expr}(\mathbb{T}_c)||\epsilon)\cdot E_\bullet : \begin{array}{l} \langle (\tau(\mathbb{T}_c)^n \cup (X^n - \tau(\mathbb{T}_c)^a), \\ \tau(\mathbb{T}_c)^p \cup (\tau(\mathbb{T}_c)^a + X_\bullet^p), \\ \tau(\mathbb{T}_c)^a + X_\bullet^a \rangle \end{array}$$

  2. From the inductive hypothesis I know that $\sum_{\alpha\in\mathbb{T}_c} \tau(\mathbb{T}_c(\alpha))^a = \tau(\mathbb{T}_c)^a$. Further I have from item 1 that $\tau(\mathbb{T})^a = \tau(\mathbb{T}_c)^a + X_\bullet^a$ for $X_\bullet = \tau(\mathbb{T}(\bullet))$ and from the structure of the tree that $\sum_{\alpha\in\mathbb{T}} \tau(\mathbb{T}(\alpha))^a = X_\bullet^a + \sum_{\alpha\in\mathbb{T}_c} \tau(\mathbb{T}_c(\alpha))^a$.
  All in all this gives me
  $$\begin{aligned} \sum_{\alpha\in\mathbb{T}} \tau(\mathbb{T}(\alpha))^a = \\ X_\bullet^a + \sum_{\alpha\in\mathbb{T}_c} \tau(\mathbb{T}_c(\alpha))^a = \\ X_\bullet^a + \tau(\mathbb{T}_c)^a = \\ \tau(\mathbb{T})^a \end{aligned}$$

  □

2.7 Proofs of soundness properties

Before I can prove the invariance theorem (2.4.15), I need an auxiliary lemma. In a way, this is a generalisation of the two first cases (osNew and osDel) in the proof of the invariance lemma below.

Lemma 2.7.1 (Change in leaf equals change in tree). *Let there be two well-typed trees $\mathbb{T} = \mathbb{R}[\mathsf{Lf}(E)]_\beta$ and $\mathbb{T}' = \mathbb{R}[\mathsf{Lf}(E')]_\beta$, which are equal except for the expression in the leaf β. Remember we can assume from well-typed (Definition 2.4.11) that there are Γ, X, Γ' and X' such that $\Gamma \vdash E : X$ and $\Gamma' \vdash E' : X'$ and that there is $\tau(\mathbb{T})$ and $\tau(\mathbb{T}')$ such that $\Gamma \vdash \mathsf{expr}(\mathbb{T}) : \tau(\mathbb{T})$ and $\Gamma' \vdash \mathsf{expr}(\mathbb{T}) : \tau(\mathbb{T})$. The following holds ($[x \mapsto c]$ stands for the hybrid set in which x has multiplicity c.)*

1. *If for some integer c it is the case that $X^n = X'^n + [x \mapsto c]$ and $X^a = X'^a - [x \mapsto c]$ then also $\tau(\mathbb{T})^n = \tau(\mathbb{T}')^n + [x \mapsto c]$ and $\tau(\mathbb{T})^a = \tau(\mathbb{T}')^a - [x \mapsto c]$.*
2. *If for some integer d it is the case that $X^n = X'^n$ and $X^a = X'^a + [x \mapsto d]$, then $\tau(\mathbb{T})^n \supseteq \tau(\mathbb{T}')^n - [x \mapsto d]$ and $\tau(\mathbb{T})^a = \tau(\mathbb{T}')^a + [x \mapsto d]$.*

3. *If for some integer e it is the case that* $X^p = X'^p - [x \mapsto e]$ *and* $X^a = X'^a - [x \mapsto e]$ *then also* $\tau(\mathbb{T})^p = \tau(\mathbb{T}')^p - [x \mapsto e]$ *and* $\tau(\mathbb{T})^a = \tau(\mathbb{T}')^a - [x \mapsto e]$.

4. *If for some integer f it is the case that* $X^p = X'^p$ *and* $X^a = X'^a - [x \mapsto f]$, *then* $\tau(\mathbb{T})^p \supseteq \tau(\mathbb{T}')^p - [x \mapsto f]$ *and* $\tau(\mathbb{T})^a = \tau(\mathbb{T}')^a - [x \mapsto f]$.

Although I will prove the general case, where c, d, e and f can be any integers, we will only use the cases where they have value $1, 0$ or -1. Note that in $X = X' + [x \mapsto c]$ only the number of x counts and that the number of instances of all other components are unchanged between X and X', both in the premise and in the conclusion.

2.7.1 Proof of lemma 2.7.1

The proof will be by structural induction on the size of the tree $\mathbb{R}$. The inductive hypothesis is:

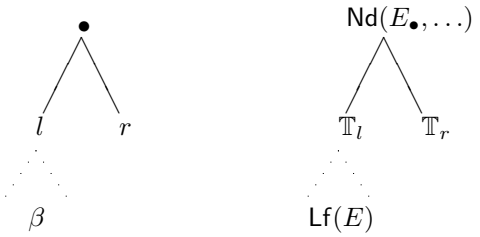
> Let there be a smaller well-typed tree $\mathbb{R}$ and any two well-typed trees $\mathbb{T} = \mathbb{R}[\mathsf{Lf}(E)]_\beta$ and $\mathbb{T}' = \mathbb{R}[\mathsf{Lf}(E')]_\beta$. The two trees are equal except for the expression in position β. I can assume $\Gamma \vdash E : X$ and $\Gamma' \vdash E' : X'$ and $\Gamma \vdash \mathsf{expr}(\mathbb{T}) : \tau(\mathbb{T})$ and $\Gamma' \vdash \mathsf{expr}(\mathbb{T}') : \tau(\mathbb{T}')$. Then it holds that:
>
> 1. If for some integer c it is the case that $X^n = X'^n + [x \mapsto c]$ and $X^a = X'^a - [x \mapsto c]$ then also $\tau(\mathbb{T})^n = \tau(\mathbb{T}')^n + [x \mapsto c]$ and $\tau(\mathbb{T})^a = \tau(\mathbb{T}')^a - [x \mapsto c]$.
> 2. If for some integer d it is the case that $X^n = X'^n$ and $X^a = X'^a + [x \mapsto d]$, then $\tau(\mathbb{T})^n \supseteq \tau(\mathbb{T}')^n - [x \mapsto d]$ and $\tau(\mathbb{T})^a = \tau(\mathbb{T}')^a + [x \mapsto d]$.
> 3. If for some integer e it is the case that $X^p = X'^p - [x \mapsto e]$ and $X^a = X'^a - [x \mapsto e]$ then also $\tau(\mathbb{T})^p = \tau(\mathbb{T}')^p - [x \mapsto e]$ and $\tau(\mathbb{T})^a = \tau(\mathbb{T}')^a - [x \mapsto e]$.
> 4. If for some integer f it is the case that $X^p = X'^p$ and $X^a = X'^a - [x \mapsto f]$, then $\tau(\mathbb{T})^p \supseteq \tau(\mathbb{T}')^p - [x \mapsto f]$ and $\tau(\mathbb{T})^a = \tau(\mathbb{T}')^a - [x \mapsto f]$.

- The base case $\mathbb{T} = \mathsf{Lf}(E)$, the smallest tree consisting of a single leaf, is easy, as $\tau(\mathbb{T}) = X$ and $\tau(\mathbb{T}') = X'$.

- There are two inductive cases. The first, and most complex, is a tree with two branches.

  $$\mathbb{T} = \mathsf{Nd}(E_\bullet, \mathbb{T}_l, \mathbb{T}_r)$$

  Since the change is limited to one leaf, this means that β must be a leaf in one of the two subtrees. Remember the root is $\bullet$. β will now be a leaf in one of the two smaller subtrees rooted in l and r:



As seen above, I will treat the case where $\beta = l\ldots$, namely in the left subtree. The other case is symmetric and can be treated by swapping l and r in the text. The expression in the root, $E_\bullet$, and the whole right subtree, $\mathbb{T}_r$, is equal in both trees, so we could have used that the change was between a leaf of $\mathbb{T}_l = \mathbb{R}_l[\mathsf{Lf}(E)]_{\beta'}$ and $\mathbb{T}'_l = \mathbb{R}_l[\mathsf{Lf}(E')]_{\beta'}$, where $\beta = l\beta'$. I then get:

$$\mathbb{T}' = \mathsf{Nd}(E_\bullet, \mathbb{T}'_l, \mathbb{T}_r)$$

Directly from $\mathbb{T}$ and $\mathbb{T}'$ well-typed (Definition 2.4.11) we get the existence of an $X_\bullet$ such that $\Gamma \vdash E_\bullet : X_\bullet$.

I now want to be able to use the inductive hypothesis on the smaller subtree $\mathbb{T}_l$. That $\mathbb{T}_l$ and $\mathbb{T}'_l$ are well-typed follows from $\mathbb{T}$ and $\mathbb{T}'$ well-typed, respectively. This means I can use the inductive hypothesis on $\mathbb{T}_l$ and $\mathbb{T}'_l$. From $\mathbb{T}$ and $\mathbb{T}'$ well-typed and tree typing (Lemma 2.4.12) I get the existence of $\tau(\mathbb{T}_r)$, $\tau(\mathbb{T}_l)$ and $\tau(\mathbb{T}'_l)$ such that $\Gamma \vdash \mathsf{expr}(\mathbb{T}_r) : \tau(\mathbb{T}_r)$, $\Gamma \vdash \mathsf{expr}(\mathbb{T}_l) : \tau(\mathbb{T}_l)$ and $\Gamma' \vdash \mathsf{expr}(\mathbb{T}'_l) : \tau(\mathbb{T}'_l)$. We then have

$$\mathsf{expr}(\mathbb{T}) = (\mathsf{expr}(\mathbb{T}_l)||\mathsf{expr}(\mathbb{T}_r)) \cdot E_\bullet$$

$$\mathsf{expr}(\mathbb{T}') = (\mathsf{expr}(\mathbb{T}'_l)||\mathsf{expr}(\mathbb{T}_r)) \cdot E_\bullet$$

I will now try to type these two expressions and see what their difference is. An application of Parallel gives:

$$\begin{aligned}&\Gamma \vdash (\mathsf{expr}(\mathbb{T}_l)||\mathsf{expr}(\mathbb{T}_r))\cdot : \tau(\mathbb{T}_l) + \tau(\mathbb{T}_r) = \\ &\langle \tau(\mathbb{T}_l)^n + \tau(\mathbb{T}_r)^n, \tau(\mathbb{T}_l)^p + \tau(\mathbb{T}_r)^p, \tau(\mathbb{T}_l)^a, \tau(\mathbb{T}_r)^a \rangle\end{aligned}$$

and further from Seq:

$$\begin{aligned}\Gamma \vdash (\mathsf{expr}(\mathbb{T}_l)||\mathsf{expr}(\mathbb{T}_r)) \cdot E_\bullet : \quad & \langle (\tau(\mathbb{T}_l)^n + \tau(\mathbb{T}_r)^n) \cup (X_\bullet^n - \tau(\mathbb{T}_l)^a - \tau(\mathbb{T}_r)^a), \\ & (\tau(\mathbb{T}_l)^p + \tau(\mathbb{T}_r)^p) \cup (X_\bullet^p + \tau(\mathbb{T}_l)^a + \tau(\mathbb{T}_r)^a), \\ & \tau(\mathbb{T}_l)^a + \tau(\mathbb{T}_r)^a + X_\bullet^a \rangle \\ = \quad & \tau(\mathbb{T})\end{aligned}$$

In the same way I can find $\tau(\mathbb{T}')$:

$$\begin{aligned}\Gamma \vdash (\mathsf{expr}(\mathbb{T}'_l)||\mathsf{expr}(\mathbb{T}_r))E_\bullet : \quad & \langle (\tau(\mathbb{T}'_l)^n + \tau(\mathbb{T}_r)^n) \cup (X_\bullet^n - \tau(\mathbb{T}'_l)^a - \tau(\mathbb{T}_r)^a), \\ & (\tau(\mathbb{T}'_l)^p + \tau(\mathbb{T}_r)^p) \cup (X_\bullet^p + \tau(\mathbb{T}'_l)^a + \tau(\mathbb{T}_r)^a), \\ & \tau(\mathbb{T}'_l)^a + \tau(\mathbb{T}_r)^a + X_\bullet^a \rangle \\ = \quad & \tau(\mathbb{T}')\end{aligned}$$

In the last step I have to consider the different cases in the lemma separately:

1. I have $X^n = X'^n + [x \mapsto c]$ and $X^a = X'^a - [x \mapsto c]$ for some constant c. From the inductive hypothesis I have $\tau(\mathbb{T}_l)^n = \tau(\mathbb{T}'_l)^n + [x \mapsto c]$ and $\tau(\mathbb{T}_l)^a = \tau(\mathbb{T}'_l)^a - [x \mapsto c]$. I have to prove that $\tau(\mathbb{T})^n = \tau(\mathbb{T}')^n + [x \mapsto c]$ and $\tau(\mathbb{T})^a = \tau(\mathbb{T}')^a - [x \mapsto c]$.

$$\begin{aligned}
\tau(\mathbb{T})^n = &\ (\tau(\mathbb{T}_l)^n + \tau(\mathbb{T}_r)^n) \cup (X_\bullet^n - \tau(\mathbb{T}_l)^a - \tau(\mathbb{T}_r)^a) \\
= &\ (\tau(\mathbb{T}'_l)^n + [x \mapsto c] + \tau(\mathbb{T}_r)^n) \cup (X_\bullet^n - (\tau(\mathbb{T}'_l)^a - [x \mapsto c]) - \tau(\mathbb{T}_r)^a) \\
= &\ (\tau(\mathbb{T}'_l)^n + [x \mapsto c] + \tau(\mathbb{T}_r)^n) \cup (X_\bullet^n - \tau(\mathbb{T}'_l)^a + [x \mapsto c] - \tau(\mathbb{T}_r)^a) \\
= &\ (\tau(\mathbb{T}'_l)^n + \tau(\mathbb{T}_r)^n) \cup (X_\bullet^n - \tau(\mathbb{T}'_l)^a - \tau(\mathbb{T}_r)^a) + [x \mapsto c] \\
= &\ \tau(\mathbb{T}')^n + [x \mapsto c]
\end{aligned}$$

$$\begin{aligned}
\tau(\mathbb{T})^a = &\ \tau(\mathbb{T}_l)^a + \tau(\mathbb{T}_r)^a + X_\bullet^a \\
= &\ \tau(\mathbb{T}'_l)^a + -[x \mapsto c] + \tau(\mathbb{T}_r)^a + X_\bullet^a \\
= &\ \tau(\mathbb{T}')^a - [x \mapsto c]
\end{aligned}$$

2. I have $X^n = X'^n$ and $X^a = X'^a + [x \mapsto d]$ for some constant d. From the inductive hypothesis I have $\tau(\mathbb{T}_l)^n \supseteq \tau(\mathbb{T}'_l)^n - [x \mapsto d]$ and $\tau(\mathbb{T}_l)^a = \tau(\mathbb{T}'_l)^a + [x \mapsto d]$. I have to prove that $\tau(\mathbb{T})^n \supseteq \tau(\mathbb{T}')^n - [x \mapsto d]$ and $\tau(\mathbb{T})^a = \tau(\mathbb{T}')^a + [x \mapsto d]$.

$$\begin{aligned}
\tau(\mathbb{T})^n = &\ (\tau(\mathbb{T}_l)^n + \tau(\mathbb{T}_r)^n) \cup (X_\bullet^n - \tau(\mathbb{T}_l)^a - \tau(\mathbb{T}_r)^a) \\
= &\ (\tau(\mathbb{T}_l)^n + \tau(\mathbb{T}_r)^n) \cup (X_\bullet^n - \tau(\mathbb{T}'_l)^a - [x \mapsto d] - \tau(\mathbb{T}_r)^a) \\
\supseteq &\ (\tau(\mathbb{T}'_l)^n - [x \mapsto d] + \tau(\mathbb{T}_r)^n) \cup (X_\bullet^n - \tau(\mathbb{T}'_l)^a - [x \mapsto d] - \tau(\mathbb{T}_r)^a) \\
= &\ (\tau(\mathbb{T}'_l)^n + \tau(\mathbb{T}_r)^n) \cup (X_\bullet^n - \tau(\mathbb{T}'_l)^a - \tau(\mathbb{T}_r)^a) - [x \mapsto d] \\
= &\ \tau(\mathbb{T}')^n - [x \mapsto d]
\end{aligned}$$

$$\begin{aligned}
\tau(\mathbb{T})^a = &\ \tau(\mathbb{T}_l)^a + \tau(\mathbb{T}_r)^a + X_\bullet^a \\
= &\ \tau(\mathbb{T}'_l)^a + [x \mapsto d] + \tau(\mathbb{T}_r)^a + X_\bullet^a \\
= &\ \tau(\mathbb{T}')^a + [x \mapsto d]
\end{aligned}$$

3. I have $X^p = X'^p - [x \mapsto c]$ and $X^a = X'^a - [x \mapsto c]$ for some constant c. From the inductive hypothesis I have $\tau(\mathbb{T}_l)^p = \tau(\mathbb{T}'_l)^p - [x \mapsto c]$ and $\tau(\mathbb{T}_l)^a = \tau(\mathbb{T}'_l)^a - [x \mapsto c]$. I have to prove that $\tau(\mathbb{T})^p = \tau(\mathbb{T}')^p - [x \mapsto c]$ and $\tau(\mathbb{T})^a = \tau(\mathbb{T}')^a - [x \mapsto c]$.

$$\begin{aligned}
\tau(\mathbb{T})^p = &\ (\tau(\mathbb{T}_l)^p + \tau(\mathbb{T}_r)^p) \cup (X_\bullet^p + \tau(\mathbb{T}_l)^a + \tau(\mathbb{T}_r)^a) \\
= &\ (\tau(\mathbb{T}'_l)^p - [x \mapsto c] + \tau(\mathbb{T}_r)^p) \cup (X_\bullet^p + \tau(\mathbb{T}'_l)^a - [x \mapsto c] + \tau(\mathbb{T}_r)^a) \\
= &\ (\tau(\mathbb{T}'_l)^p + \tau(\mathbb{T}_r)^p) \cup (X_\bullet^p + \tau(\mathbb{T}'_l)^a + \tau(\mathbb{T}_r)^a) - [x \mapsto c] \\
= &\ \tau(\mathbb{T}')^p - [x \mapsto c]
\end{aligned}$$

$$\begin{aligned}
\tau(\mathbb{T})^a = &\ \tau(\mathbb{T}_l)^a + \tau(\mathbb{T}_r)^a + X_\bullet^a \\
= &\ \tau(\mathbb{T}'_l)^a - [x \mapsto c] + \tau(\mathbb{T}_r)^a + X_\bullet^a \\
= &\ \tau(\mathbb{T}')^a - [x \mapsto c]
\end{aligned}$$

4. I have $X^p = X'^p$ and $X^a = X'^a - [x \mapsto f]$ for some integer f. From the inductive hypothesis I have $\tau(\mathbb{T}_l)^p \supseteq \tau(\mathbb{T}'_l)^p - [x \mapsto f]$ and $\tau(\mathbb{T}_l)^a = \tau(\mathbb{T}'_l)^a - [x \mapsto f]$. I have to prove that $\tau(\mathbb{T})^p \supseteq \tau(\mathbb{T}')^p - [x \mapsto f]$ and $\tau(\mathbb{T})^a = \tau(\mathbb{T}')^a - [x \mapsto f]$.

$$\begin{array}{rcl}
\tau(\mathbb{T})^p = & (\tau(\mathbb{T}_l)^p + \tau(\mathbb{T}_r)^p) \cup (X_\bullet^p + \tau(\mathbb{T}_l)^a + \tau(\mathbb{T}_r)^a) \\
= & (\tau(\mathbb{T}_l)^p + \tau(\mathbb{T}_r)^p) \cup (X_\bullet^p + \tau(\mathbb{T}'_l)^a - [x \mapsto f] + \tau(\mathbb{T}_r)^a) \\
\supseteq & (\tau(\mathbb{T}'_l)^p - [x \mapsto f] + \tau(\mathbb{T}_r)^p) \cup (X_\bullet^p + \tau(\mathbb{T}'_l)^a - [x \mapsto f] + \tau(\mathbb{T}_r)^a) \\
= & (\tau(\mathbb{T}'_l)^p + \tau(\mathbb{T}_r)^p) \cup (X_\bullet^p + \tau(\mathbb{T}'_l)^a + \tau(\mathbb{T}_r)^a) - [x \mapsto f] \\
= & \tau(\mathbb{T}')^p - [x \mapsto f]
\end{array}$$

$$\begin{array}{rcl}
\tau(\mathbb{T})^a = & \tau(\mathbb{T}_l)^a + \tau(\mathbb{T}_r)^a + X_\bullet^a \\
= & \tau(\mathbb{T}'_l)^a - [x \mapsto f] + \tau(\mathbb{T}_r)^a + X_\bullet^a \\
= & \tau(\mathbb{T}')^a - [x \mapsto f]
\end{array}$$

- The other inductive case, is a node with one child, c:

  In this case, $\mathsf{expr}(\mathbb{T}) = (\epsilon||\mathsf{expr}(\mathbb{T}_c))E_\bullet = \mathsf{expr}(\mathsf{Nd}(E_\bullet, \mathsf{Lf}(\epsilon), \mathbb{T}_c))$. In other words: the expression of the tree is the same as if it was a node with two children, one which was a leaf with an empty expression. The type is also the same. This configuration is covered by the previous case. □

2.7.2 Invariance of $M - \tau(\mathbb{T})^n$, $M + \tau(\mathbb{T})^p$ and $M + \tau(\mathbb{T})^a$ (Lemma 2.4.15)

If $\Gamma \models (M, \mathbb{T})$ and $(M, \mathbb{T}) \longrightarrow (M', \mathbb{T}')$, then

1. $\mathsf{expr}(\mathbb{T}')$ has a type under the same basis — there exists $\tau(\mathbb{T}')$ such that $\Gamma \vdash \mathsf{expr}(\mathbb{T}') : \tau(\mathbb{T}')$.
2. $$\begin{array}{l} M - \tau(\mathbb{T})^n \subseteq M' - \tau(\mathbb{T}')^n \\ M + \tau(\mathbb{T})^p \supseteq M' + \tau(\mathbb{T}')^p \\ M + \tau(\mathbb{T})^a = M' + \tau(\mathbb{T}')^a \end{array}$$

The proof is by analysis of the reduction relation. Suppose reduction occurs at position β. Since $\mathbb{T}$ is well-typed, there exist $X = \langle X^n, X^p, X^a \rangle$, M and Γ such that $\Gamma \vdash \mathbb{T}(\beta) : X$ and $M \supseteq \mathbb{T}^n$. For item 1, I will only prove that the changed expression at node β and possibly the new leaves βl and βr have a type derived from the same basis. This will by typability of trees (2.4.12) imply that the whole tree has a type.

In item 2, I will use the types found in the first item. I will also use that we at this point will know that $\mathbb{T}$ is well-typed, often without mentioning it explicitly.

- Case osNew

(osNew) if $x \prec A \in Decls$
$(M, \mathbb{T}) = (M, \mathbb{R}[\mathsf{Lf}(\text{new } x \cdot E)]_\beta) \longrightarrow (M + x, \mathbb{R}[\mathsf{Lf}(AE)]_\beta) = (M + x, \mathbb{T}')$

1. Since $\mathbb{T}'(\beta) = AE$, we must prove that $\Gamma \vdash AE : Z$ for some Z. We have $\Gamma \vdash \text{new } x \cdot E : \langle X^n, X^p, X^a \rangle$. I must now do a case distinction on whether $E = \epsilon$.
   - $E \neq \epsilon$ By the generation lemma (2.4.4) for Seq, we get $\Gamma \vdash \text{new } x\cdot : X_1$ and $\Gamma \vdash E : X_2$ with
     $$X = \langle X_1^n \cup (X_2^n - X_1^a), X_1^p \cup (X_2^p + X_1^a), X_1^a + X_2^a \rangle$$
     for some X_1 and X_2. By the generation lemma for New applied to $\Gamma \vdash \text{new } x\cdot : X_1$ we have Y, Δ and Δ' s.t. $\Delta \vdash A : \langle X_1^n, Y^p, Y^a \rangle$, $X_1^p = Y^p + x$, $X_1^a = Y^a + x$ and $\Gamma = \Delta, x \prec A, \Delta'$. Since Δ is an initial sequence of Γ, by weakening (Lemma 2.4.5) we have $\Gamma \vdash A : \langle X_1^n, Y^p, Y^a \rangle$. I must now do a new case distinction on whether $A = \epsilon$.
     * If $A \neq \epsilon$ I can sequence A with E after the typing rule for Seq :
       $$\text{(Seq)} \quad \frac{\Gamma \vdash A : \langle X_1^n, Y^p, Y^a \rangle \qquad \Gamma \vdash E : X_2}{\Gamma \vdash AE : \langle X_1^n \cup (X_2^n - Y^a), Y^p \cup (Y^a + X_2^p), Y^a + X_2^a \rangle}$$
       Since $X_1^a = Y^a + x$ this means that $\Gamma \vdash AE : Z$ with
       $$Z = \langle X_1^n \cup (X_2^n - X_1^a + x), X_1^p \cup (X_1^a + X_2^p) - x, X_1^a - x + X_2^a \rangle$$
     * If $A = \epsilon$, I get that $AE = E$ and from this follows $Z = X_2$. Further, we then have from the generation lemma for ϵ that $Y = \langle [], [], [] \rangle$ (that is, $\Gamma \vdash A : \langle [], [], [] \rangle$) which implies $X_1 = \langle [], [x], [x] \rangle$ and $X = \langle [] \cup (Z^n - x), Z^p + x, Z^a + x \rangle$.
   - $E = \epsilon$. Then we have $\text{new}\, x \cdot E = \text{new}\, x\cdot$. By the generation lemma for New applied to $\Gamma \vdash \text{new } x\cdot : X$ we have Y, Δ and Δ' s.t. $\Delta \vdash A : \langle X^n, Y^p, Y^a \rangle$, $X^p = Y^p + x, X^a = Y^a + x$ and $\Gamma = \Delta, x \prec A, \Delta'$. Since Δ is an initial sequence of Γ, by weakening (Lemma 2.4.5) we have $\Gamma \vdash A : \langle X^n, Y^p, Y^a \rangle$. Since we have $AE = A$ I get $Z = \langle X^n, Y^p, Y^a \rangle = \langle X^n, X^p - x, X^a - x \rangle$. From the generation lemma for ϵ I also have $\Gamma \vdash E : X_2$ where $X_2 = \langle [], [], [] \rangle$.

