New Foundations for Separation Logic

Hiep, H.A.

Chapter 3

Proof theory of separation logic

Our goal is to obtain a sound and complete, finitary proof system for reasoning about the valid formulas of separation logic. To that end we introduce two calculi consisting of separation logic formulas and *rooted assertions*, which are separation logic formulas that are annotated with a representation of the heap with respect to which the separation logic formula is evaluated. We shall argue that the obtained finitary proof systems are sound and complete with respect to different interpretations. However, before jumping to the conclusion, we first need to explain the development of this result.

As seen in the previous chapter, the semantics **WSL** and **FSL** can not be adequately used as interpretations, due to their failure of compactness (of the satisfaction relation or the semantic consequence relation). The main model-theoretic results are that **WSL** is already non-compact even for the pure formulas, and in the setting of **FSL** we can express: (1) finiteness of structures, (2) well-foundedness of the points-to relation, and (3) existence of countably infinite and uncountable structures. As a consequence we have that **FSL** satisfies neither compactness nor the downward and upward Löwenheim-Skolem theorems. In fact, we have seen that the well-foundedness of the points-to relation can already be expressed in **FSL** using only separating conjunction. Consequently, **FSL** without separating implication is already non-compact. For **FSL** without separating implication but in which separating conjunction only occurs positively, the fragment which we called separation logic light (SLL), we do have compactness, but its semantic consequence relation is not compact. Non-compactness (of the satisfaction relation or the semantic consequence relation) implies that there does not exist a finitary, sound and complete proof system with respect to these interpretations.

Recall that in Section 2.4 we have seen that it is possible to embed full separation logic in dyadic second-order classical logic, and in Section 2.5 we have seen an investigation of the converse: can dyadic second-order logic be embedded in full separation logic too? This is a good starting point in light of the above goal, since if separation logic is equally expressive as second-order logic we could simply use Henkin's semantics of second-order logic directly. However, this question is

still open, and we conjecture that the binding operator cannot be expressed in separation logic due to its inherent local perspective.

The question thus arises whether there exists an *alternative* interpretation of separation logic that does allow for a finitary, sound and complete proof system. Clearly, the main complexity of separation logic stems from the (second-order) quantification over heaps (or sub-heaps, in the case of the separating conjunction). For second-order logic a sound and complete axiomatization can be obtained by generalizing its semantics by means of so-called *general structures*. Such structures extend first-order structures with a set of possible interpretations of the second-order variables. For example, instead of interpreting a second-order variable of arity 1 as ranging over *all* possible subsets of the given first-order domain, a general structure restricts its interpretation to a given set of such subsets. The standard structures of second-order logic are thus a particular instance of general structure. This generalization of the semantics of second-order logic allows for a sound and complete axiomatization by restricting to Henkin structures [108]. A Henkin structure is a general structure for second-order logic which additionally satisfies the comprehension axiom scheme

$$\exists R^n \forall x_1, \ldots, x_n (R^n(x_1, \ldots, x_n) \leftrightarrow \phi(x_1, \ldots, x_n))$$

for any second-order formula $\phi(x_1, \ldots, x_n)$ which does not contain the n-ary variable R. In the *arithmetic* comprehension axiom $\phi(x_1, \ldots, x_n)$ is first-order.

Generalizing the semantics of separation logic accordingly in terms of a given set of possible heaps, which does not necessarily contain *all* heaps, we can formulate in separation logic the following version of the arithmetic comprehension axiom scheme

$$\blacklozenge(\forall x, y((x \hookrightarrow y) \leftrightarrow \phi(x, y)))$$

which expresses the existence of a heap such that its *graph*, as denoted by the points-to relation $\hookrightarrow$, satisfies the pure first-order formula $\phi(x, y)$. The formula ϕ is pure in the sense that it does not involve the separation connectives or the points-to relation. The $\blacklozenge$-modality expresses the existence of a heap which satisfies the associated formula. Such an instance of the arithmetic comprehension axiom holds if there exists a heap which is characterized by the formula $\phi(x, y)$. Therefore, we introduce a new interpretation of separation logic that restricts the (second-order) quantification over heaps to *first-order definable* heaps.