   An argument about the relation between the different parts of Z and X follows. If you feel confident of this relation, skip the paragraph and go on to case 2.
   - If $A, E \neq \epsilon$, we have $Z^n(x) = \max(X_1^n(x), (X_2^n - X_1^a + x)(x))$ and since $X_1^a(x) = 1$, we get $Z^n(x) = \max(X_1^n(x), X_2^n(x))$ and further, since $X_1^n(x) = 0$ and X_2^n is unsigned, that $Z^n(x) = X_2^n(x)$. Using the same information we get $X^n(x) = X_1^n \cup (X_2^n - X_1^a)(x) = \max(0, X_2^n(x) - 1)$.
     On the other hand, note that $x \notin \mathsf{var}(A)$. This implies that the most negative change during AE must come during E. This means that we should have $Z^n(x) = X_2^n(x)$, which we also saw in the previous paragraph. Also, if there is a negative change in E, then in the total expression $\text{new}x \cdot E$, the total negative change

in x would be one less, assuming there is a negative change, that is:

$$X^n(x) = \begin{cases} 0 \text{ if } X_2^n(x) = 0 \\ X_2^n(x) - 1 \text{ if } X_2^n(x) > 0 \end{cases} \tag{2.10}$$

This implies:

$$X^n = \begin{cases} Z^n \text{ if } X_2^n(x) = 0 \\ Z^n - x \text{ if } X_2^n(x) > 0 \end{cases} \tag{2.11}$$

If $A = \epsilon$, we have $Z^n(x) = X_2^n(x)$ and $X^n(x) = \max(0, X_2^n(x) - 1)$ directly, and get the same discussion and result as above.
If $E = \epsilon$, we have $Z^n = X^n$, but I also have $X_2^n(x) = 0$, and from the discussion above I must also have $X^n(x) = Z^n(x) = 0$, so this fits with the formulas (2.10) and (2.11).
For $y \neq x$, it should be easy to see that $Z^n(y) = X^n(y)$. Remember that $X^n \supseteq []$, so $([] \cup (X^n - x))(y) = X^n(y)$.

– For X^p, we have, if $A, E \neq \epsilon$ that

$$X_1^a = Y^a + x$$
$$X_1^p = Y^p + x$$

And further that: $X^p = X_1^p \cup (X_1^a + X_2^p) = (Y^p + x) \cup (Y^a + x + X_2^p) = Y^p \cup (Y^a + X_2^p) + x = Z^p + x$.
If $A = \epsilon$ or $E = \epsilon$, we have $X^p = Z^p + x$ directly from the type given earlier.

– For X^a I have $X^a = Z^a + x$. If $A, E \neq \epsilon$ this follows from that $X^a = X_1^a + X_2^a = Y^a + x + X_a^2 = Z^a + x$, otherwise it comes directly from the types above.

2. I now have to prove the following:

$$M - \tau(\mathbb{T})^n \subseteq M' - \tau(\mathbb{T}')^n$$
$$M + \tau(\mathbb{T})^p \supseteq M' + \tau(\mathbb{T}')^p$$
$$M + \tau(\mathbb{T})^a = M' + \tau(\mathbb{T}')^a$$

To summarise, the changes in the configuration are on the one hand an increase in the store, that is: $M' = M + x$ and on the other hand that while $\mathbb{T}(\beta) = \mathsf{new}x \cdot E$, $\mathbb{T}'(\beta) = A\,E$. I also have $\Gamma \vdash AE : Z$ and $\Gamma \vdash \mathsf{new}x \cdot E : X$. Note that we also have the following equivalence:

$$M - \tau(\mathbb{T})^n \subseteq M' - \tau(\mathbb{T}')^n$$
$$\Leftrightarrow$$
$$-\tau(\mathbb{T})^n \subseteq x - \tau(\mathbb{T}')^n$$
$$\Leftrightarrow$$
$$\tau(\mathbb{T})^n \supseteq \tau(\mathbb{T}')^n - x$$

I now have to do a case distinction on the value of $X_2^n(x)$, where X_2 is the type of E. As seen above, the relation between $Z^n(x)$ and $X^n(x)$ depends on this.

– The first case is when $X_2^n(x) > 0$. Then we have after the argument in the previous item that $X^n = Z^n - x$.
If I could show that

$$\tau(\mathbb{T}') = \langle \tau(\mathbb{T})^n + x, \tau(\mathbb{T})^p - x, \tau(\mathbb{T})^a - x \rangle \tag{2.12}$$

I would be finished, as I then would get

$$\begin{aligned} M' - \tau(\mathbb{T}')^n &= M + x - (\tau(\mathbb{T})^n + x) = M - \tau(\mathbb{T})^n \\ M' + \tau(\mathbb{T}')^p &= M + x + (\tau(\mathbb{T})^p - x) = M + \tau(\mathbb{T})^p \\ M' + \tau(\mathbb{T}')^a &= M + x + (\tau(\mathbb{T})^a - x) = M + \tau(\mathbb{T})^a \end{aligned}$$

But I can use Lemma 2.7.1, clauses 1 with $c = -1$ and 3 with $e = -1$ to show the equation (2.12). This means the following:

(a) If it is the case that $X^n = Z^n - x$ and $X^a = Z^a + x$ then also $\tau(\mathbb{T})^n = \tau(\mathbb{T}')^n - x$ and $\tau(\mathbb{T})^a = \tau(\mathbb{T}')^a + x$.

(b) If it is the case that $X^p = Z^p + x$ and $X^a = Z^a + x$ then also $\tau(\mathbb{T})^p = \tau(\mathbb{T}')^p + x$ and $\tau(\mathbb{T})^a = \tau(\mathbb{T}')^a + x$.

For the premises I have that $Z^n = X^n + x$ from the case assumption, and from item 1 I have $Z^a = X^a - x$ and $Z^p = X^p - x$. That $\mathbb{T}$ and $\mathbb{T}'$ are well-typed follows from assumptions and 1. I then get $\tau(\mathbb{T}) = \langle \tau(\mathbb{T}')^n - x, \tau(\mathbb{T}')^p + x, \tau(\mathbb{T}')^a + x \rangle$ which is exactly what I needed.

– The only other possibility (as X^n is unsigned) is $X_2^n(x) = 0$. In this case, also $X^n(x) = Z^n(x) = 0$. I will in this case prove the following:

$$\begin{aligned} \tau(\mathbb{T})^n &\supseteq \tau(\mathbb{T}')^n - x \\ \tau(\mathbb{T})^p &= x + \tau(\mathbb{T}')^p \\ \tau(\mathbb{T})^a &= x + \tau(\mathbb{T}')^a \end{aligned}$$

I will use lemma 2.7.1, clauses 2 with $d = 1$ and 3 with $e = -1$. Following are the two clauses where d and e are instantiated:

(a) If it is the case that $X^n = Z^n$ and $X^a = Z^a + x$, then $\tau(\mathbb{T})^n \supseteq \tau(\mathbb{T}')^n - x$ and $\tau(\mathbb{T})^a = \tau(\mathbb{T}')^a + x$.

(b) If it is the case that $X^p = Z^p + x$ and $X^a = Z^a + x$ then also $\tau(\mathbb{T})^p = \tau(\mathbb{T}')^p + x$ and $\tau(\mathbb{T})^a = \tau(\mathbb{T}')^a + x$.

It should be possible to see that all the premises are fulfilled by the argument in item 1 and that we are treating the special case where $X^n = Z^n$. The conclusions in the clauses above are all we need, so we are finished.

- Case osDel

$$\begin{array}{l} (\mathsf{osDel}) \quad x \in M \\ (M, \mathbb{R}[\mathsf{Lf}(\text{del } x \cdot E)]_\beta) \longrightarrow (M - x, \mathbb{R}[\mathsf{Lf}(E)]_\beta) \end{array}$$

1. First, we prove that $\Gamma \vdash E : \langle X^n - x, Z^p, X^a + x \rangle$ for some Z^p. We have $\Gamma \vdash \text{del } x \cdot E : \langle X^n, X^p, X^a \rangle$.

– $E \neq \epsilon$. I have by the generation lemma (2.4.4) for SEQ that $\Gamma \vdash \mathrm{del}\ x\cdot : X_1$ and $\Gamma \vdash E : Z$ for some X_1 and Z where

$$X = \langle X_1^n \cup (Z^n - X_1^a), X_1^p \cup (X_1^a + Z^p), X_1^a + Z^a \rangle$$

By the generation lemma for DEL applied to $\Gamma \vdash \mathrm{del}\ x\cdot : X_1$ we have $X_1 = \langle [x], [], [-x] \rangle$. So we get

$$X = \langle Z^n + [x], [] \cup (Z^p - [x]), Z^a - [x] \rangle$$

This means that $\Gamma \vdash E : \langle X^n - x, Z^p, X^a + x \rangle$ so:

$$X^p = \begin{cases} Z^p \text{ if } Z^p(x) = 0 \\ Z^p - x \text{ if } Z^p(x) > 0 \end{cases} \tag{2.13}$$

– $E = \epsilon$. I get $\mathsf{del}\, x \cdot E = \mathsf{del}\, x\cdot$. By the generation lemma for ϵ, we have that $\Gamma \vdash E : X_2$, where $X_2 = \langle [], [], [] \rangle = Z$. By the generation lemma for DEL applied to $\Gamma \vdash \mathrm{del}\ x\cdot : X$ we have

$$X = \langle [x], [], [-x] \rangle$$

This means that $Z^p = X^p$, and since $Z^p(x) = 0$, this fits with the case distinction (2.13) above.

2. To summarise, the changes made to the configuration are that $M' = M - x$ and that the expression in β changes from $\mathsf{del} x \cdot E$ to E.
Note the following equalities

$$\begin{array}{c} M + \tau(\mathbb{T})^p \supseteq M' + \tau(\mathbb{T}')^p \\ \Updownarrow \\ \tau(\mathbb{T})^p \supseteq \tau(\mathbb{T}')^p - x \end{array}$$

and

$$\begin{array}{c} M - \tau(\mathbb{T})^n = M' - \tau(\mathbb{T}')^n \\ \Updownarrow \\ -\tau(\mathbb{T})^n = -x - \tau(\mathbb{T}')^n \\ \Updownarrow \\ \tau(\mathbb{T})^n = x + \tau(\mathbb{T}')^n \end{array}$$

I will now have to do a case distinction on the value of $Z^p(x)$, as the relation between Z^p and X^p depends on whether $Z^p(x) = 0$. This is similar to the procedure used in the previous case for osNew.

– The first case is when $Z^p(x) > 0$, then we have $X^p = Z^p - x$. Now, if I could prove that

$$\tau(\mathbb{T}) = \langle \tau(\mathbb{T}')^n + x, \tau(\mathbb{T}')^p - x, \tau(\mathbb{T}')^a - x \rangle \tag{2.14}$$

I would be finished, as then I would have

$$\begin{array}{l} M - \tau(\mathbb{T})^n = M' + x - \tau(\mathbb{T}')^n - x = M' - \tau(\mathbb{T}')^n \\ M + \tau(\mathbb{T})^p = M' + x + \tau(\mathbb{T}')^p - x = M' + \tau(\mathbb{T}')^p \\ M + \tau(\mathbb{T})^a = M' + x + \tau(\mathbb{T}')^a - x = M' + \tau(\mathbb{T}')^a \end{array}$$

which is even stronger than needed for the lemma.
I will proceed as in the case for osNew and use Lemma 2.7.1 clauses 1 with $c = 1$ and 3 with $e = 1$ to prove this. Instantiating the variables in the lemma, I get the following:

(a) If it is the case that $X^n = Z^n + x$ and $X^a = Z^a - x$ then also $\tau(\mathbb{T})^n = \tau(\mathbb{T}')^n + x$ and $\tau(\mathbb{T})^a = \tau(\mathbb{T}')^a - x$.

(b) If it is the case that $X^p = Z^p - x$ and $X^a = Z^a - x$ then also $\tau(\mathbb{T})^p = \tau(\mathbb{T}')^p - x$ and $\tau(\mathbb{T})^a = \tau(\mathbb{T}')^a - x$.

Observe from point 1 that $X = \langle Z^n + [x], Z^p - [x], Z^a - [x]\rangle$. That $\mathbb{T}$ and $\mathbb{T}'$ are well-typed and have no other changes follows from 1 and the property of osDel. I then get $\tau(\mathbb{T}) = \langle \tau(\mathbb{T}')^n + x, \tau(\mathbb{T}')^p - x, \tau(\mathbb{T}')^a - x\rangle$, which is what I need.

– The only other possibility (as Z^p is unsigned) is $Z^p(x) = 0$. In this case, also $X^p(x) = Z^p(x) = 0$. I will in this case prove the following:

$$\begin{aligned}\tau(\mathbb{T})^n &= \tau(\mathbb{T}')^n + x\\ \tau(\mathbb{T})^p &\supseteq \tau(\mathbb{T}')^p - x\\ \tau(\mathbb{T})^a &= \tau(\mathbb{T}')^a - x\end{aligned}$$

I will use lemma 2.7.1, clauses 1 with $c = 1$ and 4 with $f = 1$. Following are the two clauses where d and e are instantiated:

(a) If for some integer c it is the case that $X^n = Z^n + x$ and $X^a = Z^a - x$ then also $\tau(\mathbb{T})^n = \tau(\mathbb{T}')^n + x$ and $\tau(\mathbb{T})^a = \tau(\mathbb{T}')^a - x$.

(b) If if the case that $X^p = Z^p$ and $X^a = Z^a - x$, then $\tau(\mathbb{T})^p \supseteq \tau(\mathbb{T}')^p - x$ and $\tau(\mathbb{T})^a = \tau(\mathbb{T}')^a - x$.

It should be easy to see that all the premises are fulfilled by the argument in item 1 and that we are treating the special case where $X^p = Z^p$. The conclusions in the clauses above are all we need, so we are finished.

- Case osParIntr

(osParIntr)
$(M, \mathbb{R}[\mathsf{Lf}((A \,||\, B) \cdot E)]_\beta) \longrightarrow (M, \mathbb{R}[\mathsf{Nd}(E, \mathsf{Lf}(A), \mathsf{Lf}(B))]_\beta)$

1. First, we prove that $\Gamma \vdash A : Y_1$ and $\Gamma \vdash B : Y_2$ and $\Gamma \vdash E : Z$ for some Y_1, Y_2 and Z. We have that $\mathbb{T}(\beta) = (A \,||\, B) \cdot E$ and $\mathbb{T}'(\beta) = E$ We have $\Gamma \vdash (A \,||\, B) \cdot E : \langle X^n, X^p, X^a\rangle$.

   – $E \neq \epsilon$. By the generation lemma for Seq, we get $\Gamma \vdash (A \,||\, B)\cdot : X_1$ and $\Gamma \vdash E : Z$ with

   $$X = \langle X_1^n \cup (Z^n - X_1^a), X_1^p \cup (X_1^a + Z^p), X_1^a + Z^a\rangle$$

   By the generation lemma for Parallel applied to $\Gamma \vdash (A \,||\, B)\cdot : X_1$ we have $\Gamma \vdash A : Y_1$ and $\Gamma \vdash B : Y_2$ such that $X_1 = Y_1 + Y_2$.

   – $E = \epsilon$. Then we have $(A \,||\, B)\cdot E = (A \,||\, B)\cdot$ and by the generation lemma for Parallel applied to $\Gamma \vdash (A \,||\, B)\cdot : X$ we have $\Gamma \vdash A : Y_1$ and $\Gamma \vdash B : Y_2$ such that $X = Y_1 + Y_2$. Further by the generation lemma for ϵ we get $Z = \langle [], [], []\rangle$.

2. We have $M = M'$. In addition $\mathsf{expr}(\mathbb{T}) = \mathsf{expr}(\mathbb{T}')$ could be proved by structural induction on the size of the tree by seeing that

$$\mathsf{expr}(\mathsf{Lf}((A||B) \cdot E)) = (A||B) \cdot E = \mathsf{expr}(\mathsf{Nd}(E, \mathsf{Lf}(A), \mathsf{Lf}(B))$$

Since we know from 1 above that $\tau(\mathbb{T})$ and $\tau(\mathbb{T}')$ exist we also know they must be the same, as an expression has only one type from Uniqueness of type.

- Case osParElimL

(osParElimL)
$$(M, \mathbb{R}[\mathsf{Nd}(E, \mathsf{Lf}(\epsilon), \mathbb{R}')]_\beta) \longrightarrow (M, \mathbb{R}[\mathsf{Nd}(E, \mathbb{R}')]_\beta)$$

1. Since $E = \mathbb{T}(\beta) = \mathbb{T}'(\beta)$ and $M = M'$ it follows from $(M, \mathbb{T})$ well-formed that $\Gamma \vdash E : \langle X^n, X^p, X^a \rangle$.
2. $M = M'$ and as in the previous case (osParIntr) we can prove

$$\mathsf{expr}(\mathbb{T}) = \mathsf{expr}(\mathbb{T}')$$

by structural induction and seeing that:

$$\mathsf{expr}(\mathsf{Nd}(E, \mathsf{Lf}(\epsilon), \mathbb{R}')) = (\epsilon||\mathsf{expr}(\mathbb{R}')) \cdot E = \mathsf{expr}(\mathsf{Nd}(E, \mathbb{R}'))$$

Then the properties follow from same arguments as in the case osParIntr.

- Case osParElimR

(osParElimR)
$$(M, \mathbb{R}[\mathsf{Nd}(E, \mathbb{R}', \mathsf{Lf}(\epsilon))]_\beta) \longrightarrow (M, \mathbb{R}[\mathsf{Nd}(E, \mathbb{R}')]_\beta)$$

This proof goes like (osParElimL), just substituting the positions in the transition.

- Case osParElim

(osParElim)
$$(M, \mathbb{R}[\mathsf{Nd}(E, \mathsf{Lf}(\epsilon))]_\beta) \longrightarrow (M, \mathbb{R}[\mathsf{Lf}(E)]_\beta)$$

1. Since $E = \mathbb{T}(\beta) = \mathbb{T}'(\beta)$ and $M = M'$ it follows from $(M, \mathbb{T})$ well-formed that $\Gamma \vdash E : \langle X^n, X^p, X^a \rangle$.
2. $M = M'$. We have $\mathsf{expr}(\mathsf{Nd}(E, \mathsf{Lf}(\epsilon))) = (\epsilon||\epsilon) \cdot E$ and $\mathsf{expr}(\mathsf{Lf}(E)) = E$. We have from assumptions that $\Gamma \vdash E : X$. From Axiom, Parallel and WeakenB I get $\Gamma \vdash (\epsilon||\epsilon) \cdot : \langle [], [], [] \rangle$ and from Seq $\Gamma \vdash (\epsilon||\epsilon) \cdot E : \langle [] \cup (X^n - []), [] \cup (X^p + []), [] + X^a \rangle = X$. It should the be possible to see that $\tau(\mathbb{T}) = \tau(\mathbb{T}')$, using $c = 0$ with lemma (2.7.1).

□

2.7.3 Preservation (Lemma 2.4.16)

The lemma is: *if* $\Gamma \models (M, \mathbb{T})$ *and* $(M, \mathbb{T}) \longrightarrow (M', \mathbb{T}')$ *then* $\Gamma \models (M', \mathbb{T}')$.

Proof. If $\Gamma \models (M, \mathbb{T})$ and $(M, \mathbb{T}) \longrightarrow (M', \mathbb{T}')$, I must show that $\Gamma \models (M', \mathbb{T}')$. By definition of well-formed configuration we need to prove that $\forall \alpha \in \mathbb{T}'$, where $E = \mathbb{T}'(\alpha)$ there exists an $X = \langle X^n, X^p, X^a \rangle$ such that $\Gamma \vdash E : \langle X^n, X^p, X^a \rangle$ and that $M' \supseteq \tau(\mathbb{T}')^n$ and $M' + \tau(\mathbb{T}')^p \subseteq \mathcal{R}$. In clause 1 of the proof of invariance, we treated the existence of the types. By clause 2, $M - \tau(\mathbb{T})^n \subseteq M' - \tau(\mathbb{T}')^n$. Since $M \supseteq \tau(\mathbb{T})^n$ we must then also have $M' \supseteq \tau(\mathbb{T}')^n$. By clause 2, $M + \tau(\mathbb{T})^p \supseteq M' + \tau(\mathbb{T}')^p$. Since $M + \tau(\mathbb{T})^n \subseteq \mathcal{R}$ we must then also have $M' + \tau(\mathbb{T}')^p \subseteq R$, which is all we need. $\square$

2.7.4 Progress (Lemma 2.4.17)

The lemma is: *if* $\Gamma \models (M, \mathbb{T})$ *then either* $(M, \mathbb{T})$ *is terminal or there exists a configuration* $(M', \mathbb{T}')$ *such that* $(M, \mathbb{T}) \longrightarrow (M', \mathbb{T}')$.

Proof. Since $\Gamma \models (M, \mathbb{T})$ I know from the definition of well-typed tree (2.4.11) that for any position α in $\mathbb{T}$ where $E = \mathbb{T}(\alpha)$ there exists $X = \langle X^n, X^p, X^a \rangle$ such that $\Gamma \vdash E : X$. Now I have to show that the execution cannot be stuck, i.e. it must be possible to apply a rule from the operational semantics. There are three ways execution can get stuck.

1. The execution is stuck if E has the form $\mathsf{new}\, x \cdot E'$ and $x \notin \mathsf{dom}(\Gamma)$. This will not happen by valid typing judgment (2.4.2).

2. The execution is stuck if E has the form $\mathsf{del}\, x \cdot E'$ and $x \notin M$. If $E' \neq \epsilon$, I get from the generaton lemma (2.4.4) for sequencing the existence of Y and Z such that $\Gamma \vdash \mathsf{del}\, x \cdot : Y$ and $\Gamma \vdash E' : Z$ and $X = \langle Y^n \cup (Z^n - Y^a), Y^p \cup (Z^p + Y^a), Y^a + Z^a \rangle$. Further, from the generation lemma (2.4.4) for del I get $Y = \langle [x], [], [-x] \rangle$, such that $X^n = [x] \cup (Z^n + [x]) \supseteq [x]$. If $E' = \epsilon$, I get directly from the generation lemma for del that $X^n = [x]$. In both cases we have $X^n \supseteq [x]$.

   Now I need to "expand" this to get that $\tau(\mathbb{T})^n \supseteq [x]$. I will do this by induction on the structure of $\mathbb{T}$. The inductive hypothsis is: *for any smaller tree where there is an expression in a leaf which has a type* X *s.t.* $X^n \supseteq [x]$*, then also* $\tau(\mathbb{T}) \supseteq [x]$.

   - The base case is the single leaf, in which case the result follows from $\tau(\mathbb{T}) = X$.
   - The first inductive case is a node with two subtrees, one of which contains the leaf with the expression concerned. Let the tree be $\mathbb{T} = \mathsf{Nd}(E_\bullet, \mathbb{T}_l, \mathbb{T}_r)$ for some expression $E_\bullet$ and smaller trees $\mathbb{T}_l$ and $\mathbb{T}_r$. Assume $\Gamma \vdash E_\bullet : X_\bullet$. Also assume, without loss of generality, that the expression is in the left subtree, such that from the inductive hypothesis $\tau(\mathbb{T}_l)^n \supseteq [x]$. I will now use the same arguments as on page 35 in the proof of lemma 2.7.1. First I have that $\mathsf{expr}(\mathbb{T}) = (\mathsf{expr}(\mathbb{T}_l) || \mathsf{expr}(\mathbb{T}_r)) \cdot E_\bullet$. By using an application of $\mathsf{Parallel}$ and Seq I get from this that $\tau(\mathbb{T})^n = (\tau(\mathbb{T}_l)^n + \tau(\mathbb{T}_r)^n) \cup (X_\bullet^n - (\tau(\mathbb{T}_l)^a + \tau(\mathbb{T}_r)^a))$. Then I get from the properties of union and addition of hybrid sets that:

$$\begin{array}{lcl} \tau(\mathbb{T})^n & = & (\tau(\mathbb{T}_l)^n + \tau(\mathbb{T}_r)^n) \cup (X^n_\bullet - \tau(\mathbb{T}_l)^a - \tau(\mathbb{T}_r)^a) \\ & \supseteq & \tau(\mathbb{T}_l)^n + \tau(\mathbb{T}_r)^n \\ & \supseteq & \tau(\mathbb{T}_l)^n \\ & \supseteq & [x] \end{array} \tag{2.15}$$

- The other inductive case is the node with one child. This is just a special case of the situation with two leaves.

Further from $(M, \mathbb{T})$ well-formed I get that $M \supseteq \tau(\mathbb{T})^n$. In sum I get $M \supseteq \tau(\mathbb{T})^n \supseteq [x]$ and so there is at least one instance of x in the store, and the execution cannot be stuck.

3. E has the form $\mathsf{new}\, x \cdot A$, but $M(x) \geq \mathcal{R}(x)$. Again I must do a case distinction on whether $A = \epsilon$. If $A \neq \epsilon$, the generation lemma (2.4.4) for sequencing gives me Y and Z such that $\Gamma \vdash \mathsf{new}\, x \cdot : Y$ and $\Gamma \vdash E : Z$ and $X = \langle Y^n \cup (Z^n - Y^a), Y^p \cup (Z^p + Y^a), Y^a + Z^a \rangle$. If $A = \epsilon$, let $X = Y$. In both cases, we have $X^p \supseteq Y^p$. The generation lemma for new now gives me Δ, Δ', A and V such that $\Delta, x \prec B, \Delta' = \Gamma$ and $\Delta \vdash B : V$ and $Y = \langle V^n, V^p + x, V^a + x \rangle$. This means that $Y^p \supseteq [x]$, and therefore $X^p \supseteq [x]$.

   I need now to get that $\tau(\mathbb{T})^p \supseteq [x]$. It should be possible to see that we can use almost the same proof by induction on the structure of the tree $\mathbb{T}$ as in the previous item, only replacing ^{n} with ^{p}. The only other difference is that $\tau(\mathbb{T}_l)^a + \tau(\mathbb{T}_r)^a$ is added rather that subtracted in the first line of (2.15). But this does not concern us, as the only information we need is a minimum guarantee, which we get from the other part of the union.

   Further from well-formed configuration we have $M + \tau(\mathbb{T})^p \subseteq R$. In all we can conclude that $M + x \subseteq M + \tau(\mathbb{T})^p \subseteq R$, so we must have $M(x) < R(x)$.