For this new interpretation we introduce a *sequent calculus* which is sound and complete. In this sequent calculus we introduce so-called *rooted formulas* $\phi @ \psi$ where $\psi(x, y)$ are pure first-order formulas. In the interpretation of rooted formulas, $\psi(x, y)$ determines the interpretation of the heap with respect to which ϕ is evaluated. The completeness proof is based on the construction of a model for a *deductively consistent* theory (a theory from which false is not derivable), following Henkin's approach. From the completeness proof we further derive that this new interpretation satisfies both compactness and the downward Löwenheim-Skolem theorem. By the seminal theorem of Lindström [217, 210] we then infer that this new interpretation is as expressive as first-order logic.

However, we cannot generalize arithmetic comprehension to arbitrary separation logic formulas because that leads to obvious contradictions, such as

$$\blacklozenge(\forall x, y((x \hookrightarrow y) \leftrightarrow \neg(x \hookrightarrow y))).$$

Simply requiring that the points-to relation does not occur in $\phi(x, y)$ does not give more than what the arithmetic comprehension axiom above gives, because compositions of pure first-order formulas with separating connectives are equivalent to some pure first-order formula (this easily follows from the semantics of separation logic). To overcome this issue, we extend our rooted formulas $\phi@\psi$ without any restrictions on ψ, where @ can now be understood as a special let binding connective. We need a new interpretation of separation logic, which no longer can be captured by a syntactic comprehension axiom scheme, and instead we consider a class of general structures which satisfy a closure condition called *semantic comprehension*.

For this new, second interpretation of separation logic we introduce a *natural deduction calculus* which is also sound and complete. We show completeness by constructing models for deductively consistent theories, in a similar way as for our sequent calculus.

3.1 Sequent calculus

In full relational separation logic we have that the following formulas are valid:

$$\blacklozenge(\forall x, y((x \hookrightarrow y) \leftrightarrow \phi(x, y)))$$

where ϕ is a pure, first-order formula. The above class of formulas, called the *arithmetic comprehension axiom scheme*, expresses, for each pure first-order formula $\phi(x, y)$, the existence of a relation such that its *graph*, as denoted by the points-to relation $\hookrightarrow$, satisfies $\phi(x, y)$. In this section, we shall consider a restriction of full relational separation logic in which we consider *only* those relations which have a corresponding first-order description. These relations are called first-order definable. This means that we restrict our attention to the interpretation of the separating connectives to such first-order definable binary relations.

Let ϕ denote a first-order formula which does not contain occurrences of the points-to relation $\hookrightarrow$ of separation logic. We have the standard inductive truth definition $\mathfrak{A}, \rho \models^{\mathbf{CL}} \phi$ for first-order formulas ϕ. By $\phi(x_1, \ldots, x_n)$ we denote that the free (first-order) variables of ϕ are among the distinct variables $x_1, \ldots, x_n$. A formula $\phi(x, y)$ is called a *binary* formula. For notational convenience we assume that the variables x and y of any binary formula are fixed and do not occur in any separation logic formula. A binary formula is also simply denoted by ϕ, omitting its free variables x and y. Given a structure $\mathfrak{A} = (A, \mathcal{I})$ and a first-order formula $\phi(x, y)$, we denote by $Rel_{\mathfrak{A}}(\phi)$ the relation $\{\langle \rho(x), \rho(y) \rangle \mid \mathfrak{A}, \rho \models^{\mathbf{CL}} \phi\} \subseteq A \times A$. Note that the evaluation of $\phi(x, y)$ only depends on the values of its free variables x and y, that is, $\mathfrak{A}, \rho \models^{\mathbf{CL}} \phi$ if and only if $\mathfrak{A}, \rho' \models^{\mathbf{CL}} \phi$, where $\rho(x) = \rho'(x)$ and $\rho(y) = \rho'(y)$. By $\phi(t, t')$ we denote the result of replacing in $\phi(x, y)$ the variables x and y by terms t and t', respectively (if necessary renaming bound variables to ensure that the variables of t and t' do not become bound).

Definition 3.1.1 (First-order definability)**.** For a given structure $\mathfrak{A} = (A, \mathcal{I})$, the relation $\mathcal{R} \subseteq A \times A$ is *first-order definable* if $\mathcal{R} = Rel_{\mathfrak{A}}(\phi)$, for some binary formula $\phi(x, y)$.

Note that, given a structure $\mathfrak{A} = (A, \mathcal{I})$, we have $\mathcal{I}(R) = Rel_{\mathfrak{A}}(R)$, that is, for any binary relation symbol R its interpretation $\mathcal{I}(R)$ is trivially a first-order definable relation. We introduce the abbreviation $\phi = \phi_1 \uplus \phi_2$ that denotes that the binary formulas $\phi_1(x, y)$ and $\phi_2(x, y)$ represent a partition of the binary formula $\phi(x, y)$ which is expressed by the conjunction of the three formulas

$$\begin{gathered}\forall x, y(\phi(x, y) \leftrightarrow (\phi_1(x, y) \vee \phi_2(x, y))),\\ \forall x, y, z(\phi_1(x, y) \rightarrow \neg\phi_2(x, z)),\\ \forall x, y, z(\phi_2(x, y) \rightarrow \neg\phi_1(x, z)).\end{gathered}$$

The latter two formulas, which state that the domains of the binary relations represented by $\phi_1(x, y)$ and $\phi_1(x, y)$ are disjoint, we abbreviate by $\phi_1 \perp \phi_2$. A similar abbreviation can be given for binary relation symbols $R = R_1 \uplus R_2$. By usual abuse of notation, we mean that the equality holds for the *extension* of R (so we need to universally quantify two variables x, y and apply them to R, R_1, R_2).

In this section, to avoid confusion between formulas of separation logic and formulas of first-order logic, we shall denote the former by p, q and the later by ϕ, ψ. We introduce the semantics $\mathfrak{A}, \mathcal{R}, s \models^{\mathbf{FORSL}} p$ which is a *restriction* of the general relational semantics of separation logic (see also Definition 3.4.2) such that instead of quantifying over arbitrary binary relations, the separating connectives involve quantification over first-order definable binary relations. It is worthwhile to observe here that, as for Henkin models of second-order logic, the implicit second-order quantification depends on the underlying signature of function and relation symbols. Extending or restricting the signature affects the semantics of formulas of the 'old' signature.

To reason about the implicit quantification over definable (binary) relations, we introduce *rooted* assertions of the form $p@\phi$, where ϕ denotes a binary formula and p is a formula of separation logic. We define $\mathfrak{A}, \rho \models^{\mathbf{FORSL}} p@\phi$ if and only if $\mathfrak{A}, \mathcal{R}, \rho \models^{\mathbf{FORSL}} p$, where $\mathcal{R} = Rel_{\mathfrak{A}}(\phi)$. The variables x and y of the binary formula $\phi(x, y)$ are thus implicitly bound by the @-connective, that is, $\mathfrak{A}, \rho \models^{\mathbf{FORSL}} p@\phi$ if and only if $\mathfrak{A}, \rho' \models^{\mathbf{FORSL}} p@\phi$, for any ρ and ρ' such that $\rho(z) = \rho'(z)$, for any free variable occurring in p.

We further assume that our signature includes a (countably) infinite set of binary relation symbols R (needed for the selection of fresh 'witnesses'). However, definability of binary relation by a first-order formula should not depend on these additional binary relation symbols. That is, these binary relation symbols are added as 'bookkeeping devices'. Alternatively, we could have introduced these as (second-order) *variables* and extend evaluations so that $\rho(R) \subseteq D \times D$, for any such (second-order) variable. However, for both technical and notational convenience we prefer to define their semantics as part of a structure.