□

2.7.5 Soundness (Lemma 2.4.19)

The lemma is: *let Prog = Decls;E be such that* $\Gamma \models_{\mathcal{R}} ([], E)$ *for some reordering* Γ *of Decls and restriction* $\mathcal{R}$*. Then for any* $(M, \mathbb{T})$ *such that* $([], \mathsf{Lf}(E)) \longrightarrow^* (M, \mathbb{T})$ *we have that* $(M, \mathbb{T})$ *is not stuck and* $M \subseteq X^p$*.*

Proof $([], \mathsf{Lf}(E))$ is well-formed from the definition (2.4.13). From preservation (2.4.16) and progress (2.4.17) we know that $(M, \mathbb{T})$ is not stuck. For the second conclusion, $M \subseteq X^p$, we have from invariance of $M + \tau(\mathbb{T})^p$ (Lemma 2.4.15), transitivity of $\subseteq$ and from valid typing lemma (2.4.2) which guarantees $X^p \supseteq []$ that:

$$M \subseteq M + \tau(\mathbb{T})^p \subseteq [] + X^p = X^p$$

□

2.8 Proof of sharpness (Lemma 2.4.20)

2.8.1 Auxiliary definitions and propositions.

First I must show that the change in the store through a sequence of configurations is independent of the size of the store — given of course that it starts from a well-formed configuration. As an overview, we can say that the only transition that depends on the store is DEL, which will fail if the component is not present — but we are guaranteed from soundness that this will not happen starting from a well-formed configuration. I will prove this by showing that two sequences of configurations using the exact same transitions will produce the same change in the store, independent of the size of the store in the initial configuration.

Lemma 2.8.1 (Effect of transitions invariance). *Consider two sequences of configurations of the same length j*

$$(M_0, \mathbb{T}_0) \longrightarrow \cdots \longrightarrow (M_j, \mathbb{T}_j) \tag{2.16}$$

and

$$(M'_0, \mathbb{T}'_0) \longrightarrow \cdots \longrightarrow (M'_j, \mathbb{T}'_j) \tag{2.17}$$

If for all i, where $0 \leq i < j$, the rule used from the operational semantics to transform $(M_i, \mathbb{T}_i) \longrightarrow (M_{i+1}, \mathbb{T}_{i+1})$ is the same and the subexpression to which the rule is applied is identical to the one used for the transformation $(M'_i, \mathbb{T}'_i) \longrightarrow (M'_{i+1}, \mathbb{T}'_{i+1})$, then we have that

$$M_j - M_0 = M'_j - M'_0$$

Note that I am comparing two already existing sequences. This means I do not have to show that they exist, since this is assumed. I will prove the lemma by induction on the length of the sequences of configurations. The inductive hypothesis is:

For any $k \leq j$: for any two sequences of configurations of length k:

$$(M_0, \mathbb{T}_0) \longrightarrow \cdots \longrightarrow (M_k, \mathbb{T}_k)$$

and

$$(M'_0, \mathbb{T}'_0) \longrightarrow \cdots \longrightarrow (M'_k, \mathbb{T}'_k)$$

If for all i, where $0 \leq i < k$, the rule used from the operational semantics to transform $(M_i, \mathbb{T}_i) \longrightarrow (M_{i+1}, \mathbb{T}_{i+1})$ is the same and the subexpression to which the rule is applied is identical to the one used for the transformation $(M'_i, \mathbb{T}'_i) \longrightarrow (M'_{i+1}, \mathbb{T}'_{i+1})$, then we have that $M_k - M_0 = M'_k - M'_0$.

- Base Case. The base case will be any run of length 0, in which case $M_0 = M_k$ and $M'_0 = M'_j$.
- Inductive cases. We have the lemma for sequences of configurations

  $$(M_0, \mathbb{T}_0) \longrightarrow \cdots \longrightarrow (M_k, \mathbb{T}_k)$$

  where $k \leq j$. Now I need to assure the lemma for all sequences which are one transition longer. This is done by adding the same transition at

the right hand end of two equal sequences of length j. Since all sequences shorter than $j+1$ are covered by the inductive hypothesis, we only need to create the sequences of exactly length $j+1$:

$$(M_0, \mathbb{T}_0) \longrightarrow \cdots \longrightarrow (M_j, \mathbb{T}_j) \longrightarrow (M_{j+1}, \mathbb{T}_{j+1})$$

To accomplish this, I will use a case distinction on the possible transitions from the operational semantics.

- osNew

  $$\begin{array}{l}(\mathsf{osNew}) \quad \text{if } x \prec A \in Decls \\ (M_j, \mathbb{T}[\mathsf{Lf}(\text{new } x \cdot E_r)]_\alpha) \longrightarrow (M_j + x, \mathbb{T}[\mathsf{Lf}(AE_r)]_\alpha)\end{array}$$

  We have $M_{j+1} - M_0 = M_j + x - M_0$. From the assumptions the same transition is done on $(M'_j, \mathbb{T}'_j)$ and we get $M'_{j+1} - M'_0 = M'_j + x - M'_0$. Combining this with the inductive hypothesis I now get:

  $$M_{j+1} - M_0 = M_j + x - M_0 = M'_j + x - M'_0 = M'_{j+1} - M'_0$$

  which is exactly what I needed.

- osDel

  $$\begin{array}{l}(\mathsf{osDel}) \quad x \in M \\ (M, \mathbb{T}[\mathbb{T}'_j[\mathsf{Lf}(\text{del } x \cdot E)]'_\alpha]_\alpha) \longrightarrow (M - x, \mathbb{T}[\mathbb{T}'_j[\mathsf{Lf}(E)]'_\alpha]_\alpha)\end{array}$$

  I have $M_{j+1} - M_0 = M_j - x - M_0$. From the assumptions, the same transition is added in the other sequence, and I get $M'_{j+1} - M'_0 = M'_j - x - M'_0$. Combining this with the inductive hypothesis I then get

  $$M_{j+1} - M_0 = M_j - x - M_0 = M'_j - x - M'_0 = M'_{j+1} - M'_0$$

- osPar* None of these transitions change the store, so $M_{j+1} = M_j$ and $M'_{j+1} = M'_j$. Assuming I have $M_j - M_0 = M'_j - M'_0$, I then get $M_{j+1} - M_0 = M'_{j+1} - M'_0$.

□

2.8.2 Example

Generally, the runs attaining the maxima will be different for different components, and different for the two first types of maximum.

As an example, take a look at the possible runs of this expression (where $\mathsf{new}x^3$ means three repetitions of $\mathsf{new}x$) :

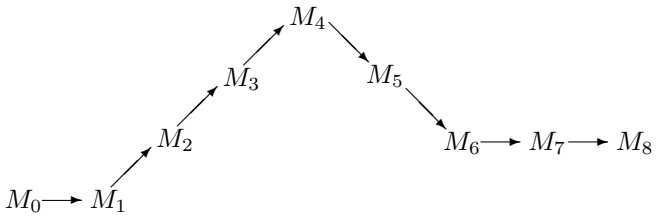
$$x \prec \epsilon; (\mathsf{new}\, x^3 || \mathsf{del}\, x^2) \tag{2.18}$$

The type of the expression is $\langle [x,x], [x,x,x], [x] \rangle$. To achieve the different maxima, we must use two different runs. First we will consider the run which gives the maximum number of x when $k = 4$, with

$$([], \mathsf{Lf}((\mathsf{new}\, x^3 || \mathsf{del}\, x^2))) \to^4 ([x,x,x], \mathsf{Nd}(\epsilon, \mathsf{Lf}(\epsilon), \mathsf{Lf}(\mathsf{del}\, x^2)))$$

$$
\begin{array}{ll}
(M, \mathsf{Lf}(\mathsf{new} x^3 || \mathsf{del} x^2)) & = (M_0, \mathbb{T}_0) \\
\to (M, \mathsf{Nd}(\epsilon, \mathsf{Lf}(\mathsf{new} x^3), \mathsf{Lf}(\mathsf{del}\, x^2))) & = (M_1, \mathbb{T}_1) \\
\to (M + [x], \mathsf{Nd}(\epsilon, \mathsf{Lf}(\mathsf{new} x^2), \mathsf{Lf}(\mathsf{del}\, x^2))) & = (M_2, \mathbb{T}_2) \\
\to (M + [x \mapsto 2], \mathsf{Nd}(\epsilon, \mathsf{Lf}(\mathsf{new} x), \mathsf{Lf}(\mathsf{del}\, x^2))) & = (M_3, \mathbb{T}_3) \\
\to (M + [x \mapsto 3], \mathsf{Nd}(\epsilon, \mathsf{Lf}(\epsilon), \mathsf{Lf}(\mathsf{del}\, x^2))) & = (M_4, \mathbb{T}_4) \\
\to (M + [x \mapsto 2], \mathsf{Nd}(\epsilon, \mathsf{Lf}(\epsilon), \mathsf{Lf}(\mathsf{del}\, x))) & = (M_5, \mathbb{T}_5) \\
\to (M + [x], \mathsf{Nd}(\epsilon, \mathsf{Lf}(\epsilon), \mathsf{Lf}(\epsilon))) & = (M_6, \mathbb{T}_6) \\
\to (M + [x], \mathsf{Nd}(\epsilon, \mathsf{Lf}(\epsilon))) & = (M_7, \mathbb{T}_7) \\
\to (M + [x], \mathsf{Lf}(\epsilon)) & = (M_8, \mathbb{T}_8)
\end{array}
$$

This run does not reach the minimum possible number of x during the run. The number of x during the run can also be visualised, letting the vertical axis represent number of x :

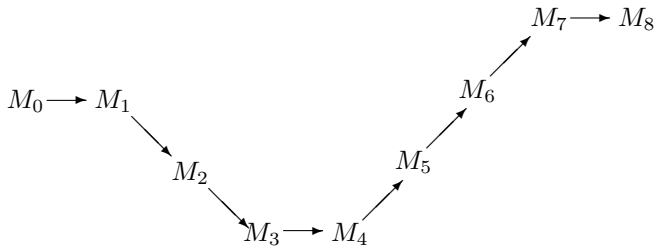


Then I will consider the run which gives the minimum number of x when $k = 3$, with

$$(M, \mathsf{Lf}((\mathsf{new}\, x^3 || \mathsf{del}\, x^2))) \to^3 (M - [x \mapsto 2], \mathsf{Nd}(\epsilon, \mathsf{Lf}(\epsilon), \mathsf{Lf}(\mathsf{new}\, x^3)))$$

$$
\begin{array}{ll}
(M, \mathsf{Lf}(\mathsf{new} x^3 || \mathsf{del} x^2)) & = (M_0, \mathbb{T}_0) \\
\to (M, \mathsf{Nd}(\epsilon, \mathsf{Lf}(\mathsf{new} x^3), \mathsf{Lf}(\mathsf{del}\, x^2))) & = (M_1, \mathbb{T}_1) \\
\to (M - [x], \mathsf{Nd}(\epsilon, \mathsf{Lf}(\mathsf{new} x^3), \mathsf{Lf}(\mathsf{del}\, x))) & = (M_2, \mathbb{T}_2) \\
\to (M - [x \mapsto 2], \mathsf{Nd}(\epsilon, \mathsf{Lf}(\mathsf{new} x^3), \mathsf{Lf}(\epsilon))) & = (M_3, \mathbb{T}_3) \\
\to (M - [x \mapsto 2], \mathsf{Nd}(\epsilon, \mathsf{Lf}(\mathsf{new} x^3))) & = (M_4, \mathbb{T}_4) \\
\to (M - [x], \mathsf{Nd}(\epsilon, \mathsf{Lf}(\mathsf{new} x^2))) & = (M_5, \mathbb{T}_5) \\
\to (M, \mathsf{Nd}(\epsilon, \mathsf{Lf}(\mathsf{new}\, x))) & = (M_6, \mathbb{T}_6) \\
\to (M + [x], \mathsf{Nd}(\epsilon, \mathsf{Lf}(\epsilon))) & = (M_7, \mathbb{T}_7) \\
\to (M + [x], \mathsf{Lf}(\epsilon)) & = (M_8, \mathbb{T}_8)
\end{array}
$$

This run does not reach the maximum possible number of x during the run. The number of x during the run can also be visualised, letting vertical axis represent number of x :



This example shows that it can be (and often is) the case that different runs, often also of different length, must be used to achieve the value for X^n and X^p for the same component.

2.8.3 Proof of sharpness.

The lemma is: *if* $\Gamma \vdash E : X$ *then, for every component* x*, for every restriction* $\mathcal{R}$ *and every well-formed configuration* $(M, \mathbb{T}[\mathsf{Lf}(E)]_\alpha) = (M_0, \mathbb{T}_0)$ *with respect to the given* $\mathcal{R}$*, there exists a run*

$$(M_0, \mathbb{T}_0) \to \cdots \to (M_n, \mathbb{T}_n) = (M_n, \mathbb{T}[\mathsf{Lf}(\epsilon)]_\alpha)$$

of E *where there is a* k*,* $0 \leq k \leq n$*, such that* $M_k(x) = M_0(x) + X^p(x)$*, and there exists a run*

$$(M_0, \mathbb{T}_0) \to \cdots \to (M_m, \mathbb{T}_m) = (M_m, \mathbb{T}[\mathsf{Lf}(\epsilon)]_\alpha)$$

of E *where there is a* j*,* $0 \leq j \leq m$*, such that* $M_j(x) = M_0(x) - X^n(x)$*, and for all runs*

$$(M_0, \mathbb{T}_0) \to \cdots \to (M_q, \mathbb{T}_q) = (M_q, \mathbb{T}[\mathsf{Lf}(\epsilon)]_\alpha)$$

of E *we have* $M_q(x) = M_0(x) + X^a(x)$*.*

The lemma will be proved in two parts, first X^a separately, and then X^n and X^p together.

X^a: First, I will show sharpness for X^a — that is: for any configuration $(M, \mathbb{T}[\mathsf{Lf}(E)]_\alpha) = (M_0, \mathbb{T}^0)$ which is well-formed with respect to some restriction $\mathcal{R}$ and some base Γ, we have that for all runs $(M_0, \mathbb{T}^0) \to \cdots \to (M_j, \mathbb{T}^j) = (M_j, \mathbb{T}[\mathsf{Lf}(\epsilon)]_\alpha)$ of E we have $M_j = X^a + M_0$.

In order to prove this, by invariance lemma (2.4.15) and transitivity of equality we have that $M_0 + \tau(\mathbb{T}^0)^a = M_n + \tau(\mathbb{T}^j)^a$. I rewrite to get

$$M_n = M_0 + \tau(\mathbb{T}^0)^a - \tau(\mathbb{T}^j)^a \tag{2.19}$$

I have from assumptions that $(M_0, \mathbb{T}^0)$ well-formed with respect to Γ and know therefore that $\Gamma \vdash E : Z$ for some Z. From typability lemma (2.4.12) I know that

$$\tau(\mathbb{T}^0)^a = \sum_{\beta \in \mathbb{T}^0} \tau(\mathbb{T}^0(\beta))^a \tag{2.20}$$

$$\tau(\mathbb{T}^j)^a = \sum_{\beta \in \mathbb{T}^j} \tau(\mathbb{T}^j(\beta))^a \tag{2.21}$$

Note that from the generation lemma for ϵ I have that $\tau(\mathbb{T}^j(\alpha))^a = []$. I can now decompose these sums into a sum using separate sums on $\mathbb{T}[]$ and the expression at the single leaf:

$$\begin{aligned}\textstyle\sum_{\beta\in\mathbb{T}^0}\tau(\mathbb{T}^0(\beta))^a &= \textstyle\sum_{\beta\in\mathbb{T}[]_\alpha}\tau(\mathbb{T}[]_\alpha(\beta))^a + \tau(\mathbb{T}^0(\alpha))^a\\ &= \textstyle\sum_{\beta\in\mathbb{T}[]_\alpha}\tau(\mathbb{T}[]_\alpha(\beta))^a + Z^a\\ \textstyle\sum_{\beta\in\mathbb{T}^j}\tau(\mathbb{T}^j(\beta))^a &= \textstyle\sum_{\beta\in\mathbb{T}[]_\alpha}\tau(\mathbb{T}[]_\alpha(\beta))^a + \tau(\mathbb{T}^j(\alpha))^a\\ &= \textstyle\sum_{\beta\in\mathbb{T}[]_\alpha}\tau(\mathbb{T}[]_\alpha(\beta))^a\end{aligned}$$

I now see that $\tau(\mathbb{T}^0)^a - \tau(\mathbb{T}^j)^a = Z^a$. Combined with equation (2.19) above, I get

$$\begin{aligned}M_n &= M_0 + \tau(\mathbb{T}^0)^a - \tau(\mathbb{T}^j)^a\\ &= M_0 + Z^a\\ &= M_0 + Z^a\end{aligned}$$

which shows sharpness of X^a as wanted.

X^n and X^p. The two other properties, X^n and X^p of the sharpness lemma (2.4.20) will be shown by induction on typing derivations. The inductive hypothesis must be strengthened a bit from the lemma: I must include runs of E ending in not only a leaf containing ϵ, but also with any expression E'. This is to make the case SEQ easier.

Let $\Gamma \models_{\mathcal{R}} (M, \mathbb{T})$ for some basis Γ, configuration $(M, \mathbb{T})$ and restriction $\mathcal{R}$. The inductive hypothesis is: *for all shorter typing derivations $\Gamma' \vdash E : X$, where Γ' is a sub-basis of Γ, it is the case that for every component x and every configuration $(M, \mathbb{T}[\mathsf{Lf}(EE')]_\alpha) = (M_0, \mathbb{T}_0)$ such that $\Gamma \models_{\mathcal{R}} (M_0, \mathbb{T}_0)$, there exists a run $(M_0, \mathbb{T}_0) \to \cdots \to (M_n, \mathbb{T}_n) = (M_n, \mathbb{T}[\mathsf{Lf}(E')]_\alpha)$ of E where there is a k, $0 \le k \le n$ such that $M_k(x) = X^p(x) + M_0(x)$, and there exists a run $(M_0, \mathbb{T}_0) \to \cdots \to (M_m, \mathbb{T}_m) = (M_m, \mathbb{T}[\mathsf{Lf}(E')]_\alpha)$ of E where there is a j, $0 \le j \le m$ such that $M_j(x) = M_0(x) - X^n(x)$.*

Base case

Axiom

$$\frac{}{\oslash \vdash \epsilon : \langle [], [], [] \rangle}$$

We have only one "run" of length 0:

$$(M_0, \mathbb{T}_0) = (M, \mathbb{T}[\mathsf{Lf}(E)]_\alpha) = (M, \mathbb{T}[\mathsf{Lf}(\epsilon)]_\alpha)$$

I choose the "run" of length 0, where no components are created nor deleted. Let $k = 0$. Since $X^n(x) = X^p(x) = 0$ this is enough.

Inductive cases

WeakenB $\Gamma = \Gamma', x \prec B$

$$\frac{\Gamma' \vdash E : X \quad \Gamma' \vdash B : Y \quad x \notin \mathsf{dom}(\Gamma')}{\Gamma', x \prec B \vdash E : X}$$

Since E and X are the same in the conclusion and the premise, this proof is easy — we know already by the inductive hypothesis on the premise $\Gamma' \vdash E : X$ that there exist runs of E with the properties needed for sharpness of X.

New $E = \mathsf{new}\, y\cdot$, $\Gamma = \Gamma', y \prec A$.

$$\frac{\Gamma' \vdash A : Y \quad y \notin \mathsf{dom}(\Gamma')}{\Gamma', y \prec A \vdash \mathsf{new}\, y\cdot : X = \langle Y^n, Y^p + y, Y^a + y\rangle}$$

From the inductive hypothesis we have existence of runs of A of the form

$$(M_0, \mathbb{T}[\mathsf{Lf}(AE')]_\alpha) \to \cdots \to (M_n, \mathbb{T}[\mathsf{Lf}(E')]_\alpha) \tag{2.22}$$

What we want is to add one transition in front of such a run to get a run of $\mathsf{new}\, y\cdot$:

$$(N_0, \mathbb{T}[\mathsf{Lf}(\mathsf{new}\, y \cdot E')]_\alpha) \to (N_1, \mathbb{T}[\mathsf{Lf}(AE')]_\alpha) \to \cdots \to (N_{n+1}, \mathbb{T}[\mathsf{Lf}(E')]_\alpha) \tag{2.23}$$

$$N_1 = N_0 + y \tag{2.24}$$

$$N_{n+1} = N_1 + M_n - M_0 = N_0 + y + M_n - M_0 \tag{2.25}$$

This is a run of $\mathsf{new}\, y\cdot$. The last equation (2.25) follows from (2.8.1) since all but the first transition are equal to the transitions in a run of A (2.22). The first step is the rule OSNEW from the operational semantics, and is possible by progress (2.4.17) since we assume it is well-formed. The rest of the run exists by the inductive hypothesis, the only difference is the addition of one y. All steps, including the first, will be possible to carry out because of progress and preservation. We can also see directly from the generation lemma for new that we have $\Delta \vdash A : Y$ where $X = \langle Y^n, Y^p + y, Y^a + y\rangle$.

- For $y \neq x$ we can use the runs of A which exist by the inductive hypothesis for the properties of Y and that $Y^*(x) = X^*(x)$.
- For $y = x$ we have by valid typing that $y \notin \mathsf{dom}(\Gamma')$ and by lemma 2.4.2 (Valid typing judgement) that $Y^* \subseteq \mathsf{dom}(\Gamma')$, so we must have $Y^*(y) = 0$ and there is no y created in the run of A. The extra y is added to the store in the first step of the run, and this will be the only y added during the run of $\mathsf{new}\, y\cdot$. I choose $k = 1$, and $N_1(y) = N_0(y) + 1$ while $X^p(y) = Y^p(y) + 1 = 1$. To get sharpness of $X^n(y) = 0$ I choose $j = 0$, and get $N_0(y) = N_0(y) - 0 = N_0(y) - X^n(y)$. So in this case all properties hold for any run of $\mathsf{new}\, y\cdot$.

Del $E = \mathsf{del}\, y\cdot$.

$$\frac{\Gamma \vdash A : Y \quad y \prec A \in \Gamma}{\Gamma \vdash \mathsf{del}\, y\cdot : \langle [y], [], [-y]\rangle}$$

Starting from a well-formed configuration $(N_0, \mathbb{T}[\mathsf{Lf}(\mathsf{del}\, y \cdot E')]_\alpha)$, there is only one run of $\mathsf{del}\, y\cdot$:

$$(N_0, \mathbb{T}_0) = (N_0, \mathbb{T}[\mathsf{Lf}(\mathsf{del}\, y \cdot E')]_\alpha) \longrightarrow (N_0 - y, \mathbb{T}[\mathsf{Lf}(E')]_\alpha)$$

This run is actually independent of the type and runs of A, so we do not need the inductive hypothesis in this case.

- For $y \neq x$: there is no change to $N_0(x)$ and for the type we have $X^*(x) = 0$.
- For $y = x$: for sharpness of $X^p(x)$ let $k = 0$, and observe that $N_0(x) = N_0(x) + 0 = N_0(x) + X^i(x)$. For $X^n(x) = 1$ choose $j = 1$ and get $N_1(x) = N_0(x) - 1 = N_0(x) - X^n(x)$.

Seq

$$\frac{\Gamma \vdash A\cdot : Y \qquad \Gamma \vdash B\cdot : Z}{\Gamma \vdash A \cdot B\cdot : X = \langle Y^n \cup (Z^n - Y^a), Y^p \cup (Y^a + Z^p), Y^a + Z^a \rangle}$$

From soundness (2.4.19) and the assumption of starting from a well-formed configuration, we know that all the transformations in the combined run are possible.

So for such a pair of a run of $A\cdot$ and a run of $B\cdot$, where the store in the last step of the run of $A\cdot$ is equal to the store in the first step of the run of $B\cdot$, there is a run of $A \cdot B\cdot$, using the same transitions. If the run of $A\cdot$ is of length j and the run of $B\cdot$ is of length k, the run of $A \cdot B\cdot$ will be of length $j + k$.

We can now go on to the three properties of sharpness:

- $X^p(x)$. Now I have to find a run of $A \cdot B\cdot$:

  $$(M_0, \mathbb{T}_0) \to \cdots \to (M_n, \mathbb{T}_n) \to \cdots \to (M_{n+m}, \mathbb{T}_{n+m})$$

  where there is k, such that $1 \leq k \leq n + m$ and

  $$\begin{array}{rcl} M_k(x) & = & M_0(x) + X^p(x) \\ & = & M_0(x) + (Y^n \cup (Z^p + Y^a))(x) \\ & = & M_0(x) + \max(Y^p(x), Z^p(x) + Y^a(x)) \end{array}$$

  Either the k with the maximum store is found during execution of $A\cdot$ (e.g.. $k \leq n$) or k is during the execution of $B\cdot$ (e.g. $k > n$).

  To prove that there will always be such a run and k, we must make a case distinction on the value of $X^p(x) = \max(Y^p(x), Y^a(x) + Z^p(x))$:

  - If $Y^p(x) = \max(Y^p(x), Y^a(x) + Z^p(x))$ we can use the run of $A\cdot$ which by the inductive hypothesis has a configuration $(M_{k_A}, \mathbb{T}_{k_A})$ such that $M_{k_A}(x) = M_0(x) + Y^p(x) = M_0(x) + X^p(x)$, so we can use k_A as k.
  - In the other case, $Y^a(x) + Z^p(x) = \max(Y^p(x), Y^a(x) + Z^p(x))$, we use any run of A and we have $(M_n, \mathbb{T}_n) = (M_n, \mathbb{T}[\mathtt{Lf}(BE')]_\alpha)$ where $M_n(x) = M_0(x) + Y^a(x)$. We can then choose the run of $B\cdot$ where there is a k_B such that

    $$M_{n+k_B}(x) = M_n(x) + Z^p(x) = M_0(x) + Y^a(x) + Z^p(x) = M_0(x) + X^p(x)$$

    and use $n + k_B$ as k.

- $X^n(x)$. Finding a run of $A \cdot B\cdot$:

  $$(M_0, \mathbb{T}_0) \to \cdots \to (M_n, \mathbb{T}_n) \to \cdots \to (M_{n+m}, \mathbb{T}_{n+m})$$

  where there is k, such that $1 \leq k \leq n + m$ and

  $$\begin{array}{rcl} M_k(x) & = & M_0(x) - X^n(x) \\ & = & M_0(x) - (Y^n \cup (Z^n - Y^a))(x) \\ & = & M_0(x) - \max(Y^n(x), Z^n(x) - Y^a(x)) \end{array}$$

will proceed as in the previous case for $X^p(x)$. Either the k with the minimum store is found during execution of $A\cdot$ (e.g. $k \leq n$) or k is during the execution of $B\cdot$ (e.g. $k > n$).