Note that the separating connectives are interpreted in terms of relations which are definable by first-order formulas which do not involve the points-to

Separating conjunction

$$\mathbf{L}_* \quad \frac{\Gamma, \phi = R_1 \uplus R_2, p@R_1, q@R_2 \Rightarrow \Delta}{\Gamma, (p * q)@\phi \Rightarrow \Delta}$$

$$\mathbf{R}_* \quad \frac{\Gamma \Rightarrow \Delta, \phi = \phi_1 \uplus \phi_2 \quad \Gamma \Rightarrow \Delta, p@\phi_1 \quad \Gamma \Rightarrow \Delta, q@\phi_2}{\Gamma \Rightarrow \Delta, (p * q)@\phi}$$

Separating implication

$$\mathbf{L}_{-\!\!*} \quad \frac{\Gamma \Rightarrow \Delta, \phi \perp \psi \quad \Gamma \Rightarrow \Delta, p@\psi \quad \Gamma, q@(\phi \vee \psi) \Rightarrow \Delta}{\Gamma, (p -\!\!* q)@\phi \Rightarrow \Delta}$$

$$\mathbf{R}_{-\!\!*} \quad \frac{\Gamma, R \perp \phi, p@R \Rightarrow \Delta, q@(\phi \vee R)}{\Gamma \Rightarrow \Delta, (p -\!\!* q)@\phi}$$

Points-to rules

$$\frac{\Gamma, p[\phi/\hookrightarrow] \Rightarrow \Delta}{\Gamma, p@\phi \Rightarrow \Delta} \qquad \frac{\Gamma \Rightarrow p[\phi/\hookrightarrow], \Delta}{\Gamma \Rightarrow p@\phi, \Delta}$$

Figure 3.1: Sequent calculus for **FORSL**. The binary relation symbols R_1, R_2 and R introduced in the rules $\mathbf{L}_*$ and $\mathbf{R}_{-\!\!*}$ are 'fresh'. In the points-to rules p denotes a semi-pure formula (which does not contain occurrences of the separating connectives).

relation $\hookrightarrow$. This allows for the following alternative *predicative*[1] characterization of the semantics of the separating connectives in rooted assertions (used in both the soundness and completeness proofs).

Lemma 3.1.2. *We have*

- $\mathfrak{A}, \rho \models^{\mathbf{FORSL}} (p * q)@\phi$ *if and only if there exist binary formulas* ϕ_1 *and* ϕ_2 *such that:*
  $\mathfrak{A}, \rho \models^{\mathbf{FORSL}} \phi = \phi_1 \uplus \phi_2$,
  $\mathfrak{A}, \rho \models^{\mathbf{FORSL}} p@\phi_1$, *and*
  $\mathfrak{A}, \rho \models^{\mathbf{FORSL}} q@\phi_2$.
- $\mathfrak{A}, \rho \models^{\mathbf{FORSL}} (p -\!\!* q)@\phi$ *if and only if*
  $\mathfrak{A}, \rho \models^{\mathbf{FORSL}} \psi \perp \phi$ *and* $\mathfrak{A}, \rho \models^{\mathbf{FORSL}} p@\psi$ *implies*
  $\mathfrak{A}, \rho \models^{\mathbf{FORSL}} q@(\phi \vee \psi)$, *for all binary formulas* ψ.

We now develop a calculus for sequents $A_1, \ldots, A_n \Rightarrow B_1, \ldots, B_m$, where each A_i (given $i = 1, \ldots, n$), and B_j (given $j = 1, \ldots, m$), is constructed from first-order

[1] For a foundational discussion concerning predicativity, see [57].

formulas and rooted assertions, which can be further composed using propositional connectives and quantification of first-order variables. In particular, we have the following abstract grammar:

$$\begin{aligned}\phi, \psi &::= \bot \mid (x \doteq y) \mid C(x_1, \ldots, x_n) \mid (\phi \to \psi) \mid (\forall x \phi) \\ p, q &::= \bot \mid (x \doteq y) \mid (x \hookrightarrow y) \mid C(x_1, \ldots, x_n) \mid (p * q) \mid (p \mathrel{-\!\!*} q) \mid (p \to q) \mid (\forall x p) \\ A, B &::= \bot \mid p@\phi \mid (A \to B) \mid (\forall x A)\end{aligned}$$

where in rooted formulas $p@\phi$ the first-order formula ϕ has at most free variables x, y. Note that the free variables of $p@\phi$ are only the free variables of p, since the @-connective binds the free variables x and y.

This calculus is an extension of standard first-order sequent calculus, where the standard rules are applicable with respect to top-level propositional connectives and quantifiers. Figure 3.1 shows the left and right rules for separating conjunction and implication. These rules closely follow the translation of relational separation logic into second-order logic, eliminating the explicit second-order quantification by applying the standard proof rules for second-order quantification (which themselves are straightforward generalizations of the rules for first-order quantification, instantiating the second-order variables by formulas). The binary relation symbols R_1, R_2 and R introduced in the rules $\mathbf{L}_*$ and $\mathbf{R}_{-\!\!*}$ are 'fresh' binary relation symbols, that is, they must not appear in the formulas of the conclusion of the rules.

We also have rules which allow classical reasoning under rooted assertions: $(p \circ q)@\phi \leftrightarrow (p@\phi) \circ (q@\phi)$, where $\circ$ denotes binary propositional connectives, e.g., conjunction, disjunction, and implication, $(\neg p)@\phi \leftrightarrow \neg(p@\phi)$, and $(\exists x p)@\phi \leftrightarrow \exists x(p@\phi)$, and similarly $(\forall x p)@\phi \leftrightarrow \forall x(p@\phi)$. Further, we have $(\forall x, y(\phi \leftrightarrow \psi)) \to (p@\phi \leftrightarrow p@\psi)$. It is straightforward to validate these rules, but we omit the details of the semantics $\mathfrak{A}, \rho \models^{\mathbf{FORSL}} A$, which follows the standard Tarski-style classical semantics, given the semantics of rooted assertions which may appear in the place of atomic formulas.

In the so-called 'points-to' rules of Figure 3.1 the formula p does not involve occurrences of the separating connectives. Such a formula of separation logic we call *semi-pure*. Note that it differs from pure first-order formulas in that semi-pure formulas additionally may involve the points-to relation. For such formulas we denote by $p[\phi/\hookrightarrow]$, for any binary formula $\phi(x, y)$, the result of replacing every atomic assertion $(t \hookrightarrow t')$ in p by $\phi(t, t')$, which is a pure first-order formula. It follows that $\mathfrak{A}, \rho \models^{\mathbf{FORSL}} p[\phi/\hookrightarrow]$ if and only if $\mathfrak{A}, Rel_{\mathfrak{A}}(\phi), \rho \models^{\mathbf{FORSL}} p$, for any semi-pure formula p.

We now see a number of example proofs, in which we use the sequent calculus defined above.

$$\dfrac{\dfrac{\dfrac{\dfrac{\Gamma \Rightarrow q@R, R_1 \perp R_2 \quad \Gamma \Rightarrow q@R, p@R_1 \quad \Gamma, q@(R_1 \vee R_2) \Rightarrow q@R}{R = R_1 \uplus R_2, p@R_1, (p \mathrel{-\!\!*} q)@R_2 \Rightarrow q@R}\,\mathbf{L}_{-\!\!*}}{(p * (p \mathrel{-\!\!*} q))@R \Rightarrow q@R}\,\mathbf{L}_*}{\Rightarrow (p * (p \mathrel{-\!\!*} q))@R \to q@R}}{\Rightarrow ((p * (p \mathrel{-\!\!*} q)) \to q)@R}$$

As a first example of the use of the sequent calculus, above we have a derivation of the sequent $\Rightarrow ((p * (p \mathrel{-\!\!*} q)) \to q)@R$ which represents the validity of $(p * (p \mathrel{-\!\!*} q)) \to q$. This derivation essentially consists of an application of the rule $\mathbf{L}_*$ followed by an application of the rule $\mathbf{L}_{-\!*}$. In this derivation Γ denotes the formulas $R = R_1 \uplus R_2, p@R_1$ generated by the application of rule $\mathbf{L}_*$. The second premise of the application of the rule $\mathbf{L}_{-\!*}$ is derivable from an instance of the axiom $\Gamma, A \Rightarrow A, \Delta$. Note that ψ (in the $\mathbf{L}_{-\!*}$ rule) is instantiated with R_1. The first and third premise follows from the fact that $R = R_1 \uplus R_2$ reduces to $R_1 \perp R_2$ and $R = R_1 \cup R_2$ (that part of the proof is not shown above).