To prove that there will always be such a run and k, we must make a case distinction on the value of $X^n(x) = \max(Y^n(x), Z^n(x) - Y^a(x))$:

- If $Y^n(x) = \max(Y^n(x), Z^n(x) - Y^a(x))$ we can use the run of $A\cdot$ which by the inductive hypothesis has a configuration $(M_{k_A}, \mathbb{T}_{k_A})$ such that $M_{k_A}(x) = M_0(x) - Y^n(x) = M_0(x) - X^n(x)$, so we can use k_A as k.
- In the other case, $Z^n(x) - Y^a(x) = \max(Y^n(x), Z^n(x) - Y^a(x))$, we use any run of $A\cdot$ and we have $(M_n, \mathbb{T}_n) = (M_n, \mathbb{T}[\mathsf{Lf}(BE')]_\alpha)$ where $M_n(x) = M_0(x) + Y^a(x)$. We can then choose the run of $B\cdot$ where there is a k_B such that

  $$M_{n+k_B}(x) = M_n(x) - Z^n(x) = \\ M_0(x) + Y^a(x) - Z^n(x) = M_0(x) - (Z^n(x) - Y^a(x)) = \\ M_0(x) - X^n(x)$$

  and use $n + k_B$ as k.

Parallel. Assume the type of $E = (A||B)\cdot$ is derived by an application of this form:

$$\frac{\Gamma \vdash A : Y \qquad \Gamma \vdash B : Z}{\Gamma \vdash (A \,||\, B)\cdot : Y + Z} \text{(Parallel)}$$

From assumptions I have $\Gamma \models_{\mathcal{R}} (M_0, \mathbb{T}[\mathsf{Lf}((A||B)\cdot E')]_\alpha)$ for some M_0 and E'. From the inductive hypothesis I have knowledge of runs of A and B of these forms:

$$(M_0, \mathbb{T}[\mathsf{Lf}(A)]_{\alpha l}) \to \cdots \to (M_j, \mathbb{T}[\mathsf{Lf}(\epsilon)]_{\alpha l}) \tag{2.26}$$
$$(M'_0, \mathbb{T}[\mathsf{Lf}(B)]_{\alpha r}) \to \cdots \to (M'_h, \mathbb{T}[\mathsf{Lf}(\epsilon)]_{\alpha r}) \tag{2.27}$$

For any of these runs, there exist runs of the following forms:

$$(M_0, \mathbb{T}[\mathsf{Nd}(E', \mathsf{Lf}(A), \mathbb{R})]_\alpha) \to \cdots \to (M_j, \mathbb{T}[\mathsf{Nd}(E', \mathsf{Lf}(\epsilon), \mathbb{R})]_\alpha) \tag{2.28}$$
$$(M'_0, \mathbb{T}[\mathsf{Nd}(E', \mathbb{R}, \mathsf{Lf}(B))]_\alpha) \to \cdots \to (M'_h, \mathbb{T}[\mathsf{Nd}(E', \mathbb{R}, \mathsf{Lf}(\epsilon))]_\alpha) \tag{2.29}$$

If the run of A is of length j and the run of B is of length h, then the length of a run of $(A||B)$ is of length $j+h+3$, since all transitions in both runs must be done, in addition there will be one osParIntr at the start of the run, one of either osParElimL or osParElimR some time during the run, and finally, at the end an instance of osParElim - in sum, three extra transitions. If the run was first exclusively transitions on A and then B, it could look like this:

$$(M_0, \mathbb{T}[\mathsf{Lf}((A||B)\cdot E')]_\alpha) \to (M_0, \mathbb{T}[\mathsf{Nd}(E', \mathsf{Lf}(A), \mathsf{Lf}(B))]_\alpha) \to \\ \cdots \to (M_j, \mathbb{T}[\mathsf{Nd}(E', \mathsf{Lf}(\epsilon), \mathsf{Lf}(B))]_\alpha) \\ \to (M_j, \mathbb{T}[\mathsf{Nd}(E', \mathsf{Lf}(B))]_\alpha) \to \\ \cdots \to (M_j + M'_h - M'_0, \mathbb{T}[\mathsf{Nd}(E', \mathsf{Lf}(\epsilon))]_\alpha) \to (M_j + M'_h - M'_0, \mathbb{T}[\mathsf{Lf}(E')]_\alpha)$$

This need not be the case - the transitions from the run of A could come in between transitions from the run of B.

I will now treat the three sharpness properties separately:

- $X^n(x)$. I must now create a run of $(A||B)$ of some length n, where there is a k such that $0 \leq k \leq n$ and $M_k(x) = M_0(x) - X^n(x) = M_0(x) - Y^n(x) - Z^n(x)$. First, choose the run of A where there is a k_A such that $M_{k_A}(x) = M_0(x) - Y^n(x)$. Stop the run at exactly this state:

  $$(M_0, \mathbb{T}[\mathsf{Nd}(E', \mathsf{Lf}(A), \mathsf{Lf}(B))]_\alpha) \to \cdots \to (M_{k_A}, \mathbb{T}[\mathsf{Nd}(E', \mathbb{R}_k, \mathsf{Lf}(B))]_\alpha)$$

  Now, equivalently, choose the run of B starting at this state (which I can do because of soundness), where there is a k_B such that $M_{k_A+k_B}(x) = M_{k_A}(x) - Z^n(x)$. Stop the run at exactly this state:

  $$(M_{k_A}, \mathbb{T}[\mathsf{Nd}(E', \mathbb{R}_k, \mathsf{Lf}(B))]_\alpha) \to \cdots \to (M_{k_A+k_B}, \mathbb{T}[\mathsf{Nd}(E', \mathbb{R}_{k_A}, \mathbb{R}'_{k_B})]_\alpha)$$

  Let $k = k_A + k_B$, and we get $M_k(x) = M_{k_A}(x) - Z^n(x) = M_0(x) - Y^n(x) - Z^n(x) = M_0(x) - X^n(x)$. For the rest of the run do the remaining transitions in the runs of A and B, which by soundness are all possible.
- $X^p(x)$. I must now create a run of $(A||B)$ of some length n, where there is a k such that $0 \leq k \leq n$ and $M_k(x) = M_0(x) + X^p(x) = M_0(x) + Y^p(x) + Z^p(x)$. First, choose the run of A where there is a k_A such that $M_{k_A}(x) = M_0(x) + Y^p(x)$. Stop the run at exactly this state:

  $$(M_0, \mathbb{T}[\mathsf{Nd}(E', \mathsf{Lf}(A), \mathsf{Lf}(B))]_\alpha) \to \cdots \to (M_{k_A}, \mathbb{T}[\mathsf{Nd}(E', \mathbb{R}_k, \mathsf{Lf}(B))]_\alpha)$$

  Now, equivalently, choose the run of B starting at this state (which I can do because of soundness), where there is a k_B such that $M_{k_A+k_B}(x) = M_{k_A}(x) + Z^p(x)$. Stop the run at exactly this state:

  $$(M_{k_A}, \mathbb{T}[\mathsf{Nd}(E', \mathbb{R}_k, \mathsf{Lf}(B))]_\alpha) \to \cdots \to (M_{k_A+k_B}, \mathbb{T}[\mathsf{Nd}(E', \mathbb{R}_{k_A}, \mathbb{R}'_{k_B})]_\alpha)$$

  Let $k = k_A + k_B$, and we get $M_k(x) = M_{k_A}(x) + Z^p(x) = M_0(x) + Y^n(x) + Z^n(x) = M_0(x) + X^p(x)$. For the rest of the run do the remaining transitions in the runs of A and B, which by soundness are all possible.

□

2.9 Termination

2.9.1 Proof of lemma 2.4.22

The lemma is: *if $\Gamma \vdash E : X$ for some Γ, E and X, then for any $\mathbb{T}$, $\mathcal{R}$, α and M such that $\Gamma \models_{\mathcal{R}} (M, \mathbb{T}[\mathsf{Lf}(E)]_\alpha)$ we have that any run of E in context $\mathbb{T}$, on position α and starting with store M has finite length.*

I will prove this by induction on the typing derivation of $\Gamma \vdash E : X$. The inductive hypothesis is: *for any shorter derivation $\Gamma' \vdash E : X$ such that Γ' is a sub-basis of Γ, it is the case that any run of E has finite length.*

Axiom

$$\frac{}{\oslash \vdash \epsilon : \langle [], [], [] \rangle}$$

We have only one degenerate "run" of length 0.

Inductive cases

WeakenB $\Gamma = \Gamma', x \prec B$

$$\frac{\Gamma' \vdash E : X \quad \Gamma' \vdash B : Y \quad x \notin \mathsf{dom}(\Gamma')}{\Gamma', x \prec B \vdash E : X}$$

Since E is the same in the conclusion and the premise, this proof is easy — we know already by the inductive hypothesis on the premise $\Gamma' \vdash E : X$ that any run of E has finite length.

New $E = \mathsf{new}\, y\cdot$, $\Gamma = \Gamma', y \prec A$.

$$\frac{\Gamma' \vdash A : Y \quad y \notin \mathsf{dom}(\Gamma')}{\Gamma', y \prec A \vdash \mathsf{new}\, y\cdot : X = \langle Y^n, Y^p + y, Y^a + y \rangle}$$

By the inductive hypothesis any run of A has finite length. Since any run of E is an instance of osNew followed by some run of A, the run of E must also have finite length, namely one more step than the run of A.

Del $E = \mathsf{del}\, y\cdot$.

$$\frac{\Gamma \vdash A : Y \quad y \prec A \in \Gamma}{\Gamma \vdash \mathsf{del}\, y\cdot : \langle [y], [], [-y] \rangle}$$

Starting from a well-formed configuration there is only one run of $\mathsf{del}\, y\cdot$. This run is actually independent of the type and runs of A, so we do not need the inductive hypothesis in this case. The length is 1.

Seq

$$\frac{\Gamma \vdash A\cdot : Y \qquad \Gamma \vdash B\cdot : Z}{\Gamma \vdash A \cdot B\cdot : X = \langle Y^n \cup (Z^n - Y^a), Y^p \cup (Y^a + Z^p), Y^a + Z^a \rangle}$$

A run of E consists of all transitions from some run of A followed by a run of B. Since both runs have finite lengths, say n_A and n_B by the inductive hypothesis, any run of E must also have finite length $n_A + n_B$.

Parallel. Assume the type of $E = (A||B)\cdot$ is inferred by an application of this form:

$$\frac{\begin{array}{c}(\textsc{Parallel}) \\ \Gamma \vdash A : Y \qquad \Gamma \vdash B : Z\end{array}}{\Gamma \vdash (A \,||\, B)\cdot : Y + Z}$$

We have from the inductive hypothesis that any runs of A and B have finite lengths n_A and n_B. A run of E starts with an instance of osParIntr.

Then follows all transitions from some runs of A and B. Every transition in the run of $(A||B)$ must now be the following transition in some run of A or of B. Since both these runs are finite by the inductive hypothesis, we will after

a finite number of steps get only ϵ in one of the leaves. After this we run the rest of the other branch and one instance of osParElimL or osParElimR in some order. It should be easy to see that the number of these transitions will be $n_A + n_B + 1$. Any transition must either be some transition from this run of A, some transition in a run of B or the single osParElimR or osParElimL. Since the runs of A and B are finite, this means the run of $(A||B)$ must be finite.

The last transition in the run is an instance of osParElim. There can be no more transitions in the run than this, so the run of E must also have finite length, namely $n_A + n_B + 3$. $\square$

Chapter 3

Sharpness of the basic system with only choice and scope from chapter 2 of [13]

This chapter is a proof of the "sharpness" of the system defined in Chapter 2 in [13]. Some important definitions of this system follow. The main differences between this system and the one described in the main chapter of this thesis ("Global Resources") is that there is no parallel composition ("||") or explicit deallocation ("del"), but there is a choice operator ("+") and scope ("{" and "}").

3.1 Definitions

Definition 3.1.1 (Language).

$$\begin{array}{rcl} Prog & \rightarrow & \underline{Decls; E} \\ Decls & \rightarrow & \overline{x \prec E;} \\ E & \rightarrow & \\ & & \epsilon \\ & | & \mathsf{new}x \\ & | & EE \\ & | & (E + E) \\ & | & \{E\} \end{array}$$

A configuration in this system is a stack of pairs (M, E) where M is a store, that is, an unsigned multiset of resources, and E is an expression, that is, a word in the language of the grammar rule E above.

I extend the syntax for stacks to allow for empty stacks:

$$\mathbb{S} ::= \gamma \,|\, \mathbb{S} \circ (M, E)$$

such that γ indicates the bottom or an empty stack. Also, if $\mathbb{S} = \gamma \circ (M_1, E_1) \circ \cdots \circ (M_k, E_k)$, where $k = \mathsf{hi}(\mathbb{S})$, let $[\mathbb{S}]$ be the multiset defined by $[\mathbb{S}](x) = \Sigma_{i=1}^{k} M_i(x)$

Definition 3.1.2 (Operational Semantics).

$$\frac{(\mathsf{osNew}) \quad x \prec A \in Decls}{\mathbb{S} \circ (M, \mathsf{new} x E) \longrightarrow \mathbb{S} \circ (M + x, AE)}$$

$$\frac{(\mathsf{osChoice}) \quad i \in \{1, 2\}}{\mathbb{S} \circ (M, (A_1 + A_2)E) \longrightarrow \mathbb{S} \circ (M, A_i E)}$$

$$\frac{(\mathsf{osPush})}{\mathbb{S} \circ (M, \{A\}E) \longrightarrow \mathbb{S} \circ (M, E) \circ ([], A)}$$

$$\frac{(\mathsf{osPop})}{\mathbb{S} \circ (M, E) \circ (M', \epsilon) \longrightarrow \mathbb{S} \circ (M, E)}$$

Types are pairs $X = \langle X^i, X^o \rangle$, where X^i and X^o are multisets. X^i represents the maximum positive increase in the number of simultaneously active instances during the run of the expression, while X^o is the upper bound for the number of instances active after execution. These properties are formalised in the sharpness lemma below.

A typing judgement is of the form $\Gamma \vdash E : X$. Γ is a basis, E an expression and X a type. X^o corresponds to the type X^a in "Global resources".

$$\frac{(\textsc{Axiom})}{\oslash \vdash \epsilon : \langle [], [] \rangle} \qquad \frac{(\textsc{WeakenB}) \quad \Gamma \vdash A : X \qquad \Gamma \vdash B : Y \quad x \notin \mathsf{dom}(\Gamma)}{\Gamma, x \prec B \vdash A : X}$$

$$\frac{(\textsc{Scope}) \quad \Gamma \vdash A : X}{\Gamma \vdash \{A\} : \langle X^i, [] \rangle} \qquad \frac{(\textsc{New}) \quad \Gamma \vdash A : X \quad x \notin \mathsf{dom}(\Gamma)}{\Gamma, x \prec A \vdash \mathsf{new}\, x : \langle X^i + x, X^o + x \rangle}$$

$$\frac{(\textsc{Choice}) \quad \Gamma \vdash A : X \qquad \Gamma \vdash B : Y}{\Gamma \vdash (A + B) : \langle X^i \cup Y^i, X^o \cup Y^o \rangle} \qquad \frac{(\textsc{Seq}) \quad \Gamma \vdash A : X \qquad \Gamma \vdash B : Y \quad A, B \neq \epsilon}{\Gamma \vdash AB : \langle X^i \cup (X^o + Y^i), X^o + Y^o \rangle}$$

Definition 3.1.3 (Well-typed programs). *Program $Prog = Decls; E$ is well-typed if there exist a reordering Γ of declarations in $Decls$ and a type X such that $\Gamma \vdash E : X$.*

Definition 3.1.4 (Well-typed configurations). *Configuration $\mathbb{S}$ is well-typed with respect to a basis Γ, notation $\Gamma \models \mathbb{S}$, if for all $1 \leq k \leq \mathsf{hi}(\mathbb{S})$ such that $\mathbb{S}(k) = (M, E)$, there exists X such that*

$$\Gamma \vdash E : X$$

The lemmas of progress, preservation and soundness give a kind of minimal guarantee for a well-typed program: it will not get stuck. But the type of a program is given in an "interval" because of the possibilities of choice, so we lack an exact type. What we would like is to know that the bounds are reachable — that there exist possible runs of a well-typed program exploiting the upper bounds of the type. This is the sharpness of the typing system.

Definition 3.1.5 (Run of an expression). *A run of an expression E is a sequence of configurations, where*

- *E is the expression at the top of the stack in the first configuration in the sequence.*
- *In any pair of two consecutive configurations the second is formed from the first using one of the rules in the operational semantics.*
- *The last configuration only differs from the start configuration in the top of the stack, and the expression at the top of the stack is empty (ϵ).*
- *The length of the run is the number of configurations minus one.*

I will enumerate the configurations in a run from 0 to length: $\mathbb{S}_0 \to \cdots \to \mathbb{S}_{\mathsf{length}}$

Lemma 3.1.6 (Sharpness). *If $\Gamma \vdash E : X$ then, for every component x, for every well-typed configuration $\mathbb{S}_0 = \mathbb{S} \circ (M, E)$ we have the following properties:*

1. *There exists a run $\mathbb{S}_0 \to \cdots \to \mathbb{S}_n = \mathbb{S} \circ (M', \epsilon)$ of E where there is a k, $0 \leq k \leq n$ such that $[\mathbb{S}_k](x) = X^i(x) + [\mathbb{S}_0](x)$.*
2. *There exists a (generally different) run $\mathbb{S}_0 \to \cdots \to \mathbb{S}_m$ of E where $[\mathbb{S}_m](x) = X^o(x) + [\mathbb{S}_0](x)$.*

Generally, the runs attaining the different maxima will be different for different components, and different for the two types of maximum, because of the CHOICE rule.

As an example, take a look at the possible runs of this expression (where $\mathsf{new}x^3$ means three repetitions of $\mathsf{new}x$) :

$$(\{\mathsf{new}\, x^3\} + \mathsf{new}x)\mathsf{new}x \tag{3.1}$$

The type of this expression is $\langle [x \mapsto 3], [x \mapsto 2] \rangle$. To achieve the different maxima, we must use two different runs. First we will consider the run which gives the maximum number of x when $k = 5$, with

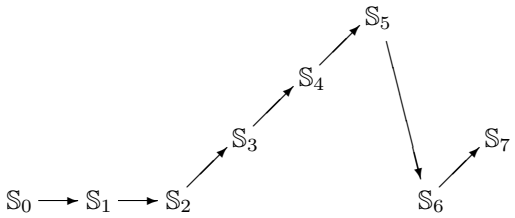
$$[\mathbb{S}_5](x) = [\mathbb{S}](x) + M(x) + 3 = [\mathbb{S}_0](x) + X^i(x)$$

$$\begin{array}{ll}
\mathbb{S} \circ (M, (\{\mathsf{new}x^3\} + \mathsf{new}x)\mathsf{new}x) & = \mathbb{S}_0 \\
\to \mathbb{S} \circ (M, \{\mathsf{new}x^3\}\mathsf{new}x) & = \mathbb{S}_1 \\
\to \mathbb{S} \circ (M, \mathsf{new}x) \circ ([], \mathsf{new}x^3) & = \mathbb{S}_2 \\
\to^3 \mathbb{S} \circ (M, \mathsf{new}x) \circ ([x \mapsto 3], \epsilon) & = \mathbb{S}_5 \\
\to \mathbb{S} \circ (M, \mathsf{new}x) & = \mathbb{S}_6 \\
\to \mathbb{S} \circ (M + [x], \epsilon) & = \mathbb{S}_7
\end{array}$$

This run does not leave the maximum number of x after the run, as

$$[\mathbb{S}_7](x) = [\mathbb{S}](x) + M(x) + 1 = [\mathbb{S}_0](x) + 1 < [\mathbb{S}_0](x) + 2 = [\mathbb{S}_0](x) + X^o(x)$$

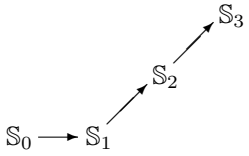
The number of x during the run can also be visualised, letting vertical axis represent number of x :



To get the maximum number of x after the run, we must use another, shorter run:

$$\begin{array}{ll} \mathbb{S} \circ (M, (\{\mathsf{new}x^3\} + \mathsf{new}x)\mathsf{new}x) & = \mathbb{S}_0 \\ \rightarrow \mathbb{S} \circ (M, \mathsf{new}x\ \mathsf{new}x) & = \mathbb{S}_1 \\ \rightarrow \mathbb{S} \circ (M + [x], \mathsf{new}x) & = \mathbb{S}_2 \\ \rightarrow \mathbb{S} \circ (M + [x \mapsto 2], \epsilon) & = \mathbb{S}_3 \end{array}$$

The last run could also be visualised like this:



This run does leave the maximum number of x after the run, as the length of the run is 3 and

$$[\mathbb{S}_3](x) = [\mathbb{S}](x) + M(x) + 2 = [\mathbb{S}_0](x) + 2 = [\mathbb{S}_0](x) + X^o(x)$$

but the maximum number of x during the run is lower than the maximum which we got using the previous run. These are the only two possible runs of the expression, as there is only one "+" in the expression, so there is no other run which achieves both maxima. This example shows that it can be (and often is) the case that different runs, often also of different length, must be used to achieve the different maxima for the same resource.

Going back to the formulation of the lemma, we see that there must be a run of length m where $[\mathbb{S}_m](x) = X^o(x) + [\mathbb{S}_0](x)$. Now, since $\mathbb{S}_m = \mathbb{S} \circ (M', \epsilon)$ and $\mathbb{S}_0 = \mathbb{S} \circ (M, E)$, we also get $M'(x) = M(x) + X^o(x)$.

Corollary 3.1.7 (Sharpness of program). *For any program $Prog = Decls; E$ such that $\Gamma \models ([], E)$ where Γ some reordering of $Decls$, for every component x, there is a run $([], Prog) = \mathbb{S}_0 \rightarrow \cdots \rightarrow \mathbb{S}_n = (M, \epsilon)$, where there is a k, $0 \leq k \leq n$ such that $[\mathbb{S}_k](x) = X^i(x)$ and there exists a run $([], Prog) \rightarrow \cdots \rightarrow (M, \epsilon)$ where $M(x) = X^o(x)$.*

Together with proving sharpness, I will also prove another property of the runs, which looks quite similar to soundness, but is not the same. In the later chapters I will need this property during the proof of sharpness. In this case, I have added the lemma only because it is an interesting property by itself.

Lemma 3.1.8 (Runs change store respecting limits). *If $\Gamma \vdash E : X$ for some E, X and Γ, it is the case that for all $\mathbb{S}$ and M such that $\Gamma \models \mathbb{S}_0 = \mathbb{S} \circ (M, E)$ and for all runs of the form $\mathbb{S}_0 \rightarrow \cdots \rightarrow \mathbb{S}_n$ of E, it is the case that $[\mathbb{S}_n] - [\mathbb{S}_0] \subseteq X^o$.*

3.2 Proof

The proof is by induction on typing derivations. The inductive hypothesis is: for all shorter typing derivations $\Gamma \vdash E : X$, it is the case that for every component x and well-typed configuration $\mathbb{S}_0 = \mathbb{S} \circ (M, E)$ we have the following properties:

1. There exists a run $\mathbb{S}_0 \to \cdots \to \mathbb{S}_n = \mathbb{S} \circ (M', \epsilon)$ of E where there is a k, $1 \leq k \leq n$ such that $[\mathbb{S}_k](x) = X^i(x) + [\mathbb{S}_0](x)$.
2. There exists a (generally different) run $\mathbb{S}_0 \to \cdots \to \mathbb{S}_m = \mathbb{S} \circ (M', \epsilon)$ of E where $[\mathbb{S}_m](x) = X^o(x) + [\mathbb{S}_0](x)$.
3. For all runs $\mathbb{S}_0 \to \cdots \to \mathbb{S}_n = \mathbb{S} \circ (M', \epsilon)$ of E we have that $[\mathbb{S}_n](x) - [\mathbb{S}_0](x) \leq X^o(x)$.

The important step in each part of the proof below is the relation between the type and the operational semantics: we must show that runs giving the values in the types are possible given the operational semantics. Each part of the proof considers one typing rule. First I give an instance of the rule, how it could have been used to deduce $\Gamma \vdash E : X$. Then I try to establish what kinds of runs we can get using E and what their correspondence is with runs of expressions in the premises. Finally I must show the existence of the runs with the wanted properties, often using runs of the expressions in the premises, which we have by the inductive hypothesis.

Since the proof only deals with well-typed configurations, preservation is given by the preservation lemma: if $\Gamma \models \mathbb{S}$ and $\mathbb{S} \to \mathbb{S}'$, then also $\Gamma \models S'$.

Definition 3.2.1 ($\Gamma - \{x \prec A\}$). *By $\Gamma - \{x \prec A\}$ I mean the basis containing all declarations in Γ except the last one, in the case that this last one is equal to $\{x \prec A\}$. The expression is only valid if $\{x \prec A\}$ is actually the last declaration in Γ, and it is not possible to remove other declarations than the last.*

Base case

Axiom

$$\frac{}{\oslash \vdash \epsilon : \langle [], [] \rangle}$$

$$\mathbb{S}_0 = \mathbb{S} \circ (M, E) = \mathbb{S} \circ (M, \epsilon)$$

There is only one "run" of length 0, where no resources are created. Let $k = 0$. Since $X^i(x) = X^o(x) = 0$ this suffices.

Inductive cases

WeakenB

$$\frac{\Gamma - \{x \prec B\} \vdash E : X \quad \Gamma - \{x \prec B\} \vdash B : Y \quad x \notin \mathsf{dom}(\Gamma - \{x \prec B\})}{\Gamma \vdash E : X}$$

This proof is easy — we know by the inductive hypothesis that there exist runs of E with the properties needed for sharpness of X, and this is what we need to prove.