Next we show how to use the calculus in reasoning about the equivalence of weakest preconditions that arise in the practice of verifying the correctness of heap manipulating programs. Let p denote the weakest precondition

$$(u \hookrightarrow -) \wedge (z = 0 \triangleleft u = v \triangleright v \hookrightarrow z)$$

of the heap update $[u] := 0$ which ensures the postcondition $v \hookrightarrow z$ after assigning the value 0 to the location denoted by the variable u, where $\phi \triangleleft b \triangleright \psi$ abbreviates $(b \wedge \phi) \vee (\neg b \wedge \psi)$ (in Section 4.4 a dynamic logic extension of separation logic is introduced which generates this weakest precondition). The standard rule for backwards reasoning in [188] gives the weakest precondition $(u \mapsto -) * (u \mapsto 0 \mathrel{-\!\!*} v \hookrightarrow z)$, which we denote by p'. These preconditions are equivalent because both are the weakest.

In fact, the equivalence between the above two formulas can be expressed in quantifier-free separation logic, for which a complete axiomatization of all valid formulas has been given in [70]. In the sequent calculus we can express the equivalence of p and p' in terms of the sequent $\mathit{fun}(R) \Rightarrow (p \leftrightarrow p')@R$. Here R is an arbitrary binary relation symbol used to represent the current interpretation of the points-to relation. We abbreviate $\forall x, y, z((R(x, y) \wedge R(x, z)) \to y = z)$ by $\mathit{fun}(R)$. A proof of the above sequent amounts to proving the sequents $\mathit{fun}(R), p'@R \Rightarrow p@R$ and $\mathit{fun}(R), p@R \Rightarrow p'@R$.

Proposition 3.1.3. $\vdash \mathit{fun}(R), p@R \Rightarrow p'@R$.

Proof. This direction is easy to prove, by a case analysis whether $u = v$ holds or not. If $u = v$, then $z = 0$ and so we can easily prove $v \hookrightarrow z$ in a heap where $u \hookrightarrow 0$. Otherwise, if $u \neq v$, then $v \hookrightarrow z$ follows immediately. □

Lemma 3.1.4. $\vdash \mathit{fun}(R), p'@R \Rightarrow p@R$.

Proof. Below we present a high-level proof of the first sequent, abstracting from some basic first-order reasoning in the calculus. By an application of $\mathbf{L}_*$ to derive the sequent $\mathit{fun}(R), p'@R \Rightarrow p@R$ it suffices to derive

$$\mathit{fun}(R), R = R_1 \uplus R_2, (u \mapsto -)@R_1, (u \mapsto 0 \mathrel{-\!\!*} v \hookrightarrow z)@R_2 \Rightarrow p@R$$

for some fresh R_1 and R_2. Let $\psi(x, y)$ denote the binary formula $x = u \wedge y = 0$. Further, let Γ denote the set of formulas $\mathit{fun}(R), R = R_1 \uplus R_2, (u \mapsto -)@R_1$. By an application of the rule $\mathbf{L}_{-\!*}$ it then suffices to prove the following sequents (from

$\Gamma \Rightarrow \Delta$ we can derive $\Gamma \Rightarrow A, \Delta$ by right-weakening). First we prove $\Gamma \Rightarrow R_2 \cap \psi = \emptyset$: By the points-to rules the rooted assertion $(u \mapsto -)@R_1$ (appearing in Γ) reduces to $\exists z(R_1(u,z) \wedge \forall x, y(R_1(x,y) \rightarrow x = u \wedge y = z))$ (the forall-part of the formula is due to the 'strict' points-to which states that the domain contains u as its only location). Further, $R_2 \cap \psi = \emptyset$ logically boils down to $\neg\exists x, y(R_2(x,y) \wedge (x = u \wedge y = 0))$, that is, $\neg R_2(u,0)$, which in basic first-order logic follows from $\exists z R_1(u,z)$ and the assumptions $R = R_1 \uplus R_2$ and $\mathit{fun}(R)$.