New Let $E = \mathsf{new}\, y$ and $\Gamma - \{y \prec A\} \vdash A : Y$.

$$\frac{\Gamma - \{y \prec A\} \vdash A : Y \quad y \notin \mathsf{dom}(\Gamma - \{y \prec A\})}{\Gamma \vdash \mathsf{new}\, y : \langle Y^i + y, Y^o + y\rangle}$$

For any run $\mathbb{S} \circ (M + y, A) \to \cdots \to \mathbb{S} \circ (M' + y, \epsilon)$ of A, there is a corresponding run

$$\mathbb{S}_0 = \mathbb{S} \circ (M, \mathsf{new}\, y) \to \mathbb{S} \circ (M + y, A) \to \cdots \to \mathbb{S} \circ (M' + y, \epsilon) = \mathbb{S}_n$$

of $\mathsf{new}\, y$.

- For $y \neq x$ we can use the runs of A which exist by the inductive hypothesis for the properties of Y and that $Y^*(x) = X^*(x)$.
- For $y = x$ we have $y \notin \mathsf{dom}(\Gamma - \{y \prec A\})$ and by Lemma 2.3.9 (Valid typing judgement), $Y^* \subseteq \mathsf{dom}(\Gamma - \{y \prec A\})$, so $Y^*(y) = 0$ and there is no y created in the run of A. The extra y is added to the store in the first step of the run, and this will be the only y during the run of A. I choose $k = 1$, and $[\mathbb{S}_1](y) = [\mathbb{S}_0](y) + 1$ while $X^i(y) = Y^i(y) + 1 = 1$. We also have $X^o(y) = Y^o(y) + 1 = 1$ and $[\mathbb{S}_n](y) = [\mathbb{S}_0](y) + 1$. So all three properties hold for any run of $\mathsf{new}\, y$.

Seq

$$\frac{\Gamma \vdash A : Y \qquad \Gamma \vdash B : Z \quad A, B \neq \epsilon}{\Gamma \vdash AB : \langle Y^i \cup (Y^o + Z^i), Y^o + Z^o\rangle}$$

A run of $A\,B$ consists of a run of A followed by a run of B. From inductive hypothesis we have knowledge of runs of A ending in ϵ. Adding B to this gives a sequence of configurations from $\mathbb{S} \circ (M, AB)$ to $\mathbb{S} \circ (M', B)$ using the same transitions. In other words, for any run of length n

$$\mathbb{S} \circ (M, A) \to \cdots \to \mathbb{S} \circ (M', \epsilon)$$

there is a sequence of $n + 1$ configurations

$$\mathbb{S} \circ (M, AB) \to \cdots \to \mathbb{S} \circ (M', B)$$

with the same transitions. For the runs of B I need no such transformation, and can directly use the runs existing by the inductive hypothesis. So for any pair of a run of A and a run of B, there is a run

$$\mathbb{S}_0 = \mathbb{S} \circ (M, AB) \to \cdots \to \mathbb{S} \circ (M', B) = \mathbb{S}_n \to \cdots \to \mathbb{S} \circ (M'', \epsilon) = \mathbb{S}_{n+m} \quad (3.2)$$

of $A\,B$, using the same transitions. If the run of A is of length n and the run of B is of length m, the run of $A\,B$ will be of length $n + m$.

I will start with finding a run resulting in $[\mathbb{S}_{n+m}](x) = [\mathbb{S}_0](x) + X^o(x) = [\mathbb{S}_0](x) + Y^o(x) + Z^o(x)$. First I choose the run of A resulting in $[\mathbb{S}_n](x) = [\mathbb{S}_0](x) + Y^o(x)$ and then the run of B finally resulting in :

$$[\mathbb{S}_{n+m}](x) = [\mathbb{S}_n](x) + Z^o(x) = [\mathbb{S}_0](x) + Y^o(x) + Z^o(x) = [\mathbb{S}_0](x) + X^o(x)$$

and we are done with this first part.

Finding a run of $A\,B$: $\mathbb{S}_0 \to \cdots \to \mathbb{S} \circ (M', B) = \mathbb{S}_{n'} \to \cdots \to \mathbb{S}_{n'+m'}$, where there is k, such that $1 \leq k \leq n' + m'$ and

$$\begin{array}{rcl} [\mathbb{S}_k](x) & = & [\mathbb{S}_0](x) + X^i(x) \\ & = & [\mathbb{S}_0](x) + (Y^i \cup (Y^o + Z^i))(x) \\ & = & [\mathbb{S}_0](x) + \mathsf{max}(Y^i(x), Y^o(x) + Z^i(x)) \end{array}$$

is not that easy. Either the k with the maximum store is found during execution of A (i.e. $k \leq n'$) or during the execution of B (i.e. $k > n'$).

As an example, compare the expression

$$(\{\mathsf{new}\, x^3\} + \mathsf{new}x)\mathsf{new}x$$

which we also looked at earlier (3.1) and which has type $\langle [x \mapsto 3], [x \mapsto 2] \rangle$ with this expression:

$$(\{\mathsf{new}\, x\} + \mathsf{new}x)\mathsf{new}x \tag{3.3}$$

(3.3) has type $\langle [x \mapsto 2], [x \mapsto 2] \rangle$. In (3.1) we saw that the run reaching the maximal number of x used the left choice $\{\mathsf{new}\, x^3\}$. To get the maximal amount of x in (3.3) we must use the right hand choice to get the following run:

$$\begin{array}{ll} \mathbb{S} \circ (M, (\{\mathsf{new}x\} + \mathsf{new}x)\mathsf{new}x) & = \mathbb{S}_0 \\ \to \mathbb{S} \circ (M, \mathsf{new}x\, \mathsf{new}x) & = \mathbb{S}_1 \\ \to \mathbb{S} \circ (M + [x], \mathsf{new}x) & = \mathbb{S}_2 \\ \to \mathbb{S} \circ (M + [x \mapsto 2], \epsilon) & = \mathbb{S}_3 \end{array}$$

To prove that there will always be such a run and k, we must do a case distinction on the value of $X^i(x) = \mathsf{max}(Y^i(x), Y^o(x) + Z^i(x))$:

- If $Y^i(x) = \mathsf{max}(Y^i(x), Y^o(x) + Z^i(x))$ we can use the run of A which by the inductive hypothesis has a configuration $\mathbb{S}_{k_A}$ such that $[\mathbb{S}_{k_A}](x) = [\mathbb{S}_0](x) + Y^i(x) = [\mathbb{S}_0](x) + X^i(x)$, so we can use k_A as k.
- In the other case, $Y^o(x) + Z^i(x) = \mathsf{max}(Y^i(x), Y^o(x) + Z^i(x))$, we use the run of A which ends in $\mathbb{S}_n = \mathbb{S} \circ (M', B)$ where $[\mathbb{S}_n](x) = [\mathbb{S}_0](x) + Y^o(x)$ and then the run of B where there is a k_B such that

  $$[\mathbb{S}_{k_B}](x) = [\mathbb{S}_n](x) + Z^i(x) = [\mathbb{S}_0](x) + Y^o(x) + Z^i(x) = [\mathbb{S}_0](x) + X^i(x)$$

  and use $n + k_B$ as k.

All I have left is now showing that for any run of AB we have $[\mathbb{S}_{n+m}](x) - [\mathbb{S}_0](x) \leq X^o(x)$, where n is the length of the run of A and m is the length of the run of B as in (3.2). From the inductive hypothesis I have $[\mathbb{S}_n] - [\mathbb{S}_0](x) \leq Y^o(x)$ and $[\mathbb{S}_{n+m}] - [\mathbb{S}_n](x) \leq Z^o(x)$. Adding these inequalities I get $[\mathbb{S}_{n+m}] - [\mathbb{S}_0](x) \leq Y^o(x) + Z^o(x) = X^o(x)$.

Choice Let $E = (A + B)$, $\Gamma \vdash A : Y$ and $\Gamma \vdash B : Z$.

$$\frac{\Gamma \vdash A : Y \quad \Gamma \vdash B : Z}{\Gamma \vdash (A + B) : \langle Y^i \cup Z^i, Y^o \cup Z^o \rangle}$$

For this rule, I must use two inductive hypotheses, one for each of the premises in the typing rule ($A : Y$ and $B : Z$). This means the whole proof is an instance

of simultaneous induction. To run $(A+B)$, we must choose a run of A or a run of B. For any run of A or B, that is, $\mathbb{S} \circ (M, A) \to \cdots \to \mathbb{S} \circ (M', \epsilon)$, there is a corresponding run of $(A + B)$, with the same transitions, only one instance of osChoice added in front, e.g..:

$$\mathbb{S} \circ (M, (A + B)) \to \mathbb{S} \circ (M, A) \to \cdots \to \mathbb{S} \circ (M', \epsilon)$$

By the inductive hypothesis there is a run of A and a state k_A in the run such that $[\mathbb{S}_{k_A}](x) = [\mathbb{S}_0](x) + Y^i(x)$, and correspondingly for B there is a run and a k_B. For a run of $(A + B)$ with a state k achieving $[\mathbb{S}_k](x) = [\mathbb{S}_0](x) + X^i(x) = [\mathbb{S}_0](x) + (Y^i \cup Z^i)(x) = [\mathbb{S}_0](x) + \mathsf{max}(Y^i(x), Z^i(x))$, choose the run of A and $k = k_A$ if $Y^i(x) > Z^i(x)$, otherwise choose the run of B and $k = k_B$. We will then have

$$[\mathbb{S}_k](x) = [\mathbb{S}_0](x) + \mathsf{max}(Y^i(x), Z^i(x)) = [\mathbb{S}_0](x) + X^i(x)$$

The same argument can be used for $[\mathbb{S}_0](x) + X^o(x)$.

Now I must show that for any $\mathbb{S}$ and M such that $\Gamma \models \mathbb{S}_0 = \mathbb{S} \circ (M, (A+B))$ and any run of the form $\mathbb{S}_0 \to \mathbb{S}_1 \to \cdots \to \mathbb{S}_{n+1} = \mathbb{S} \circ (M', \epsilon)$ of $(A + B)$ we have $[\mathbb{S}_{n+1}](x) - [\mathbb{S}_0](x) \leq X^o(x)$. From the inductive hypothesis I have $[\mathbb{S}_{n+1}](x) - [\mathbb{S}_1](x) \leq Y^o(x)$ if we chose to run A and $[\mathbb{S}_{n+1}](x) - [\mathbb{S}_1](x) \leq Z^o(x)$ if we chose to run B. Since we have from the typing rule that $Y^o(x) \leq X^o(x)$ and $Z^o(x) \leq X^o(x)$ and we have that $[\mathbb{S}_1] = [\mathbb{S}_0]$, we are done.

Scope $E = \{A\}$.

$$\frac{\Gamma \vdash A : Y}{\Gamma \vdash \{A\} : \langle Y^i, [] \rangle}$$

In the operational semantics, a new pair $([], A)$ is created on top of the stack through the transition rule osPush, A is run, and then osPop removes the pair again. So, for any run

$$\mathbb{S} \circ ([], A) \to \cdots \to \mathbb{S} \circ (M', \epsilon)$$

of A there is a run

$$\begin{array}{ll} \mathbb{S} \circ (M, \{A\}) & \mathbb{S}_0 \\ \to \mathbb{S} \circ (M, \epsilon) \circ ([], A) & \mathbb{S}_1 \\ \to \cdots \to \mathbb{S} \circ (M, \epsilon) \circ (M', \epsilon) & \mathbb{S}_{n-1} \\ \to \mathbb{S} \circ (M, \epsilon) & \mathbb{S}_n \end{array}$$

of $\{A\}$ using the same transitions but in addition having osPush and osPop at the start and the end. I can assume existence of wanted runs of A, since $\Gamma \vdash A : Y$ must hold by the typing rule. For X^o any run of A is okay, since no resources are returned ($[\mathbb{S}_n](x) = [\mathbb{S}_0](x)$) and $X^o = []$. For the other property, choose the run and k_A such that

$$[\mathbb{S}_{k_A}](x) = [\mathbb{S}](x) + M(x) + Y^i(x) = [\mathbb{S}_0](x) + Y^i(x) = X^i(x) + [\mathbb{S}_0](x)$$

which exist by the inductive hypothesis. So we can let $k = k_A$.

Chapter 4

Sharpness of the system with choice, scope and del ("Explicit deallocation") in chapter 3 of [13]

This chapter is a proof of the "sharpness" of the system defined in Chapter 3 in [13]. Some important definitions of this system follow. The main differences between this system and the one described in the main chapter of this thesis ("Global Resources") is that there is no parallel composition ("||"), but there is a choice operator ("+") and scope ("{" and "}").

4.1 Definitions

Definition 4.1.1 (Language).

$$
\begin{array}{rcl}
Prog & \rightarrow & \overline{Decls}; E \\
Decls & \rightarrow & \overline{x \prec E}; \\
E & \rightarrow & \\
 & & \epsilon \\
 & | & \mathsf{new}x \\
 & | & \mathsf{del}x \\
 & | & EE \\
 & | & (E + E) \\
 & | & \{E\}
\end{array}
$$

A configuration in this system is a stack of pairs as in the previous chapter. (See page 57.)

Definition 4.1.2 (Operational Semantics).

$$\frac{(\mathsf{osNew}) \quad x \prec A \in Decls}{\mathbb{S} \circ (M, \mathsf{new} x E) \longrightarrow \mathbb{S} \circ (M + x, AE)}$$

$$\frac{(\mathsf{osDel}) \quad x \in M}{\mathbb{S} \circ (M, \mathsf{del} x E) \longrightarrow \mathbb{S} \circ (M - x, E)}$$

$$\frac{(\mathsf{osChoice}) \quad i \in \{1, 2\}}{\mathbb{S} \circ (M, (A_1 + A_2)E) \longrightarrow \mathbb{S} \circ (M, A_i E)}$$

$$\frac{(\mathsf{osPush})}{\mathbb{S} \circ (M, \{A\}E) \longrightarrow \mathbb{S} \circ (M, E) \circ ([], A)}$$

$$\frac{(\mathsf{osPop})}{\mathbb{S} \circ (M, E) \circ (M', \epsilon) \longrightarrow \mathbb{S} \circ (M, E)}$$

Types are triples $X = \langle X^i, X^o, X^l \rangle$, where X^i is an unsigned multiset and the two others are signed multisets. X^i represents the maximum positive increase in the number of simultaneously active instances during the run of the expression, while X^o and X^l are the upper and lower bounds for the number of instances active after execution. These properties are formalised in the sharpness lemma below.

A typing judgement is of the form $\sigma, \Gamma \vdash E : X$. Γ is a basis, E an expression and X a type. σ corresponds to the part X^n of the type in "global resources" (Section 2.3, page 11). X^l and X^o corresponds to the type X^a in "Global resources". The reason why there are two types here is the presence of the choice operator.

$$\frac{(\textsc{Del}) \quad \sigma, \Gamma \vdash A : X \qquad x \in \mathsf{dom}(\Gamma)}{[x], \Gamma \vdash \mathsf{del}\, x : \langle [], [-x], [-x] \rangle} \qquad \frac{(\textsc{WeakenB}) \quad \sigma_1, \Gamma \vdash A : X \qquad \sigma_2, \Gamma \vdash B : Y \quad x \notin \mathsf{dom}(\Gamma)}{\sigma_1, \Gamma, x \prec B \vdash A : X}$$

$$\frac{(\textsc{WeakenS}) \quad \sigma, \Gamma \vdash A : X \qquad \sigma \subseteq \sigma_1}{\sigma_1, \Gamma \vdash A : X} \qquad \frac{(\textsc{Choice}) \quad \sigma_1, \Gamma \vdash A : X \qquad \sigma_2, \Gamma \vdash B : Y}{\sigma_1 \cup \sigma_2, \Gamma \vdash (A + B) : \langle X^i \cup Y^i, X^o \cup Y^o, X^l \cap Y^l \rangle}$$

$$\frac{(\textsc{New}) \quad \sigma, \Gamma \vdash A : X \quad x \notin \mathsf{dom}(\Gamma)}{\sigma, \Gamma, x \prec A \vdash \mathsf{new}\, x : \langle X^i + x, X^o + x, X^l + x \rangle} \qquad \frac{(\textsc{Scope}) \quad [], \Gamma \vdash A : X}{[], \Gamma \vdash \{A\} : \langle X^i, [], [] \rangle}$$

$$\frac{(\textsc{Axiom})}{[], \oslash \vdash \epsilon : \langle [], [], [] \rangle} \qquad \frac{(\textsc{Seq}) \quad \sigma_1, \Gamma \vdash A : X \qquad \sigma_2, \Gamma \vdash B : Y \quad A, B \neq \epsilon}{\sigma_1 \cup (\sigma_2 - X^l), \Gamma \vdash AB : \langle X^i \cup (X^o + Y^i), X^o + Y^o, X^l + Y^l \rangle}$$

Definition 4.1.3 (Well-typed configurations). *Configuration $\mathbb{S}$ is well-typed with respect to a basis Γ, notation $\Gamma \models \mathbb{S}$, if for all $1 \leq k \leq \mathsf{hi}(\mathbb{S})$ such that $\mathbb{S}(k) = (M, E)$, there exists X such that*

$$M, \Gamma \vdash E : X$$

Note now that in this system, the size of the store in a well-typed configuration must be equal to M in the type. This forces the inclusion of the rule WeakenS which destroys sharpness of M. Contrast this with the previous system "global resources", where I could prove sharpness for X^n. For a counterexample of sharpness of M,

$$[x \mapsto c], \oslash \vdash \epsilon : \langle [], [], [] \rangle \quad c \in \mathcal{N}$$

is a valid typing judgement, but the "run" of ϵ does not change the store.

4.2 Sharpness

Lemma 4.2.1 (Sharpness). *If $M, \Gamma \vdash E : X$ then, for every component x, for every well-typed configuration $\mathbb{S}_0 = \mathbb{S} \circ (M, E)$ there exist three generally different runs of E with lengths n_1, n_2 and n_3:*

$$\mathbb{S}_0 \to \cdots \to \mathbb{S}_{n_i} = \mathbb{S} \circ (M^i_{n_i}, \epsilon) \qquad (i \in \{1, 2, 3\})$$

which fulfill one each of the following properties:

1. *There is a k, $0 \leq k \leq n_1$ such that $[\mathbb{S}_k](x) = X^i(x) + [\mathbb{S}_0](x)$.*
2. *$[\mathbb{S}_{n_2}](x) = X^o(x) + [\mathbb{S}_0](x)$.*
3. *$[\mathbb{S}_{n_3}](x) = X^l(x) + [\mathbb{S}_0](x)$.*

Corollary 4.2.2 (Sharpness of programs). *For any program $Prog = Decls; E$ s.t. $[], \Gamma \vdash E : X$ for some reordering Γ of $Decls$, for every component x, there exist three generally different runs with lengths n_1, n_2 and n_3:*

$$([], Prog) = \mathbb{S}_0 \to \cdots \to \mathbb{S}_{n_i} = (M^i_{n_i}, \epsilon) \qquad (i \in \{1, 2, 3\})$$

which fulfill one each of the following properties:

1. *there is a k, $0 \leq k \leq n_1$ such that $[\mathbb{S}_k](x) = X^i(x)$.*
2. *$M^2_{n_2}(x) = X^o(x)$.*
3. *$M^3_{n_3}(x) = X^l(x)$.*

4.3 Introduction

The proof must be changed somewhat from the simpler case. I still do structural induction on typing derivations, but the inductive hypothesis must be strengthened to include cases with a larger than necessary store. The reason for this is that in the proof-cases for Choice and Seq I need to have from the inductive hypothesis that there exist runs starting with a larger store. To do this, I will in each case of the proof give an argument that there exist runs starting from a store of the given size M or larger. I will express this by adding another unsigned multiset N. This is the same as saying that there can be any application of WeakenS after the application of the given rule.

$$\frac{M, \Gamma \vdash E : X \quad M \subseteq M + N}{M + N, \Gamma \vdash E : X}$$

I also use the fact that any number of consecutive applications of WeakenS can be replaced by one single application. This follows from the properties of $\subseteq$.

A run is defined as in definition 3.1.5 on page 59 in the previous chapter.

I must also make sure that if $\Gamma \models \mathbb{S}_0 = \mathbb{S} \circ (M, E)$, that is, $\mathbb{S}_0$ is a well-typed configuration, then $\mathbb{S} \circ (M + N, E)$ is also a well-typed configuration. Otherwise, we could not use the progress lemma to guarantee the existence of the first step of the run.

Since the only change between the two stacks is changing the store from M to $M + N$ at the top of the stack, and we have from WeakenS that the type is still X, the new stack is also well-typed.

In most of the cases of the proofs, we also need to use that the change to the store during a sequence of configurations is independent of the size of this store, as long as it is large enough for any application of del.

Proposition 4.3.1 (Change of store independent of size of store). *For any two sequences of configurations of the same length j*

$$\mathbb{S}_0 = \mathbb{S} \circ (M_0, E_0) \longrightarrow \cdots \longrightarrow \mathbb{S}_j = \mathbb{S} \circ (M_j, E_j)$$

and

$$\mathbb{S}'_0 = \mathbb{S}' \circ (N_0, E'_0) \longrightarrow \cdots \longrightarrow \mathbb{S}'_j = \mathbb{S}' \circ (N_j, E'_j)$$

where for all i, $0 \leq i < j$ the rule used for the transformation $\mathbb{S}_i \longrightarrow \mathbb{S}_{i+1}$ and the subexpression to which the rule is applied is identical to the one used for the transformation $\mathbb{S}'_i \longrightarrow \mathbb{S}'_{i+1}$, we have that

$$M_j - M_0 = N_j - N_0$$

Note that I am comparing two already existing sequences. This means I do not have to show that they exist, since this is assumed. I will prove the lemma by induction on the length of the sequences of configurations. The inductive hypothesis is:

For any $k \leq j$: for any two sequences of configurations of length k:

$$\mathbb{S}_0 = \mathbb{S} \circ (M_0, E_0) \longrightarrow \cdots \longrightarrow \mathbb{S}_j = \mathbb{S} \circ (M_k, E_k)$$

and

$$\mathbb{S}'_0 = \mathbb{S}' \circ (N_0, E'_0) \longrightarrow \cdots \longrightarrow \mathbb{S}'_j = \mathbb{S}' \circ (N_k, E'_k)$$

If for all i, where $0 \leq i < k$, the rule used from the operational semantics to transform $\mathbb{S}_i \longrightarrow \mathbb{S}_{i+1}$ and the subexpression to which the rule is applied is identical to the one used for the transformation $\mathbb{S}'_i \longrightarrow \mathbb{S}'_{i+1}$, then we have that $M_k - M_0 = N_k - N_0$.

- Base Case. The base case is the sequence of length 0. This means $j = 0$ and the wanted property follows immediately since $M_j = M_0$ and $N_j = N_0$.
- Inductive cases. We have the lemma for sequences of configurations

$$\mathbb{S}_0 \longrightarrow \cdots \longrightarrow \mathbb{S}_k$$

where $k \leq j$. Now I need to assure the lemma for all sequences which are one transition longer. This is done by adding the same transition at the right hand end of two equal sequences of length j. Since all sequences shorter than $j+1$ are covered by the inductive hypothesis, we only need to create the sequences of exactly length $j+1$:

$$\mathbb{S}_0 \longrightarrow \cdots \longrightarrow \mathbb{S}_j \longrightarrow \mathbb{S}_{j+1}$$

To accomplish this, I will use a case distinction on the possible transitions from the operational semantics. First, I will treat separately the cases when the stack is higher than it was in the starting configuration, that is, transitions of this form:

$$\mathbb{S} \circ (M_j, E_j) \circ \cdots \circ (M, E) \to \mathbb{S} \circ (M_j, E_j) \circ \cdots \circ (M', E')$$

As we can see, in these cases the store we are analysing does not change, that is $M_{j+1} = M_j$ and $N_{j+1} = N_j$, so we only need to look at the transitions where the store we are looking at is at the top of the stack.

- osNew
$$\mathbb{S} \circ (M_j, \mathsf{new}\, x E') \to \mathbb{S} \circ (M_j + x, A E')$$
We have $M_{j+1} - M_j = x$. Since I assume the exact same transition is added to the other sequence I also have $N_{j+1} - N_j = x$. Combined with the inductive hypothesis this gives $M_{j+1} - M_0 = N_{j+1} - N_0$ as wanted.
- osDel
$$\mathbb{S} \circ (M_j, \mathsf{del}\, x E') \to \mathbb{S} \circ (M_j - x, E')$$
This goes like the previous case. We have $M_{j+1} = M_j - x$ and by assuming the same transition in the other sequence we also get $N_{j+1} = N_j - x$. Combining this with the inductive hypothesis gives the result.
- osChoice This transition makes no change to the store, so $N_{j+1} = N_j$ and $M_{j+1} = M_j$ and the wanted result follows from the inductive hypothesis.
- osPush There are two possibilities:
$$\mathbb{S} \circ (M_j, \{A\}E) \to \mathbb{S} \circ (M_j, E) \circ ([], A)$$
or
$$\mathbb{S} \circ (M_j, E_j) \circ \cdots \circ (M, \{A\}E) \to \mathbb{S} \circ (M_j, E_j) \circ \cdots \circ (M, E) \circ ([], A)$$
In both cases $M_{j+1} = M_j$, and since I assume the same transition takes place in the other sequence, $N_{j+1} = N_j$.
- osPop There are two possibilities:
$$\mathbb{S} \circ (M_j, E) \circ (M, \epsilon) \to \mathbb{S} \circ (M_j, E)$$
or
$$\mathbb{S} \circ (M_j, E_j) \circ \cdots \circ (M, E) \circ (M', \epsilon) \to \mathbb{S} \circ (M_j, E_j) \circ \cdots \circ (M, E)$$
In both cases $M_{j+1} = M_j$, and since I assume the same transition takes place in the other sequence, $N_{j+1} = N_j$.

As in the previous chapter, I will prove also a new property of the runs, which looks quite similar to soundness, but is not the same. As before, I will prove it together with sharpness, as a separate case. During this proof though, it will also turn out that we need this property for the "strictly" sharpness properties in the case of SEQ.

Lemma 4.3.2 (Runs change store respecting limits). *If $\Gamma \vdash E : X$ for some E, X and Γ, it is the case that for all $\mathbb{S}$ and M such that $\Gamma \models \mathbb{S}_0 = \mathbb{S} \circ (M, E)$ for all runs of the form $\mathbb{S}_0 \to \cdots \to \mathbb{S}_n$ of E, it is the case that $X^l \subseteq [\mathbb{S}_n] - [\mathbb{S}_0] \subseteq X^o$.*

4.4 Proof of Lemma 4.2.1 and 4.3.2.

Let $\Gamma \models \mathbb{S}$ for some basis Γ and configuration $\mathbb{S}$. The inductive hypothesis is:

For all shorter typing derivations $M, \Gamma' \vdash E : X$, where Γ' is a sub-basis of Γ, for every component x, any unsigned multiset N of resources and for every configuration $\mathbb{S}_0 = \mathbb{S} \circ (M + N, E)$ where $\Gamma \models \mathbb{S}_0$, there exist three generally different runs of E with lengths n_1, n_2 and n_3:

$$\mathbb{S}_0 \to \cdots \to \mathbb{S}_{n_i} = \mathbb{S} \circ (M^i_{n_i} + N, \epsilon) \qquad (i \in \{1, 2, 3\})$$

which fulfill one each of the following properties.

1. *There is a k, $0 \leq k \leq n_1$ such that $[\mathbb{S}_k](x) = X^i(x) + [\mathbb{S}_0](x)$.*
2. $[\mathbb{S}_{n_2}](x) = X^o(x) + [\mathbb{S}_0](x)$.
3. $[\mathbb{S}_{n_3}](x) = X^l(x) + [\mathbb{S}_0](x)$.

And for all runs $\mathbb{S}_0 \to \cdots \to \mathbb{S}_n$ of E, it is the case that $X^l \subseteq [\mathbb{S}_n] - [\mathbb{S}_0] \subseteq X^o$.

Base cases

Axiom

$$\frac{}{[], \oslash \vdash \epsilon : \langle [], [], [] \rangle}$$

We have $M + N = N$.

$$\mathbb{S}_0 = \mathbb{S} \circ (N, E) = \mathbb{S} \circ (N, \epsilon)$$

There is only one degenerate run of ϵ of length 0, where no resources are created or deleted. Let $k = 0$. Since $X^i(x) = X^o(x) = X^l(x) = 0$ this is enough.

Inductive cases

Del Assume $M, \Gamma \vdash E : X$ is inferred by an application of DEL:

$$\frac{M', \Gamma \vdash A : Y \quad y \in \mathsf{dom}(\Gamma)}{[y], \Gamma \vdash \mathsf{del}\, y : \langle [], [-y], [-y] \rangle}$$

We then have $E = \mathsf{del}\, y$ and $M + N = [y] + N$. Starting from a store $[y] + N$, there is only one run of $\mathsf{del}\, y$:

$$\mathbb{S}_0 = \mathbb{S} \circ ([y] + N, \mathsf{del}\, y) \to \mathbb{S} \circ (N, \epsilon) = \mathbb{S}_1$$

This run is actually independent of the type and runs of A, so I will not need the inductive hypothesis in this case.

- For $y \neq x$ we have $([y]+N)(x) = N(x)$ and for the type we have $X^*(x) = 0$ and we can use $k = 0$ or $k = 1$ to attain the maximum for x.
- For $y = x$ we have that for sharpness of $X^i(y) = 0$, obviously $(N+[y])(y) = (N+[y])(y)+X^i(y)$, so take $k = 0$. For sharpness of $X^l(y) = X^o(y) = -1$, we have $(N)(y) = (N + [y])(y) - 1$.

WeakenB Assume $M, \Gamma \vdash E : X$ is inferred by an application of WeakenB:

$$\frac{M, \Gamma' \vdash E : X \quad M', \Gamma' \vdash B : Y \quad x \notin \mathsf{dom}(\Gamma')}{M, \Gamma', x \prec B \vdash E : X}$$

This case is easy — we know already by the inductive hypothesis on the premise $M, \Gamma' \vdash E : X$ that there exist runs of E with the properties needed for sharpness of X.

WeakenS Assume $M, \Gamma \vdash E : X$ is inferred by an application of WeakenS

$$\frac{M', \Gamma \vdash E : X \quad M' \subseteq M}{M, \Gamma \vdash E : X}$$

By the inductive hypothesis we have that for any unsigned multiset N' there are runs with the wanted properties of this form:

$$\mathbb{S} \circ (M' + N', E) \longrightarrow \cdots \longrightarrow \mathbb{S} \circ (M'' + N', \epsilon)$$

Let $M^\delta = M - M'$, which is an unsigned multiset, since $M \supseteq M'$. What I want for the conclusion is runs for any unsigned multiset N of this form

$$\mathbb{S} \circ (M + N, E) \longrightarrow \cdots \longrightarrow \mathbb{S} \circ (M''' + N, \epsilon)$$

But we can get this by letting $N' = M + N - M' = N + M^\delta$. By proposition 4.3.1 the desired property carries over from the run with $(M' + N', E)$ on top to the run with $(M + N, E)$ on top.

New Assume $M, \Gamma \vdash E : X$ is inferred by an application of New:

$$\frac{M, \Gamma' \vdash A : Y \quad y \notin \mathsf{dom}(\Gamma')}{M, \Gamma', y \prec A \vdash \mathsf{new}\, y : X = \langle Y^i + y, Y^o + y, Y^l + y \rangle}$$

We have $E = \mathsf{new}\, y$ and $\Gamma = \Gamma', y \prec A$. By the inductive hypothesis we have for any unsigned multiset N' existence of runs of the form $\mathbb{S} \circ (M + N', A) \to \cdots \to \mathbb{S} \circ (M' + N', \epsilon)$ of A. What we want are the corresponding runs for any unsigned multiset N:

$$\mathbb{S}_0 = \mathbb{S} \circ (M + N, \mathsf{new}\, y) \to \mathbb{S} \circ (M + N + y, A) \to \cdots \to \mathbb{S} \circ (M' + N + y, \epsilon) = \mathbb{S}_n$$

of $\mathsf{new}\, y$. The first step is the rule OSNEW from the operational semantics. The rest of the run exists by inductive hypothesis, the only difference is the addition of one y, but since N' from the inductive hypothesis is any unsigned multiset, it must be okay to also let $N' = N + y$, for fixed N. So I know I can use the runs of A, but now I must show they actually fulfill sharpness.

- For $y \neq x$ we can use the runs of A which exist by the inductive hypothesis for the properties of Y and that $Y^*(x) = X^*(x)$.
- For $y = x$: by valid typing $y \notin \mathsf{dom}(\Gamma - \{y \prec A\})$ and by lemma 2.3.9, valid typing judgement, in [13] $Y^* \subseteq \mathsf{dom}(\Gamma - \{y \prec A\})$, so $Y^*(y) = 0$ and there is no y created in the run of A. The extra y is added to the store in the first step of the run, and this will be the only y during the run of A. I choose $k = 1$, and $[\mathbb{S}_1](y) = [\mathbb{S}_0](y) + 1$ while $X^i(y) = Y^i(y) + 1 = 1$. We also have $X^o(y) = Y^o(y) + 1 = 1$ and $[\mathbb{S}_n](y) = [\mathbb{S}_0](y) + 1$ and the corresponding holds for $X^l(x)$. So all properties hold for any run of $\mathsf{new}\, y$.

Finally I must prove that for any run $\mathbb{S}_0 \to \cdots \to \mathbb{S}_n$ of $\mathsf{new}x$ we have $X^l \subseteq [\mathbb{S}_n] - [\mathbb{S}_0] \subseteq X^o$. From the inductive hypothesis we have $Y^l \subseteq [\mathbb{S}_n] - [\mathbb{S}_1] \subseteq Y^o$. Add one $[y]$ to every part of the inequality to get

$$\begin{aligned} Y^l + [y] \subseteq [\mathbb{S}_n] - [\mathbb{S}_1] + [y] \subseteq Y^o(x) + [y] \\ Y^l + [y] \subseteq [\mathbb{S}_n] - [\mathbb{S}_1] + [\mathbb{S}_1] - [\mathbb{S}_0] \subseteq Y^o + [y] \\ X^l \subseteq [\mathbb{S}_n] - [\mathbb{S}_0] \subseteq X^o \end{aligned}$$

Seq Assume $M, \Gamma \vdash E : X$ is inferred by an application of SEQ:

$$\frac{M_1, \Gamma \vdash A : Y \qquad M_2, \Gamma \vdash B : Z \quad A, B \neq \epsilon}{M_1 \cup (M_2 - Y^l), \Gamma \vdash AB : X = \langle Y^i \cup (Y^o + Z^i), Y^o + Z^o, Y^l + Z^l \rangle}$$

A run of $A\,B$ consists of a run of A followed by a run of B. By the inductive hypothesis we have knowledge of runs of A starting with store $M_1 + N_1$:

$$\mathbb{S} \circ (M_1 + N_1, A) \to \cdots \to \mathbb{S} \circ (M_1' + N_1, \epsilon)$$

What I want is runs for any N starting with $M + N$. We have $M = M_1 \cup (M_2 - Y^l)$, so we have $M + N \supseteq M \supseteq M_1$. I can therefore get the wanted runs of A starting with $M + N$ by letting $N_1 = M + N - M_1$. The subtraction $M - M_1$ still creates an unsigned multiset since $M_1 \subseteq M$ by assumption. So I get runs of this form:

$$\mathbb{S} \circ (M + N, A) \to \cdots \to \mathbb{S} \circ (M' + N, \epsilon)$$

where we from (4.3.1) have $M' = M + M_1' - M_1$. So I get $M_1' + N_1 = M_1' + M + N - M_1 = M' + N$, as needed.

Adding B to the expression gives a sequence of configurations from $\mathbb{S} \circ (M + N, AB)$ to $\mathbb{S} \circ (M' + N, B)$ using the same transitions. In other words, for any run of length n

$$\mathbb{S} \circ (M + N, A) \to \cdots \to \mathbb{S} \circ (M' + N, \epsilon)$$

there is a sequence of $n + 1$ configurations

$$\mathbb{S} \circ (M + N, AB) \to \cdots \to \mathbb{S} \circ (M' + N, B)$$

with the same transitions. Now we go on to the runs of B. First I will look at the store $M' + N$ at the end of a run of A.

$$\begin{array}{rcll}(M'+N)(x) & \geq & (M+N)(x) + Y^l(x) & \\ & \geq & (M_1 \cup (M_2 - Y^l))(x) + Y^l(x) & \\ & = & \mathsf{max}(M_1(x), (M_2 - Y^l)(x)) + Y_l(x) & (4.1) \\ & \geq & (M_2 - Y^l)(x) + Y_l(x) & \\ & = & M_2(x) & \end{array}$$

The first line follows from the last clause of the induction hypothesis ($M' - M \supseteq X^l$). The second line follows from the typing derivation ($M = M_1 \cup (M_2 - Y^l)$). So we have $M' + N \supseteq M_2$ for any such sequence of configurations. By the inductive hypothesis we have runs starting with a store $M_2 + N_2$. Letting $N_2 = M' + N - M_2$ we then get runs starting with $M' + N = M_2 + N_2$:

$$\mathbb{S} \circ (M' + N, B) \to \cdots \to \mathbb{S} \circ (M'' + N, \epsilon)$$

Where $M'' - M = M_2' - M_2$. For correctness of the last store, remember from (4.3.1) that $M'' - M' = M_2' - M_2$ so I get:

$$M_2' + N_2 = M_2' + (M' + N - M_2) = (M' + M_2' - M_2) + N = M'' + N$$

For the runs of B I need no transformation as in the case of A, and can directly use the runs existing by the inductive hypothesis. So for any pair of a run of A and a run of B, there is a run

$$\mathbb{S}_0 = \mathbb{S} \circ (M+N, AB) \to \cdots \to \mathbb{S} \circ (M'+N, B) = \mathbb{S}_n \to \cdots \to \mathbb{S} \circ (M''+N, \epsilon) = \mathbb{S}_{n+m}$$

of $A\,B$, using the same transitions. If the run of A is of length n and the run of B is of length m, the run of $A\,B$ will be of length $n + m$.

I will now start with finding a run resulting in $[\mathbb{S}_{n+m}](x) = [\mathbb{S}_0](x) + X^o(x) = [\mathbb{S}_0](x) + Y^o(x) + Z^o(x)$. First I choose the run of A resulting in $[\mathbb{S}_n](x) = [\mathbb{S}_0](x) + Y^o(x)$. I can then choose the run of B finally resulting in:

$$[\mathbb{S}_{n+m}](x) = [\mathbb{S}_n](x) + Z^o(x) = [\mathbb{S}_0](x) + Y^o(x) + Z^o(x) = [\mathbb{S}_0](x) + X^o(x)$$

and we are done with this first part. For $X^l(x)$, we can use the same argument, just replacing ^{o} with ^{l}.

Finding a run of $A\,B$: $\mathbb{S}_0 \to \cdots \to \mathbb{S} \circ (M' + N, B) \to \cdots \to \mathbb{S}_{n'+m'}$, where there is k, such that $1 \leq k \leq n' + m'$ and

$$\begin{array}{rcl}[\mathbb{S}_k](x) & = & [\mathbb{S}_0](x) + X^i(x) \\ & = & [\mathbb{S}_0](x) + (Y^i \cup (Y^o + Z^i))(x) \\ & = & [\mathbb{S}_0](x) + \mathsf{max}(Y^i(x), Y^o(x) + Z^i(x))\end{array}$$

is not that easy. The k with the maximum store could be found both during execution of A (e.g. $k \leq n'$) or k during execution of B (e.g. $k > m'$).

To prove that there will always be such a run and k, I must make a case distinction on the value of $X^i(x) = \mathsf{max}(Y^i(x), Y^o(x) + Z^i(x))$:

- If $Y^i(x) = \mathsf{max}(Y^i(x), Y^o(x) + Z^i(x))$ we can use the run of A which by the inductive hypothesis has a configuration $\mathbb{S}_{k_A}$ such that $[\mathbb{S}_{k_A}](x) = [\mathbb{S}_0](x) + Y^i(x) = [\mathbb{S}_0](x) + X^i(x)$, so I can use k_A as k.

- In the other case, $Y^o(x) + Z^i(x) = \mathsf{max}(Y^i(x), Y^o(x) + Z^i(x))$, we use the run of A which ends in $\mathbb{S}_n = \mathbb{S} \circ (M' + N, B)$ where $[\mathbb{S}_n](x) = [\mathbb{S}_0](x) + Y^o(x)$. By equation 4.1 above we have $M' + N \supseteq M_2$. I can then choose the run of B where there is a k_B such that

  $$[\mathbb{S}_{k_B}](x) = [\mathbb{S}_n](x) + Z^i(x) = [\mathbb{S}_0](x) + Y^o(x) + Z^i(x) = [\mathbb{S}_0](x) + X^i(x)$$

  and use $n' + k_B$ as k.

For the last property, given any run

$$\mathbb{S}_0 = \mathbb{S} \circ (M, AB) \to \cdots \to \mathbb{S}_n = \mathbb{S} \circ (M', B) \to \cdots \to \mathbb{S}_{n+m} = \mathbb{S} \circ (M'', \epsilon)$$

of AB, we have

$$Y^l \subseteq [\mathbb{S}_n] - [\mathbb{S}_0] \subseteq Y^o$$
$$Z^l \subseteq [\mathbb{S}_{n+m}] - [\mathbb{S}_n] \subseteq Z^o$$

by the inductive hypothesis. Adding these two inequalities we get:

$$Y^l + Z^l \subseteq [\mathbb{S}_n] - [\mathbb{S}_0] + [\mathbb{S}_{n+m}] - [\mathbb{S}_n] \subseteq Y^o + Z^o$$

which implies $X^l \subseteq [\mathbb{S}_{n+m}] - [\mathbb{S}_0] \subseteq X^o$.

Choice Assume $M, \Gamma \vdash E : X$ is inferred by an application of CHOICE:

$$\frac{M_1, \Gamma \vdash A : Y \quad M_2, \Gamma \vdash B : Z}{M_1 \cup M_2, \Gamma \vdash (A + B) : X = \langle Y^i \cup Z^i, Y^o \cup Z^o, Y^l \cap Z^l \rangle}$$

We then have $E = (A+B)$ and $M = M_1 \cup M_2$. To run $(A+B)$, we must choose a run of A or a run of B. For any run of A or B, e.g. $\mathbb{S} \circ (M_1 + N_1, A) \to \cdots \to \mathbb{S} \circ (M_1' + N_1, \epsilon)$, there is a corresponding run of $(A + B)$, with the same transitions, only with one instance of OSCHOICE added in front, e.g.:

$$\mathbb{S} \circ (M + N, (A + B)) \to \mathbb{S} \circ (M + N, A) \to \cdots \to \mathbb{S} \circ (M' + N, \epsilon)$$

This run exists because we can let $N_1 = M+N-M_1$. This is a valid subtraction since $M \supseteq M_1$. Since $M' - M = M_1' - M_1$ from (4.3.1), for the last store I get

$$M_1' + N_1 = M_1' + (M + N - M_1) = (M + M_1' - M_1) + N = M' + N$$

By the inductive hypothesis there is then a run of A and a state k_A in the run such that $[\mathbb{S}_{k_A}](x) = [\mathbb{S}_0](x) + Y^i(x)$, and correspondingly for B there is a run and a k_B. For a run of $(A + B)$ with a state k achieving $[\mathbb{S}_k](x) = [\mathbb{S}_0](x) + X^i(x) = [\mathbb{S}_0](x) + (Y^i \cup Z^i)(x) = [\mathbb{S}_0](x) + \mathsf{max}(Y^i(x), Z^i(x))$, choose the run of A and $k = k_A$ if $Y^i(x) > Z^i(x)$, otherwise choose the run of B and $k = k_B$. We will then have

$$[\mathbb{S}_k](x) = [\mathbb{S}_0](x) + \mathsf{max}(Y^i(x), Z^i(x)) = [\mathbb{S}_0](x) + X^i(x)$$

Correspondingly, almost equal arguments can be used for $[\mathbb{S}_0](x) + X^o(x)$ and $[\mathbb{S}_0](x) + X^l(x)$.

For the last property, given any run

$$\mathbb{S}_0 = \mathbb{S} \circ (M, (A + B)) \to \cdots \to \mathbb{S}_n = \mathbb{S} \circ (M', \epsilon)$$

of AB, we have

$$\begin{array}{c} Y^l \cap Z^l \subseteq [\mathbb{S}_n] - [\mathbb{S}_1] \subseteq Y^o \cup Z^o \\ \Downarrow \\ X^l \subseteq [\mathbb{S}_m] - [\mathbb{S}_0] \subseteq X^o \end{array}$$

by the inductive hypothesis, the properties of intersection and union and that the first transition does not change the store.

Scope Assume $M, \Gamma \vdash E : X$ is inferred by an application of SCOPE:

$$\frac{[], \Gamma \vdash A : Y}{[], \Gamma \vdash \{A\} : \langle Y^i, [], [] \rangle}$$

We have $E = \{A\}$ and $M + N = [] + N = N$. In the operational semantics, a new pair $([], A)$ is created on top of the stack through the transition rule OSPUSH, A is run, and then OSPOP removes the pair again. So, for any run

$$\mathbb{S} \circ ([], A) \to \cdots \to \mathbb{S} \circ (M', \epsilon)$$

of A there is a run

$$\begin{array}{ll} \mathbb{S} \circ (N, \{A\}) & \mathbb{S}_0 \\ \to \mathbb{S} \circ (N, \epsilon) \circ ([], A) & \mathbb{S}_1 \\ \to \cdots \to \mathbb{S} \circ (N, \epsilon) \circ (M', \epsilon) & \mathbb{S}_{n-1} \\ \to \mathbb{S} \circ (N, \epsilon) & \mathbb{S}_n \end{array}$$

of $\{A\}$ using the same transitions but in addition having OSPUSH and OSPOP at the start and the end. In all but the first and last transitions, we are guaranteed that N is not used or changed by the properties of scope. In the first and last rules, this follows from the operational semantics. I can assume existence of the wanted runs of A, since $[], \Gamma \vdash A : Y$ must hold by the typing rule. For X^o and X^l any run of A is okay, since no resources are returned ($[\mathbb{S}_n](x) = [\mathbb{S}_0](x)$) and $X^o = X^l = []$. For the other property, choose the run and k_A such that

$$[\mathbb{S}_{k_A}](x) = ([\mathbb{S}] + M)(x) + Y^i(x) = [\mathbb{S}](x) + M(x) + Y^i(x) = [\mathbb{S}_0](x) + Y^i(x) = X^i + [\mathbb{S}_0](x)$$

which exist by the inductive hypothesis. So we can let $k = k_A$.

The last property is easy, as for all runs $X^l = X^o = []$ and the store is not changed.

Chapter 5

Sharpness of the system with choice, scope, del and parallel composition ("Explicit deallocation and Parallel Composition") in chapter 4 of [13]

This chapter is a proof of the "sharpness" of the system defined in Chapter 4 in [13]. Some important definitions of this system follow:

5.1 Definitions

Definition 5.1.1 (Language).

$$
\begin{array}{rcl}
Prog & \rightarrow & \overline{Decls}; E \\
Decls & \rightarrow & \overline{x \prec E}; \\
E & \rightarrow & \\
 & & \epsilon \\
 & | & \mathsf{new}x \\
 & | & \mathsf{del}x \\
 & | & EE \\
 & | & (E + E) \\
 & | & (E||E) \\
 & | & \{E\}
\end{array}
$$

A configuration in this system is a tree of stacks, where the stacks are as in the previous chapter.

A configuration is

$\mathbb{T},\mathbb{R}$			Configurations
	$\rightarrow$	$\mathsf{Lf}(\mathbb{S})$	Leaf
	$\mid$	$\mathsf{Nd}(\mathbb{S},\mathbb{T})$	Node with one branch
	$\mid$	$\mathsf{Nd}(\mathbb{S},\mathbb{T},\mathbb{T})$	Node with two branches

Definition 5.1.2 (Operational Semantics).

$$(\mathsf{osNew}) \quad x \prec A \in Decls$$
$$\mathsf{Lf}(\mathbb{S} \circ (M, \mathsf{new}xE)) \longrightarrow \mathsf{Lf}(\mathbb{S} \circ (M + x, AE))$$

$$(\mathsf{osDel}) \quad x \in M$$
$$\mathsf{Lf}(\mathbb{S} \circ (M, \mathsf{del}xE)) \longrightarrow \mathsf{Lf}(\mathbb{S} \circ (M - x, E))$$

$$(\mathsf{osChoice}) \quad i \in \{1,2\}$$
$$\mathsf{Lf}(\mathbb{S} \circ (M, (A_1 + A_2)E)) \longrightarrow \mathsf{Lf}(\mathbb{S} \circ (M, A_i E))$$

$$(\mathsf{osPush})$$
$$\mathsf{Lf}(\mathbb{S} \circ (M, \{A\}E)) \longrightarrow \mathsf{Lf}(\mathbb{S} \circ (M, E) \circ ([], A))$$

$$(\mathsf{osPop})$$
$$\mathsf{Lf}(\mathbb{S} \circ (M, E) \circ (M', \epsilon)) \longrightarrow \mathsf{Lf}(\mathbb{S} \circ (M, E))$$

$$(\mathsf{osParIntr})$$
$$\mathsf{Lf}(\mathbb{S} \circ (M, (A \,||\, B)E)) \longrightarrow \mathsf{Nd}(\mathbb{S} \circ (M, E), \mathsf{Lf}([], A), \mathsf{Lf}([], B))$$

$$(\mathsf{osParElimL})$$
$$\mathsf{Nd}(\mathbb{S} \circ (M, E), \mathsf{Lf}(M', \epsilon), \mathbb{R}) \longrightarrow \mathsf{Nd}(\mathbb{S} \circ (M + M', E), \mathbb{R})$$

$$(\mathsf{osParElimR})$$
$$\mathsf{Nd}(\mathbb{S} \circ (M, E), \mathbb{R}, \mathsf{Lf}(M', \epsilon)) \longrightarrow \mathsf{Nd}(\mathbb{S} \circ (M + M', E), \mathbb{R})$$

$$(\mathsf{osParElim})$$
$$\mathsf{Nd}(\mathbb{S} \circ (M, E), \mathsf{Lf}(M', \epsilon)) \longrightarrow \mathsf{Lf}(\mathbb{S} \circ (M + M', E))$$

Types are triples $X = \langle X^i, X^o, X^l \rangle$, where X^i is an unsigned multiset and the two others are signed multisets. X^i represents the maximum positive increase in the number of simultaneously active instances during the run of the expression, while X^o and X^l are the upper and lower bounds for the number of instances active after execution. These properties are formalised in the sharpness lemma below.

A typing judgement is of the form $M, \Gamma \vdash E : X$. Γ is a basis, E an expression and X a type. M corresponds to the part X^n of the type in "global resources" (Section 2.3, page 11).

$$(\textsc{Del}) \quad \frac{\sigma, \Gamma \vdash A : X \qquad x \in \mathsf{dom}(\Gamma)}{[x], \Gamma \vdash \mathsf{del}\, x : \langle [], [-x], [-x] \rangle}$$

$$(\textsc{WeakenB}) \quad \frac{\sigma_1, \Gamma \vdash A : X \qquad \sigma_2, \Gamma \vdash B : Y \quad x \notin \mathsf{dom}(\Gamma)}{\sigma_1, \Gamma, x \prec B \vdash A : X}$$

$$\text{(WeakenS)}\ \frac{\sigma, \Gamma \vdash A : X \qquad \sigma \subseteq \sigma_1}{\sigma_1, \Gamma \vdash A : X} \qquad \text{(New)}\ \frac{\sigma, \Gamma \vdash A : X \quad x \notin \mathsf{dom}(\Gamma)}{\sigma, \Gamma, x \prec A \vdash \mathsf{new}\, x : \langle X^i + x, X^o + x, X^l + x\rangle}$$

$$\text{(Scope)}\ \frac{[], \Gamma \vdash A : X}{[], \Gamma \vdash \{A\} : \langle X^i, [], []\rangle} \qquad \text{(Parallel)}\ \frac{[], \Gamma \vdash A : X \qquad [], \Gamma \vdash B : Y}{[], \Gamma \vdash (A \,||\, B) : \langle X^i + Y^i, X^o + Y^o, X^l + Y^l\rangle}$$

$$\text{(Axiom)}\ \frac{}{[], \oslash \vdash \epsilon : \langle [], [], []\rangle} \qquad \text{(Choice)}\ \frac{\sigma_1, \Gamma \vdash A : X \qquad \sigma_2, \Gamma \vdash B : Y}{\sigma_1 \cup \sigma_2, \Gamma \vdash (A \,+\, B) : \langle X^i \cup Y^i, X^o \cup Y^o, X^l \cap Y^l\rangle}$$

$$\text{(Seq)}\ \frac{\sigma_1, \Gamma \vdash A : X \qquad \sigma_2, \Gamma \vdash B : Y \quad A, B \neq \epsilon}{\sigma_1 \cup (\sigma_2 - X^l), \Gamma \vdash AB : \langle X^i \cup (X^o + Y^i), X^o + Y^o, X^l + Y^l\rangle}$$

Definition 5.1.3.

$$\mathsf{retl}_{\mathbb{T}}(\alpha.k) = \begin{cases} [], \text{ if } k < \mathsf{hi}(\mathbb{T}(\alpha)) \text{ or } \alpha \in \mathsf{leaves}(\mathbb{T}) \\ \biguplus_{\beta \in \{\alpha l, \alpha r\}} (M + X^l + \mathsf{retl}_{\mathbb{T}}(\beta.1)), \text{otherwise} \end{cases}$$

Definition 5.1.4 (Well-typed configurations). *Configuration $\mathbb{T}$ is well-typed with respect to a basis Γ, notation $\Gamma \models \mathbb{T}$, if for each pair (M, E) at position $\alpha.k \in \mathbb{T}$ there exists X such that*

$$M + \mathsf{retl}_{\mathbb{T}}(\alpha.k), \Gamma \vdash E : X$$

In this system, as in the previous, we have the rule WeakenS which destroys sharpness of M.