Second, we prove $\Gamma \Rightarrow (u \mapsto 0)@\psi$: By the points-to rules $(u \mapsto 0)@\psi$ (using the expanded definition ϕ of $u \mapsto 0$ and the definition of the substitution $\phi[\psi/\hookrightarrow]$) reduces to $(u = u) \wedge (0 = 0) \wedge \forall x, y((x = u \wedge y = 0) \rightarrow (x = u \wedge y = 0))$ which is equivalent to **true**.

And, finally, we prove $\Gamma, (v \hookrightarrow z)@(R_2 \vee \psi) \Rightarrow p@R$: First note that (again, by the points-to rules)

$$((u \hookrightarrow -) \wedge (z = 0 \triangleleft u = v \triangleright v \hookrightarrow z))@R$$

reduces to

$$(\exists z R(u,z)) \wedge (z = 0 \triangleleft u = v \triangleright R(v,z))).$$

The assertion $\exists z R(u,z)$ clearly follows from the assumptions $R = R_1 \uplus R_2$ and $(u \mapsto -)@R_1$ in Γ. To prove $z = 0 \triangleleft u = v \triangleright R(v,z)$, we first reduce the assumption $(v \hookrightarrow z)@(R_2 \vee \psi)$ to $R_2(v,z) \vee (v = u \wedge z = 0)$. Now, if $v = u$ then $\neg R_2(v,z)$, because of the assumptions $\mathit{fun}(R)$, $R = R_1 \uplus R_2$ and $(u \mapsto -)@R_1$. So we have that $z = 0$. Otherwise, we have $R_2(v,z)$, and thus $R(v,z)$, because $R = R_1 \uplus R_2$. □

3.2 Soundness and completeness

We denote by $\vdash \Gamma \Rightarrow \Delta$ that there exists a proof of the sequent $\Gamma \Rightarrow \Delta$. To define $\models \Gamma \Rightarrow \Delta$, let σ denote a substitution which assigns to every binary relation symbol R of the sequent $\Gamma \Rightarrow \Delta$ a binary formula ϕ. Such a substitution σ simply replaces occurrences of $R(t,t')$ by $\phi(t,t')$, where $\sigma(R) = \phi(x,y)$. By $\models \Gamma \Rightarrow \Delta$ we then denote that $\mathfrak{A}, \rho \models \bigwedge \Gamma\sigma$ (that is, $\mathfrak{A}, \rho \models A\sigma$, for every $A \in \Gamma$) implies $\mathfrak{A}, \rho \models \bigvee \Delta\sigma$ (that is, $\mathfrak{A}, \rho \models B\sigma$, for some $B \in \Delta$), for every $\mathfrak{A}, \rho$ and every substitution σ.

In the soundness proof below we use these substitutions to instantiate the fresh binary relation symbols introduced in the rules $\mathbf{L}_*$ and $\mathbf{R}_{-*}$. Note that updating the interpretation of these symbols (as provided by $\mathfrak{A}$) would affect the semantics of the separating connectives if binary formulas would refer to these fresh binary relation symbols (note that they are only supposed not to appear in formulas of the conclusion of the rules $\mathbf{L}_*$ and $\mathbf{R}_{-*}$). See also the previous discussion about 'bookkeeping devices'.

We generalize the above notions of derivability and validity to possibly infinite Γ: $\Gamma \vdash \Delta$ indicates that $\vdash \Gamma' \Rightarrow \Delta$, for some finite $\Gamma' \subseteq \Gamma$, and $\Gamma \models \Delta$ indicates that for every substitution σ we have that $\mathfrak{A}, \rho \models \Gamma\sigma$ (that is, $\mathfrak{A}, \rho \models A\sigma$, for every $A \in \Gamma$) implies $\mathfrak{A}, \rho \models B\sigma$, for some $B \in \Delta$.

For the soundness proof we need the following substitution lemma.