5.2 Sharpness

Lemma 5.2.1 (Sharpness). *If $M, \Gamma \vdash E : X$ then, for every component x, for every well-typed configuration $\mathbb{T}_0 = \mathbb{T}[\mathsf{Lf}(\mathbb{S} \circ (M, E))]_\alpha$ there exist three generally different runs of E with lengths n_1, n_2 and n_3:*

$$\mathbb{T}_0 \to \cdots \to \mathbb{T}^i_{n_i} = \mathbb{T}[\mathsf{Lf}(\mathbb{S} \circ (M^i_{n_i}, \epsilon))]_\alpha \qquad (i \in \{1, 2, 3\})$$

which fulfill one each of the following properties:

1. *There is a k, $0 \leq k \leq n_1$ such that $[\mathbb{T}_k](x) = X^i(x) + [\mathbb{T}_0](x)$.*
2. *$[\mathbb{T}^2_{n_2}](x) = X^o(x) + [\mathbb{T}_0](x)$.*
3. *$[\mathbb{T}^3_{n_3}](x) = X^l(x) + [\mathbb{T}_0](x)$.*

Corollary 5.2.2 (Sharpness of programs). *For any program $Prog = Decls; E$ s.t. $[], \Gamma \vdash E : X$ for some reordering Γ of Decls, for every component x, there exist three generally different runs with lengths n_1, n_2 and n_3:*

$$\mathsf{Lf}([], Prog) = \mathbb{T}_0 \to \cdots \to \mathbb{T}^i_{n_i} = \mathsf{Lf}(M^i_{n_i}, \epsilon) \qquad (i \in \{1, 2, 3\})$$

which fulfill one each of the following properties:

1. *there is a k, $0 \leq k \leq n_1$ such that $[\mathbb{T}_k](x) = X^i(x)$.*
2. *$M^2_{n_2}(x) = X^o(x)$.*
3. *$M^3_{n_3}(x) = X^l(x)$.*

5.3 Run of an expression

Definition 5.3.1 (Run of an expression). *A run of an expression E on position α in context $\mathbb{T}$ is a sequence of configurations, where*

- *E is the expression in the top of the stack at one of the leaves in the first configuration in the sequence, that is,*

  $$\mathbb{T}_0 = \mathbb{T}[\mathsf{Lf}(\mathbb{S} \circ (M, E))]_\alpha$$

  for some $\mathbb{S}$ and M. We also have $\Gamma \models \mathbb{T}_0$ for some Γ.

- *In any pair of two consecutive configurations the second is formed from the first using one of the rules in the operational semantics.*

- *Only transitions of the forms*

  $$\mathbb{T}[\mathsf{Lf}(\mathbb{S} \circ \cdots \circ (M'', E''))]_\alpha \to \mathbb{T}[\mathsf{Lf}(\mathbb{S}'')]_\alpha$$

  and

  $$\mathbb{T}[\mathsf{Lf}(\mathbb{S}' \circ (M'', E''))]_{\alpha\beta} \to \mathbb{T}[\mathbb{R}']_{\alpha\beta}$$

  are allowed, that is, only transitions on α or any positions below it, or on the same or higher position in the stack at α.

- *The last configuration is of the form:*

  $$\mathbb{T}[\mathsf{Lf}(\mathbb{S} \circ (M', \epsilon))]_\alpha$$

  that is, position α is a leaf, the stack in this leaf $\mathbb{T}(\alpha)$ is the same as in the start configuration, and the expression at the top of the stack is empty (ϵ).

- *The length of the run is the number of configurations minus one.*

I will enumerate the configurations in a run from 0 to length: $\mathbb{T}_0 \to \cdots \to \mathbb{T}_{\mathsf{length}}$.

Proposition 5.3.2 (Change of store independent of size of store). *For any two sequences of configurations of the same length j*

$$\mathbb{T}_0 = \mathbb{T}[\mathsf{Lf}(\mathbb{S} \circ (M_0, E_0))]_\alpha \longrightarrow \cdots \longrightarrow \mathbb{T}_j = \mathbb{T}[\mathsf{Lf}(\mathbb{S} \circ (M_j, E_j))]_\alpha$$

and

$$\mathbb{T}'_0 = \mathbb{T}'[\mathsf{Lf}(\mathbb{S}' \circ (N_0, E'_0))]_\alpha \longrightarrow \cdots \longrightarrow \mathbb{T}'_j = \mathbb{T}'[\mathsf{Lf}(\mathbb{S} \circ (N_j, E'_j))]_\alpha$$

where for all i, $0 \leq i < j$ the rule used for the transformation $\mathbb{T}_i \longrightarrow \mathbb{T}_{i+1}$ and the subexpression to which the rule is applied are identical to the one used for the transformation $\mathbb{T}'_i \longrightarrow \mathbb{T}'_{i+1}$, we have that

$$M_j - M_0 = N_j - N_0$$

I will not write out the proof of this lemma. It is easy to change the proof of lemma 4.3.1 into a proof of this lemma.

At last, the following property will also here be proved together with sharpness.

Lemma 5.3.1 (Runs change store respecting limits). *If $\Gamma \vdash E : X$ for some E, X and Γ, it is the case that for all $\mathbb{T}$, $\mathbb{S}$ and M such that $\Gamma \models \mathbb{T}_0 = \mathbb{T}[\mathsf{Lf}(\mathbb{S} \circ (M, E))]_\alpha$ for all runs of the form $\mathbb{T}_0 \to \cdots \to \mathbb{T}_n$ of E, it is the case that $X^l \subseteq [\mathbb{T}_n] - [\mathbb{T}_0] \subseteq X^o$.*

5.4 Proof of sharpness (Lemma 5.2.1).

Let $\Gamma \models \mathbb{T}$ for some basis Γ and configuration $\mathbb{T}$. The inductive hypothesis is: *for all shorter typing derivations $M, \Gamma' \vdash E : X$, where Γ' is a sub-basis of Γ, for every component x, every unsigned multiset N and every configuration of the form $\mathbb{T}_0 = \mathbb{T}[\mathsf{Lf}(\mathbb{S} \circ (M + N, E))]_\alpha$ where $\Gamma \models \mathbb{T}_0$, there exist three generally different runs of E with lengths n_1, n_2 and n_3:*

$$\mathbb{T}_0 \to \cdots \to \mathbb{T}^i_{n_i} = \mathbb{T}[\mathsf{Lf}(\mathbb{S} \circ (M^i_{n_i} + N, \epsilon))]_\alpha \qquad (i \in \{1, 2, 3\})$$

which fulfill one each of the following properties:

1. there is a $k, 0 \leq k \leq n$, such that $[\mathbb{T}_k](x) = X^i(x) + [\mathbb{T}_0](x)$.
2. $[\mathbb{T}^2_{n_2}](x) = X^o(x) + [\mathbb{T}_0](x)$.
3. $[\mathbb{T}^3_{n_3}](x) = X^l(x) + [\mathbb{T}_0](x)$.

And for all runs $\mathbb{T}_0 \to \cdots \to \mathbb{T}_n$ of E, it is the case that $X^l \subseteq [\mathbb{T}_n] - [\mathbb{T}_0] \subseteq X^o$.

All cases from the proof of sharpness in the previous chapter (page 70) can be used with small modifications in this proof, so I will not repeat them here.

But I must show the case for Parallel:

Parallel. Assume $M, \Gamma \vdash E : X$ is inferred by an application of Parallel:

$$\frac{[], \Gamma \vdash A : Y \quad [], \Gamma \vdash B : Z}{[], \Gamma \vdash (A||B) : Y + Z}$$

Then we have $E = (A||B)$, $X = Y + Z$ and $M + N = N$. From assumptions I have $\Gamma \models_{\mathcal{R}} \mathbb{T}[\mathsf{Lf}(N, (A||B) \cdot E')]_\alpha$ for some E'. From the inductive hypothesis I have knowledge of runs of A and B of these forms:

$$\mathbb{T}[\mathsf{Lf}([], A)]_{\alpha'} \to \cdots \to \mathbb{T}[\mathsf{Lf}(M_j, \epsilon)]_{\alpha'} \tag{5.1}$$
$$\mathbb{T}[\mathsf{Lf}([], B)]_{\alpha''} \to \cdots \to \mathbb{T}[\mathsf{Lf}(M'_h, \epsilon)]_{\alpha''} \tag{5.2}$$

for some α' and α''. Note that we can have $\alpha' = \bullet$ or $\alpha'' = \bullet$. For any of these runs, there exist runs of the following forms:

$$\mathbb{T}[\mathsf{Nd}(N, E', \mathsf{Lf}([], A), \mathbb{R})]_\alpha \to \cdots \to \mathbb{T}[\mathsf{Nd}(N, E', \mathsf{Lf}(M_j, \epsilon), \mathbb{R})]_\alpha \tag{5.3}$$
$$\mathbb{T}[\mathsf{Nd}(N', E', \mathbb{R}, \mathsf{Lf}([], B))]_\alpha \to \cdots \to \mathbb{T}[\mathsf{Nd}(N', E', \mathbb{R}, \mathsf{Lf}(M'_h, \epsilon))]_\alpha) \tag{5.4}$$

If the run of A is of length j and the run of B is of length h, then the length of a run of $(A||B)$ is of length $j + h + 3$, since all transitions in both runs must be done, in addition there will be one osParIntr at the start of the run, one of either osParElimL or osParElimR some time during the run, and finally, at the end an instance of osParElim - in sum, three extra transitions. If the run was first exclusively transitions from the run of A and then from the run of B, it could look like this:

$$\begin{aligned}
&\mathbb{T}[\mathsf{Lf}(N, (A||B) \cdot E')]_\alpha \to \mathbb{T}[\mathsf{Nd}(N, E', \mathsf{Lf}([], A), \mathsf{Lf}([], B))]_\alpha \to \\
&\cdots \to \mathbb{T}[\mathsf{Nd}(N, E', \mathsf{Lf}(M_j, \epsilon), \mathsf{Lf}(B))]_\alpha \\
&\to \mathbb{T}[\mathsf{Nd}(N + M_j, E', \mathsf{Lf}([], B))]_\alpha \to \\
&\cdots \to \mathbb{T}[\mathsf{Nd}(N + M_j, E', \mathsf{Lf}(M'_h, \epsilon))]_\alpha \to \mathbb{T}[\mathsf{Lf}(N + M_j + M'_h, E')]_\alpha)
\end{aligned} \tag{5.5}$$

This need not be the case - the transitions from the run of A could come in between transitions from the run of B.

I will now treat the three sharpness properties separately:

- $X^i(x)$. I must now create a run of $(A||B)$ of some length n, where there is a k such that $0 \leq k \leq n$ and $[\mathbb{T}_k](x) = [\mathbb{T}_0](x) + X^i(x) = [\mathbb{T}_0](x) + Y^i(x) + Z^i(x)$. First, choose the run of A where there is a k_A such that $[\mathbb{T}_{k_A}](x) = [\mathbb{T}_0](x) + Y^i(x)$. Stop the run at exactly this state:

$$\mathbb{T}[\mathsf{Nd}(N, E', \mathsf{Lf}([], A), \mathsf{Lf}([], B))]_\alpha \to \cdots \to \mathbb{T}[\mathsf{Nd}(N, E', \mathbb{R}_k, \mathsf{Lf}([], B))]_\alpha)$$

  where $[\mathbb{R}_k](x) = Y^i(x)$. This I can assume, because all the transitions are from the run of A on $\mathsf{Lf}([], A)$. Now, equivalently, choose the run of B starting at this state (which I can do because of soundness), where there is a k_B such that $[\mathbb{T}_{k_A+k_B}](x) = [\mathbb{T}_{k_A}](x) + Z^p(x)$. Stop the run at exactly this state:

$$\mathbb{T}[\mathsf{Nd}(N, E', \mathbb{R}_k, \mathsf{Lf}(B))]_\alpha \to \cdots \to \mathbb{T}[\mathsf{Nd}(E', \mathbb{R}_{k_A}, \mathbb{R}'_{k_B})]_\alpha)$$

  where $[\mathbb{R}'_{k_B}](x) = Z^i(x)$ since all the transitions are from a run of B starting in $\mathsf{Lf}([], B)$. Let $k = k_A + k_B$, and we get $[\mathbb{T}_k](x) = [\mathbb{T}_{k_A}](x) + Z^p(x) = [\mathbb{T}_0](x) + Y^n(x) + Z^n(x) = [\mathbb{T}_0](x) + X^p(x)$. For the rest of the run do the remaining transitions in the runs of A and B, which by soundness are all possible.

- $X^l(x)$ and $X^o(x)$. I will try to convince you that sharpness of $X^l(x)$ and $X^o(x)$ consists only of using the runs of A and B with the same properties using the following argument. Let $* \in \{l, o\}$: In the illustration of the run (5.5) assume $M_j(x) = X^*(x)$ and $M'_h(x) = Y^*(x)$, both which we can assume from the inductive hypothesis. Now we have that the total store at the end is:

$$[\mathbb{T}_n](x) = [\mathbb{T}_0](x) + Y^*(x) + Z^*(x) = [\mathbb{T}_0](x) + X^*(x)$$

- $X^l \subseteq [\mathbb{T}_n] - [\mathbb{T}_0] \subseteq X^o$. Looking again at the illustration of a run in (5.5) I have from the inductive hypothesis that

$$Y^l \subseteq M_j \subseteq Y^o$$
$$Z^l \subseteq M'_h \subseteq Z^o$$

  This implies by the properties of addition of multisets that:

$$X^l = Y^l + Z^l \subseteq M_j + M'_h \subseteq Y^o + Z^o = X^o$$

□

Chapter 6

Sharpness of the system with choice, scope and reu ("Reuse instantiation") in chapter 5 of [13]

This chapter is a proof of the "sharpness" of the system defined in Chapter 5 in [13]. Some important definitions of this system follows:

6.1 Definitions

Definition 6.1.1 (Language).

$$\begin{array}{rcl} Prog & \rightarrow & \overline{Decls}; E \\ Decls & \rightarrow & \overline{x \prec E}; \\ E & \rightarrow & \\ & & \epsilon \\ & | & \mathsf{new}x \\ & | & \mathsf{reu}x \\ & | & EE \\ & | & (E + E) \\ & | & \{E\} \end{array}$$

A configuration in this system is a stack of pairs like in the simple system in chapter 3.

Definition 6.1.2 (Operational Semantics).

$$\begin{array}{l} (\mathsf{osNew}) \quad x \prec A \in Decls \\ \mathbb{S} \circ (M, \mathsf{new}xE) \longrightarrow \mathbb{S} \circ (M + x, AE) \end{array}$$

$$\begin{array}{l} (\mathsf{osReu1}) \quad x \prec A \in Decls \quad x \notin [\mathbb{S}] + M \\ \mathbb{S} \circ (M, \mathsf{reu}xE) \longrightarrow \mathbb{S} \circ (M + x, AE) \end{array}$$

$$\begin{array}{l} (\mathsf{osReu2}) \quad x \prec A \in Decls \quad x \in [\mathbb{S}] + M \\ \mathbb{S} \circ (M, \mathsf{reu}xE) \longrightarrow \mathbb{S} \circ (M, AE) \end{array}$$

(osChoice) $\quad i \in \{1,2\}$
$\mathbb{S} \circ (M, (A_1 + A_2)E) \longrightarrow \mathbb{S} \circ (M, A_i E)$

(osPush)
$\mathbb{S} \circ (M, \{A\}E) \longrightarrow \mathbb{S} \circ (M, E) \circ ([], A)$

(osPop)
$\mathbb{S} \circ (M, E) \circ (M', \epsilon) \longrightarrow \mathbb{S} \circ (M, E)$

A typing judgement is of the form $\Gamma \vdash_{\mathcal{R}} E : X$ where $\mathcal{R}$ is a restriction. Types are tuples $X = \langle X^i, X^o, X^j, X^p \rangle$, of unsigned multisets. X^i and X^o are the same as in chapter 3. X^j and X^p represent the same bounds as X^i and X^o respectively, but with respect to executing the expression in a state where every component already has at least one reusable instance. These properties are formalised in the sharpness lemma below.

(Reu)
$$\frac{\Gamma \vdash A : X \quad x \notin \mathsf{dom}(\Gamma)}{\Gamma, x \prec A \vdash \mathsf{reu}\, x : \langle X^i + x, X^o + x, X^j, X^p \rangle}$$

(WeakenB)
$$\frac{\Gamma \vdash A : X \qquad \Gamma \vdash B : Y \quad x \notin \mathsf{dom}(\Gamma)}{\Gamma, x \prec B \vdash A : X}$$

(Axiom)
$$\frac{}{\oslash \vdash \epsilon : \langle [], [], [], [] \rangle}$$

(Scope)
$$\frac{\Gamma \vdash A : X}{\Gamma \vdash \{A\} : \langle X^i, [], X^j, [] \rangle}$$

(New)
$$\frac{\Gamma \vdash A : X \quad x \notin \mathsf{dom}(\Gamma)}{\Gamma, x \prec A \vdash \mathsf{new}\, x : \langle X^i + x, X^o + x, X^j + x, X^p + x \rangle}$$

(Choice)
$$\frac{\Gamma \vdash A : X \qquad \Gamma \vdash B : Y}{\Gamma \vdash (A + B) : \langle X^i \cup Y^i, X^o \cup Y^o, X^j \cup Y^j, X^p \cup Y^p \rangle}$$

(Seq)
$$\frac{\Gamma \vdash A : X \qquad \Gamma \vdash B : Y \quad X^o + Y^j \subseteq R \quad A, B \neq \epsilon}{\Gamma \vdash AB : \langle X^i \cup (X^o + Y^j) \cup Y^i, (X^o + Y^p) \cup Y^o, X^j \cup (X^p + Y^j), X^p + Y^p \rangle}$$

Lemma 6.1.3 (Valid typing judgement). *If* $\Gamma \vdash_{\mathcal{R}} A : X$*, then*

1. $\mathsf{var}(A) \subseteq \mathsf{dom}(\Gamma), \mathsf{dom}(X^*) \subseteq \mathsf{dom}(\Gamma)$,
2. $\Gamma \vdash \epsilon : \langle [], [], [], [] \rangle$
3. *every variable in* $\mathsf{dom}(\Gamma)$ *is declared only once in* Γ,
4. $X^o \subseteq X^i \subseteq \mathcal{R}$ *and* $X^p \subseteq X^j \subseteq \mathcal{R}$,
5. $0 \leq X^i(z) - X^j(z) \leq 1$ *and* $0 \leq X^o(z) - X^p(z) \leq 1$

Definition 6.1.4 (Well-typed configurations). *Configuration* $\mathbb{S} = (M_1, E_1) \circ \cdots \circ (M_n, E_n)$ *is well-typed with respect to a basis* Γ *and a restriction* $\mathcal{R}$*, notation* $\Gamma \models_{\mathcal{R}} \mathbb{S}$*, if for all* $1 \leq k \leq n$*, we have* $\Gamma \vdash_{\mathcal{R}} E_k : X_k$ *and*

$$[\mathbb{S}|_k] + X_k^j \subseteq \mathcal{R}$$

Definition 6.1.5 (Well-typed programs). *Program* $Prog = Decls; E$ *is well-typed with respect to a requirement* $\mathcal{R}$ *if there exists a reordering* Γ *of declarations in* $Decls$ *and a type* X *such that* $\Gamma \vdash_{\mathcal{R}} E : X$*.*

6.2 Sharpness

Lemma 6.2.1 (Sharpness). *If* $\Gamma \vdash E : X$ *then, for every component* x*, for every well-typed configuration* $\mathbb{S}_0 = \mathbb{S} \circ (M, E)$ *there exist four generally different runs of* E *with lengths* n_1, n_2, n_3 *and* n_4*:*

$$\mathbb{S}_0 \to \cdots \to \mathbb{S}_{n_i} = \mathbb{S} \circ (M_{n_i}^i, \epsilon) \qquad (i \in \{1, 2, 3, 4\})$$

which fulfill one each of the following properties.

1. *If* $x \notin [\mathbb{S}_0]$ *there is a* k*,* $0 \leq k \leq n_1$ *such that* $[\mathbb{S}_k](x) = X^i(x)$
2. *If* $x \in [\mathbb{S}_0]$ *there is a* k*,* $0 \leq k \leq n_2$ *such that* $[\mathbb{S}_k](x) = X^j(x) + [\mathbb{S}_0](x)$
3. *If* $x \notin [\mathbb{S}_0]$*, then* $[\mathbb{S}_{n_3}](x) = X^o(x)$*.*
4. *if* $x \in [\mathbb{S}_0]$*, then* $[\mathbb{S}_{n_4}](x) = X^p(x) + [\mathbb{S}_0](x)$*.*

Corollary 6.2.2 (Sharpness of program). *For any program* $Prog = Decls; E$ *s.t.* $\Gamma \vdash_{\mathcal{R}} E : X$ *for some reordering* Γ *of* $Decls$ *and restriction* $\mathcal{R}$*, for every component* x*, there exist two generally different runs with lengths* n_1 *and* n_2*:*

$$([], Prog) = \mathbb{S}_0 \to \cdots \to \mathbb{S}_{n_i} = (M_{n_i}^i, \epsilon) \qquad (i \in \{1, 2\})$$

which fulfill one each of the following properties:

1. *there is a* k*,* $0 \leq k \leq n_1$ *such that* $[\mathbb{S}_k](x) = X^i(x)$
2. $M_{n_2}^2(x) = X^o(x)$

6.3 Introduction

A run is defined as in chapter 3, see page 59. I will also in this chapter prove another property of the runs. I will prove it together with sharpness, as a separate case.

Lemma 6.3.1 (Runs change store respecting limits). *If* $\Gamma \vdash_{\mathcal{R}} E : X$ *for some* E*,* $\mathcal{R}$*,* X *and* Γ*, it is the case that for all* $\mathbb{S}$ *and* M *such that* $\Gamma \models_{\mathcal{R}} \mathbb{S}_0 = \mathbb{S} \circ (M, E)$ *then for all runs* $\mathbb{S}_0 \to \cdots \to \mathbb{S}_n$ *of* E*, it is the case that if* $x \in [\mathbb{S}_0]$*, then* $[\mathbb{S}_n](x) - [\mathbb{S}_o] \leq X^p(x)$*, and otherwise* $[\mathbb{S}_n](x) \leq X^o(x)$*.*

6.4 Proof of Sharpness (Lemma 6.2.1)

Let $\Gamma \models_{\mathcal{R}} \mathbb{S}$ for some basis Γ, restriction $\mathcal{R}$ and configuration $\mathbb{S}$. The inductive hypothesis is: *for all shorter typing derivations* $\Gamma' \vdash_{\mathcal{R}} E : X$*, where* Γ' *is a sub-basis of* Γ*, for every component* x*, for every configuration* $\mathbb{S}_0 = \mathbb{S} \circ (M, E)$ *where* $\Gamma \models_{\mathcal{R}} \mathbb{S}_0$*, there exist four generally different runs of* E *with lengths* n_1, n_2, n_3 *and* n_4*:*

$$\mathbb{S}_0 \to \cdots \to \mathbb{S}_{n_i} = \mathbb{S} \circ (M^i_{n_i}, \epsilon) \qquad (i \in \{1, 2, 3, 4\})$$

which fulfill one each of the following properties:

1. *If* $x \notin [\mathbb{S}_0]$ *there is a* k*,* $0 \leq k \leq n_1$ *such that* $[\mathbb{S}_k](x) = X^i(x)$*.*
2. *If* $x \in [\mathbb{S}_0]$ *there is a* k*,* $0 \leq k \leq n_2$ *such that* $[\mathbb{S}_k](x) = X^j(x) + [\mathbb{S}_0](x)$*.*
3. *If* $x \notin [\mathbb{S}_0]$ *then* $[\mathbb{S}_{n_3}](x) = X^o(x)$*.*
4. *If* $x \in [\mathbb{S}_0]$ *then* $[\mathbb{S}_{n_4}](x) = X^p(x) + [\mathbb{S}_0](x)$*.*

And for all runs : if $x \in [\mathbb{S}_0]$ *we have* $[\mathbb{S}_n](x) - [\mathbb{S}_0](x) \leq X^p(x)$ *and if* $x \notin [\mathbb{S}_0]$ *we have* $[\mathbb{S}_n](x) \leq X^o(x)$*.*

Base cases

Axiom

$$\frac{}{\oslash \vdash \epsilon : \langle [], [], [], [] \rangle}$$

$$\mathbb{S}_0 = \mathbb{S} \circ (M, E) = \mathbb{S} \circ (M, \epsilon)$$

There is only one degenerate run of ϵ of length 0, where no resources are created. Let $k = 0$. Since $X^i(x) = X^j(x) = X^o(x) = X^p(x) = 0$ this is enough.

Inductive cases

WeakenB Assume $\Gamma \vdash E : X$ is inferred by an application of WeakenB:

$$\frac{\Gamma' \vdash E : X \quad \Gamma' \vdash B : Y \quad x \notin \mathsf{dom}(\Gamma')}{\Gamma', x \prec B \vdash E : X}$$

This case is easy — we know already by the inductive hypothesis on the premise $\Gamma' \vdash E : X$ that there exist runs of E with the properties needed for sharpness of X.

New Assume $\Gamma \vdash E : X$ is inferred by an application of New:

$$\frac{\Gamma' \vdash A : Y \quad y \notin \mathsf{dom}(\Gamma')}{\Gamma', y \prec A \vdash \mathsf{new}\, y : X = \langle Y^i + y, Y^o + y, Y^j + y, Y^p + y \rangle}$$

We have $E = \mathsf{new}\, y$ and $\Gamma = \Gamma', y \prec A$. From the inductive hypothesis we have existence of runs of the form $\mathbb{S} \circ (M + y, A) \to \cdots \to \mathbb{S} \circ (M' + y, \epsilon)$ of A. What we want are the corresponding runs:

$$\mathbb{S}_0 = \mathbb{S} \circ (M, \mathsf{new}\, y) \to \mathbb{S} \circ (M + y, A) \to \cdots \to \mathbb{S} \circ (M' + y, \epsilon) = \mathbb{S}_n$$

of $\mathsf{new}\, y$. The first step is the rule osNew from the operational semantics. The rest of the run exists by the inductive hypothesis. So I know I can use the runs, but now I must show they actually fulfill sharpness:

- For $y \neq x$ we can use the runs of A which exist by the inductive hypothesis for the properties of Y and that $Y^*(x) = X^*(x)$ and $[\mathbb{S} \circ (M + y, A)](x) = [\mathbb{S} \circ (M, A)](x)$.
- For $y = x$ we have that by valid typing $y \notin \mathsf{dom}(\Gamma - \{y \prec A\})$ and by lemma 6.1.3 (Valid typing judgement), $Y^* \subseteq \mathsf{dom}(\Gamma - \{y \prec A\})$, so $Y^*(y) = 0$ and there is no y created in the run of A. The extra y is added to the store in the first step of the run, and this will be the only y during the run of A.
  - X^i and X^j. I choose $k = 1$, and $[\mathbb{S}_1](y) = [\mathbb{S}_0](y) + 1$ while $X^*(y) = Y^*(y) + 1 = 1$.
  - X^o and X^p. We have $X^*(y) = Y^*(y)+1 = 1$ and $[\mathbb{S}_n](y) = [\mathbb{S}_0](y)+1$.
  - That $[\mathbb{S}_n](x) - [\mathbb{S}_0](x) \leq X^o(x)$ if $x \notin [\mathbb{S}_0]$ and $[\mathbb{S}_n](x) - [\mathbb{S}_0](x) \leq X^p(x)$ otherwise follows from the argument in the previous item.

Reu Assume $\Gamma \vdash E : X$ is inferred by an application of Reu:

$$\frac{\Gamma' \vdash A : Y \quad y \notin \mathsf{dom}(\Gamma')}{\Gamma', y \prec A \vdash \mathsf{reu}\, y : X = \langle Y^i + y, Y^o + y, Y^j, Y^p \rangle}$$

We have $E = \mathsf{reu}\, y$ and $\Gamma = \Gamma', y \prec A$. From the inductive hypothesis we have existence of runs of the form $\mathbb{S} \circ (M, A) \to \cdots \to \mathbb{S} \circ (M', \epsilon)$ and $\mathbb{S} \circ (M + y, A) \to \cdots \to \mathbb{S} \circ (M' + y, \epsilon)$ of A. What we want are the corresponding runs:

$$\mathbb{S}_0 = \mathbb{S} \circ (M, \mathsf{reu}\, y) \to \mathbb{S} \circ (M + y, A) \to \cdots \to \mathbb{S} \circ (M' + y, \epsilon) = \mathbb{S}_n$$

$$\mathbb{S}_0 = \mathbb{S} \circ (M, \mathsf{reu}\, y) \to \mathbb{S} \circ (M, A) \to \cdots \to \mathbb{S} \circ (M', \epsilon) = \mathbb{S}_n$$

of $\mathsf{reu}\, y$. The first step is the rule osReu1 or osReu2 from the operational semantics. The rest of the run exists by the inductive hypothesis. So I know I can use the runs, but now I must show they actually fulfill sharpness:

- For $y \neq x$ we can use the runs of A which exist by the inductive hypothesis for the properties of Y and that $Y^*(x) = X^*(x)$ and $[\mathbb{S} \circ (M + y, A)](x) = [\mathbb{S} \circ (M, A)](x)$.
- For $y = x$ we have that by valid typing $y \notin \mathsf{dom}(\Gamma - \{y \prec A\})$ and by lemma 6.1.3 (Valid typing judgement), $Y^* \subseteq \mathsf{dom}(\Gamma - \{y \prec A\})$, so $Y^*(y) = 0$ and there is no y created in the run of A. The possible extra y is added to the store in the first step of the run, and this will be the only y during the run of A.
  - X^i Since $x \notin [\mathbb{S}_0]$, the first transition in the run must be osReu1. I can choose $k \in \{1, \ldots, n_1\}$, and $[\mathbb{S}_k](y) = [\mathbb{S}_0](y) + 1 = 1$ while $X^i(y) = Y^i(y) + 1 = 1$.
  - X^j Since $x \in [\mathbb{S}_0]$, the first transition in the run must be osReu2. I can choose $k \in \{0, 1, \ldots, n_2\}$, and we have $[\mathbb{S}_k](y) = [\mathbb{S}_0](y)$ while $X^j(y) = Y^j(y) = 0$.
  - X^o Since $x \notin [\mathbb{S}_0]$, the first transition in the run must be osReu1. We also have $X^o(y) = Y^o(y) + 1 = 1$ and $[\mathbb{S}_{n_3}](y) = [\mathbb{S}_0](y) + 1 = 1$.

- X^p Since $x \in [\mathbb{S}_0]$, the first transition in the run must be osReu2. We also have $X^p(y) = Y^p(y) = 0$ and $[\mathbb{S}_{n_4}](y) = [\mathbb{S}_0](y)$.
- That $[\mathbb{S}_n](x) - [\mathbb{S}_0](x) \leq X^o(x)$ if $x \notin [\mathbb{S}_0]$ and $[\mathbb{S}_n](x) - [\mathbb{S}_0](x) \leq X^p(x)$ otherwise follows from the argument in the two previous items.

Seq Assume $\Gamma \vdash E : X$ is inferred by an application of SEQ:

$$\frac{\Gamma \vdash A : Y \qquad \Gamma \vdash B : Z \quad A, B \neq \epsilon}{\Gamma \vdash AB : X = \langle Y^i \cup (Y^o + Z^j) \cup Y^i, (Y^o + Z^p) \cup Z^o, Y^j \cup (Y^p + Z^j), Y^p + Z^p \rangle}$$

A run of $A\,B$ consists of a run of A followed by a run of B. From the inductive hypothesis we have knowledge of runs of A and B:

$$\mathbb{S} \circ (M_1, A) \to \cdots \to \mathbb{S} \circ (M_1', \epsilon)$$

and

$$\mathbb{S} \circ (M_2, B) \to \cdots \to \mathbb{S} \circ (M_2', \epsilon)$$

Adding B to the expression in the first configuration of the run of A gives a sequence of configurations from $\mathbb{S} \circ (M_1, AB)$ to $\mathbb{S} \circ (M_1', B)$ using the same transitions. In other words, for any run of length n

$$\mathbb{S} \circ (M_1, A) \to \cdots \to \mathbb{S} \circ (M_1', \epsilon)$$

there is a sequence of $n + 1$ configurations

$$\mathbb{S} \circ (M_1, AB) \to \cdots \to \mathbb{S} \circ (M_1', B)$$

with the same transitions. Now we go on to the runs of B. I choose $M_2 = M_1'$ and can then use the run directly.

$$\mathbb{S} \circ (M_1', B) \to \cdots \to \mathbb{S} \circ (M_2', \epsilon)$$

For the runs of B I need no transformation as in the case of A, and can directly use the runs existing by the inductive hypothesis. So for any pair of a run of A and a run of B, there is a run

$$\mathbb{S}_0 = \mathbb{S} \circ (M_1, AB) \to \cdots \to \mathbb{S} \circ (M_1', B) = \mathbb{S}_n \to \cdots \to \mathbb{S} \circ (M_2', \epsilon) = \mathbb{S}_{n+m}$$

of $A\,B$, using the same transitions. If the run of A is of length n and the run of B is of length m, the run of $A\,B$ will be of length $n + m$.

- $X^o(x)$. I have $x \notin [\mathbb{S}_0]$ and must find a run resulting in

  $$[\mathbb{S}_{n+m}](x) = X^o(x) = \max(Z^o(x), Y^o(x) + Z^p(x))$$

  I choose the run of A resulting in $[\mathbb{S}_n](x) = Y^o(x)$. If $x \notin Y^o$, we get that also $x \notin [\mathbb{S}_n]$ and that $X^o(x) = Z^o(x)$. I can then choose the run of B finally resulting in :

  $$[\mathbb{S}_{n+m}](x) = [\mathbb{S}_n](x) + Z^o(x) = \max(Z^o(x), Y^o(x) + Z^p(x)) = X^o(x)$$

  The second equality holds because $Y^o(x) = 0$ and since we have from valid typing judgement, lemma 6.1.3, that $Z^p(x) \leq Z^o(x)$.

If, on the other hand, $x \in Y^o$, we get $[\mathbb{S}_n](x) > 0$. By the inductive hypothesis there is now a run of B resulting in:

$$[\mathbb{S}_{n+m}](x) = [\mathbb{S}_n](x) + Z^p(x) = \\ = [\mathbb{S}_0](x) + Y^o(x) + Z^p(x) = \mathsf{max}(Z^o(x), Y^o(x) + Z^p(x)) = X^o(x)$$

The third equality holds since we have $Y^o(x) > 0$ and from valid typing judgement, lemma 6.1.3 that $Z^o(x) - Z^p(x) \leq 1$.

- $X^p(x)$. I have $x \in [\mathbb{S}_0]$ and must find a run resulting in:

$$[\mathbb{S}_{n+m}](x) = [\mathbb{S}_0](x) + X^p(x) = [\mathbb{S}_0](x) + Y^p(x) + Z^p(x)$$

From the inductive hypothesis there is a run of A resulting in $[\mathbb{S}_n](x) = [\mathbb{S}_0](x) + Y^p(x)$. Since we must have also $x \in [\mathbb{S}_n]$, I can then use the run of B finally resulting in:

$$[\mathbb{S}_{n+m}](x) = [\mathbb{S}_n](x) + Z^p(x) = [\mathbb{S}_0](x) + Y^p(x) + Z^p(x) = [\mathbb{S}_0](x) + X^p(x)$$

- $X^i(x)$. I have $x \notin [\mathbb{S}_0]$ and must find a run of $A\,B$: $\mathbb{S}_0 \to \cdots \to \mathbb{S}_n \to \cdots \to \mathbb{S}_{n+m}$, where there is k, such that $1 \leq k \leq n+m$ and

$$\begin{array}{rcl} [\mathbb{S}_k](x) & = & [\mathbb{S}_0](x) + X^i(x) = X^i(x) \\ & = & (Y^i \cup (Y^o + Z^j) \cup Z^i)(x) \\ & = & \mathsf{max}(Y^i(x), Y^o(x) + Z^j(x), Z^i(x)) \end{array}$$

The k with the maximum store can be found both during execution of A (i.e. $k \leq n$) or during execution of B (i.e. $k > n$).

To prove that there will always be such a run and k, I must do a case distinction on the value of $X^i(x) = \max(Y^i(x), Y^o(x) + Z^j(x), Z^i(x))$:

  - If $Y^i(x) = \max(Y^i(x), Y^o(x) + Z^j(x), Z^i(x))$ we can use the run of A which by the inductive hypothesis has a configuration $\mathbb{S}_{k_A}$ such that $[\mathbb{S}_{k_A}](x) = Y^i(x) = X^i(x)$, so I can use k_A as k.
  - Otherwise, if $Y^o(x) + Z^j(x) = \max(Y^i(x), Y^o(x) + Z^j(x), Z^i(x))$, we use the run of A which ends in $\mathbb{S}_n = \mathbb{S} \circ (M', B)$ where $[\mathbb{S}_n](x) = Y^o(x)$. If $x \notin Y^o$, I can then choose the run of B where there is a k_B such that

$$[\mathbb{S}_{k_B}](x) = [\mathbb{S}_n](x) + Z^i(x) = Z^i(x) = \max(Y^o(x) + Z^j(x), Z^i(x)) = \\ = \max(Y^i(x), Y^o(x) + Z^j(x), Z^i(x)) = X^i(x)$$

and use $n + k_B$ as k. The third equality holds by $x \notin Y^o$ and $0 \leq Z^i(x) - Z^j(x) \leq 1$ from valid typing judgement, lemma 6.1.3, clause 5. The fourth equality holds from the assumptions in this case $(Y^o(x) + Z^j(x) = \max(Y^i(x), Y^o(x) + Z^j(x), Z^i(x)))$. If, on the other hand, $x \in Y^o$, I must choose the run of B and the k_B such that

$$[\mathbb{S}_{k_B}](x) = [\mathbb{S}_n](x) + Z^j(x) = Y^o(x) + Z^j(x) = \\ = \max(Y^i(x), Y^o(x) + Z^j(x), Z^i(x)) = X^i(x)$$

Here, the third equality holds from the assumptions on this case, namely $Y^o(x) + Z^j(x) = \max(Y^i(x), Y^o(x) + Z^j(x), Z^i(x))$.

– If neither of the other hold, we have $Z^i(x) = \max(Y^i(x), Y^o(x) + Z^j(x), Z^i(x))$. Since we already treated the other cases, we must have

$$Z^i(x) > (Z^j(x) + Y^o(x) \tag{6.1}$$

From valid typing judgement we get

$$Z^i(x) \leq Z^j(x) + Y^o(x) \tag{6.2}$$

By combining (6.1) and (6.1), we get that $Y^o(x) = 0$. From the inductive hypothesis I can then use any run of A and it will end in $\mathbb{S}_n = \mathbb{S} \circ (M', B)$ where $[\mathbb{S}_n](x) = 0$. I can then choose the run of B where there is a k_B such that

$$\begin{array}{l}[\mathbb{S}_{k_B}](x) = [\mathbb{S}_n](x) + Z^i(x) = Z^i(x) = \\ = \max(Y^i(x), Y^o(x) + Z^j(x), Z^i(x)) = X^i(x)\end{array}$$

and use $n + k_B$ as k.

- $X^j(x)$. I have $x \in [\mathbb{S}_0]$ and must find a run of $A\,B$: $\mathbb{S}_0 \to \cdots \to \mathbb{S}_n = \mathbb{S} \circ (M, B) \to \cdots \to \mathbb{S}_{n+m}$, where there is k, such that $1 \leq k \leq n + m$ and

$$\begin{array}{rcl}[\mathbb{S}_k](x) & = & [\mathbb{S}_0](x) + X^j(x) \\ & = & [\mathbb{S}_0](x) + (Y^j \cup (Y^p + Z^j))(x) \\ & = & [\mathbb{S}_0](x) + \max(Y^j(x), Y^p(x) + Z^j(x))\end{array}$$

The k with the maximum store can be found both during execution of A (i.e. $k \leq n$) or during execution of B (i.e. $k > n$).

To prove that there will always be such a run and k, I must do a case distinction on the value of $X^j(x) = \max(Y^j(x), Y^p(x) + Z^j(x))$:

– If $Y^j(x) = \max(Y^j(x), Y^p(x) + Z^j(x))$ we can use the run of A which by the inductive hypothesis has a configuration $\mathbb{S}_{k_A}$ such that $[\mathbb{S}_{k_A}](x) = [\mathbb{S}_0](x) + Y^j(x) = [\mathbb{S}_0](x) + X^j(x)$, so I can use k_A as k.

– Otherwise, we must have $Y^p(x) + Z^j(x) > Y^j(x)$, and I use the run of A which ends in $\mathbb{S}_n = \mathbb{S} \circ (M', B)$ where $[\mathbb{S}_n](x) = [\mathbb{S}_0](x) + Y^p(x)$. I can now choose the run of B and the k_B such that

$$\begin{array}{l}[\mathbb{S}_{k_B}](x) = [\mathbb{S}_n](x) + Z^j(x) = [\mathbb{S}_0](x) + Y^p(x) + Z^j(x) = \\ = [\mathbb{S}_0](x) + \max(Y^j(x), Y^p(x) + Z^j(x)) = [\mathbb{S}_0](x) + X^j(x)\end{array}$$

Here, the third equality holds from the assumptions on this case, $(Y^p(x) + Z^j(x) = \max(Y^j(x), Y^p(x) + Z^j(x)))$.

- I must also show that

$$[\mathbb{S}_{n+m}](x) \leq X^o(x) = \max(Y^o(x) + Z^p(x), Z^o(x))$$

for any run where $x \notin [\mathbb{S}_0]$. I have from the inductive hypothesis that for any run of A starting from such a configuration, that $[\mathbb{S}_n](x) \leq Y^o(x)$. If the run does not produce any instances of x, such that we get also $x \notin [\mathbb{S}_n]$, I then have from the inductive hypothesis that for any run of B

starting from this configuration, we get $[\mathbb{S}_{n+m}](x) \leq Z^o(x)$, and adding these inequalities I get $[\mathbb{S}_{n+m}](x) \leq Z^o(x) \leq X^o(x)$. If on the other hand, the run of A does produce some instance of x, we get $x \in [\mathbb{S}_n](x)$. I then have from the inductive hypothesis that for any run of B, we have $[\mathbb{S}_{n+m}](x) - [\mathbb{S}_n](x) \leq Z^p(x)$. Since $[\mathbb{S}_n](x) \leq Y^o(x)$ this implies further that

$$[\mathbb{S}_{n+m}](x) \leq Z^p(x) + Y^o(x) \leq X^o(x)$$

- Finally I must show that $[\mathbb{S}_{n+m}](x) - [\mathbb{S}_0](x) \leq X^p(x) = Y^p(x) + Z^p(x)$ for any run where $x \in [\mathbb{S}_0]$. I have from the inductive hypothesis that for any run of A, $[\mathbb{S}_n](x) - [\mathbb{S}_0](x) \leq Y^p(x)$. I now have from the inductive hypothesis that for any run of B, we have $[\mathbb{S}_{n+m}](x) - [\mathbb{S}_n](x) \leq Z^p(x)$. Adding these three inequalities I get $[\mathbb{S}_{n+m}](x) - [\mathbb{S}_0](x) \leq Y^p(x) + Z^p(x) = X^p(x)$.

Choice Let $E = (A + B)$, $\Gamma \vdash A : Y$ and $\Gamma \vdash B : Z$.

$$\frac{\Gamma \vdash A : Y \quad \Gamma \vdash B : Z}{\Gamma \vdash (A + B) : \langle Y^i \cup Z^i, Y^o \cup Z^o, Y^j \cup Z^j, Y^p \cup Z^p \rangle}$$

For this rule, I must use two inductive hypotheses, one for each of the premises in the typing rule ($A : Y$ and $B : Z$). This means the whole proof is an instance of simultaneous induction. To run $(A + B)$, we must choose a run of A or a run of B. For any run of A or B, that is, $\mathbb{S} \circ (M, A) \to \cdots \to \mathbb{S} \circ (M', \epsilon)$, there is a corresponding run of $(A + B)$, with the same transitions, only one instance of osChoice added in front, e.g..:

$$\mathbb{S} \circ (M, (A + B)) \to \mathbb{S} \circ (M, A) \to \cdots \to \mathbb{S} \circ (M', \epsilon) = \mathbb{S}_n$$

- $X^i(x)$. By the inductive hypothesis, if $x \notin [\mathbb{S}_0]$, there is a run of A and a state k_A in the run such that $[\mathbb{S}_{k_A}](x) = Y^i(x)$, and correspondingly for B there is a run and a k_B. For a run of $(A + B)$ with a state k achieving $[\mathbb{S}_k](x) = X^i(x) = (Y^i \cup Z^i)(x) = \max(Y^i(x), Z^i(x))$, choose the run of A and $k = k_A$ if $Y^i(x) > Z^i(x)$, otherwise choose the run of B and $k = k_B$. We will then have

$$[\mathbb{S}_k](x) = \max(Y^i(x), Z^i(x)) = X^i(x)$$

- $X^j(x)$. We can use almost the same argument as in the previous item. Replace ^{i} with ^{j} and add $[\mathbb{S}_0](x)$ to the equations where necessary.

- $X^o(x)$ By the inductive hypothesis, if $x \notin [\mathbb{S}_0]$, there is a run of A of length n_A such that $[\mathbb{S}_{n_A}](x) = Y^o(x)$, and correspondingly for B. For a run of $(A + B)$ achieving $[\mathbb{S}_n](x) = X^o(x) = (Y^o \cup Z^o)(x) = \max(Y^o(x), Z^o(x))$, choose the run of A if $Y^o(x) > Z^o(x)$, otherwise choose the run of B. We will then have

$$[\mathbb{S}_n](x) = \max(Y^o(x), Z^o(x)) = X^o(x)$$

- $X^p(x)$. This can be proven by modifying the argument in the previous item: replace ^{o} with ^{p} and add $[\mathbb{S}_0](x)$ to the equations where necessary.

- I must also show that $[\mathbb{S}_n](x) \leq X^o(x)$ for any run where $x \notin [\mathbb{S}_0]$. I have from the inductive hypothesis that for any run of A starting from such a configuration, that if n_A is the length, then $[\mathbb{S}_{n_A}](x) \leq Y^o(x)$, and that for any run of B starting from such a configuration, that if n_B is the length, then $[\mathbb{S}_{n_B}](x) \leq Z^o(x)$. Since the run of $A + B$ is only a run of A or B with one transition in front which does not alter any store, we get that the maximum size of the store after the run of $A + B$, is the maximum it could be after any run of A or of B, that is:

$$[\mathbb{S}_n](x) \leq \max(Y^o(x), Z^o(x)) = X^o(x)$$

- Finally I must show that $[\mathbb{S}_{n+m}](x) - [\mathbb{S}_0](x) \leq X^p(x)$ for any run where $x \in [\mathbb{S}_0]$. Use the argument from the previous item, only replace ^{o} with ^{p} and add $[\mathbb{S}_0](x)$ to the equations where necessary.

Scope Let $E = \{A\}$ and $\Gamma \vdash A : Y$.

$$\frac{\Gamma \vdash A : Y}{\Gamma \vdash \{A\} : \langle Y^i, [], Y^j, [] \rangle}$$

In the operational semantics, a new pair $([], A)$ is created on top of the stack through the transition rule osPush, A is run, and then osPop removes the pair again. So, for any run

$$\mathbb{S} \circ ([], A) \to \cdots \to \mathbb{S} \circ (M', \epsilon)$$

of A there is a run

$$\begin{array}{ll} \mathbb{S} \circ (M, \{A\}) & \mathbb{S}_0 \\ \to \mathbb{S} \circ (M, \epsilon) \circ ([], A) & \mathbb{S}_1 \\ \to \cdots \to \mathbb{S} \circ (M, \epsilon) \circ (M', \epsilon) & \mathbb{S}_{n-1} \\ \to \mathbb{S} \circ (M, \epsilon) & \mathbb{S}_n \end{array}$$

of $\{A\}$ using the same transitions but in addition having osPush and osPop at the start and the end. I can assume existence of wanted runs of A, since $\Gamma \vdash A : Y$ must hold by the typing rule. For X^o and X^p any run of A is okay, since no resources are returned ($[\mathbb{S}_n](x) = [\mathbb{S}_0](x)$) and $X^o = X^p = []$. For the last two properties concerning $X^i(x)$ and $X^j(x)$, choose the run and k_A such that

$$[\mathbb{S}_{k_A}](x) = [\mathbb{S}_0](x) + Y^i(x) = X^i(x)$$

or correspondingly for X^j, the run and k_A, such that

$$[\mathbb{S}_{k_A}](x) = [\mathbb{S}_0](x) + Y^j(x)X^j(x) + [\mathbb{S}_0](x)$$

which exist by the inductive hypothesis. So we can let $k = k_A$.

Bibliography

[1] Hendrik P. Barendregt. Lambda calculi with types. In S. Abramsky, Dov M. Gabbay, and T.S.E. Maibaum, editors, *Handbook of Logic in Computer Science*, volume 2, pages 117-309. Oxford Univertity Press, 1992.

[2] Marc Bezem and Hoang A. Truong. Counting instances of software components. In Didier Galmiche, Peter O'Hearn, and David J. Pym, editors, *Proceedings of the ICALP/LICS Workshop on Logics for Resources, Processes, and Programs*, July 2004. Submitted to the Journal of Logic and Computation Semantics Corner. `http://hdl.handle.net/1956/1172`.

[3] D.U.M.A. - Detect Unintended Memory Access. `http://duma.sourceforge.net`.

[4] GCC, the Gnu Compiler Collection. `http://gcc.gnu.org`.

[5] John E. Hopcroft, Jeffrey D. Ullman. *Introduction to automata theory, languages and computation*, (1979). Addison-Wesley Publishing Company.

[6] Dave Jones. Why Userspace Sucks - (Or, 101 Really Dumb Things Your App Shouldn't Do) in *Proceedings of the Linux Symposium, Volume One*, July 2006, Canada. `http://www.linuxsymposium.org/2006/linuxsymposium_procv1.pdf`.

[7] Haakon Nilsen. An Implementation of a Type System for the Safe Instantiation of Components. `http://www.ii.uib.no/~haakon/components/`.

[8] Splint - Secure Programming Lint. `http://www.splint.org`.

[9] Apostolos Syropolous. Mathematics of Multisets. In C.S.Calude et al., editors, *Multiset Processing*, pages 347-358. Springer-Verlag 2001.

[10] Valgrind. `http://valgrind.org`.

[11] Hoang A. Truong and Marc Bezem. Finding Resource Bounds in the Presence of Explicit Deallocation, in *Lecture Notes in Computer Science, Theoretical Aspects of Computing - 2013 ICTAC 2005: Second International Colloquium*, October 2005. `http://hdl.handle.net/1956/1174`.

[12] Hoang A. Truong. Guaranteeing Resource Bounds for Component Software, in *Lecture Notes in Computer Science, Formal Methods for Open Object-Based Distributed Systems: 7th IFIP WG 6.1 International Conference, FMOODS 2005*, June 2005. `http://hdl.handle.net/1956/1173`.

[13] Hoang A. Truong. *Type Systems for Guaranteeing Resource Bounds of Component Software*, (2006). Thesis for the degree philosophiae doctor, University of Bergen, Norway. `http://hdl.handle.net/1956/1175`.

[14] Wagner et al. A First Step Towards Automated Detection of Buffer Overrun Vulnerabilities. `http://http.cs.berkeley.edu/~daw/papers/overruns-ndss00.pdf`.