Lemma 3.2.1 (Substitution lemma). *$\mathfrak{A}, Rel_{\mathfrak{A}}(\phi), \rho \models p$ if and only if $\mathfrak{A}, \rho \models p[\phi/\hookrightarrow]$, for any semi-pure formula p.*

Theorem 3.2.2 (Soundness). *We have that $\vdash \Gamma \Rightarrow \Delta$ implies $\models \Gamma \Rightarrow \Delta$.*

Proof. We prove that the rules for the separating connectives preserve validity. The points-to rules are sound because $\mathfrak{A}, Rel_{\mathfrak{A}}(\phi), \rho \models p$ if and only if $\mathfrak{A}, \rho \models p[\phi/\hookrightarrow]$, for any semi-pure formula p (note that $p[\phi/\hookrightarrow]$ is a pure first-order formula which does not depend on the heap).

$\mathbf{L}_*$: Let $\mathfrak{A}, \rho \models \Gamma\sigma$ and $\mathfrak{A}, \rho \models (p\sigma * q\sigma)@\phi\sigma$. We have to show that $\mathfrak{A}, \rho \models \bigvee \Delta\sigma$. By Lemma 3.1.2, there exist ϕ_1 and ϕ_2 such that $\mathfrak{A}, \rho \models (\phi\sigma) = \phi_1 \uplus \phi_2$, $\mathfrak{A}, \rho \models p\sigma@\phi_1$, and $\mathfrak{A}, \rho \models q\sigma@\phi_2$. Let $\sigma' = \sigma[R_1, R_2 := \phi_1, \phi_2]$. Since R_1 and R_2 are fresh and as such do not appear in $\Gamma, (p * q)@\phi$, it follows that $\mathfrak{A}, \rho \models \Gamma'\sigma'$, where $\Gamma' = \Gamma, \phi = R_1 \uplus R_2, p@R_1, q@R_2$. By the validity of the premise we thus obtain that $\mathfrak{A}, \rho \models \bigvee \Delta\sigma'$. Since R_1 and R_2 also do not appear in Δ, we conclude that $\mathfrak{A}, \rho \models \bigvee \Delta\sigma$.

$\mathbf{R}_*$: Let $\mathfrak{A}, \rho \models \Gamma\sigma$ and suppose that $\mathfrak{A}, \rho \not\models \bigvee \Delta\sigma$. From the validity of the premises it then follows that $\mathfrak{A}, \rho \models \phi\sigma = (\phi_1 \uplus \phi_2)\sigma$, $\mathfrak{A}, \rho \models p\sigma@\phi_1\sigma$, and $\mathfrak{A}, \rho \models q\sigma@\phi_2\sigma$, By Lemma 3.1.2 we conclude $\mathfrak{A}, \rho \models (p\sigma * q\sigma)@\phi\sigma$.

$\mathbf{L}_{-\!\!*}$: Let $\mathfrak{A}, \rho \models \Gamma\sigma$ and $\mathfrak{A}, \rho \models (p\sigma \mathrel{-\!\!*} q\sigma)@\phi\sigma$, and suppose that $\mathfrak{A}, \rho \not\models \bigvee \Delta\sigma$. From the validity of the first two premises it then follows that $\mathfrak{A}, \rho \models \phi\sigma \perp \psi\sigma$ and $\mathfrak{A}, \rho \models p\sigma@\psi\sigma$. By Lemma 3.1.2 again, it follows that $\mathfrak{A}, \rho \models q\sigma@(\phi\sigma \vee \psi\sigma)$. By the validity of the third premise we thus derive that $\mathfrak{A}, \rho \not\models \bigvee \Delta\sigma$, which contradicts our assumption.

$\mathbf{R}_{-\!\!*}$: Let $\mathfrak{A}, \rho \models \Gamma\sigma$ and suppose that $\mathfrak{A}, \rho \not\models \bigvee \Delta\sigma$. We have to show that $\mathfrak{A}, \rho \models (p\sigma \mathrel{-\!\!*} q\sigma)@\phi\sigma$. Let ψ be such that $\mathfrak{A}, \rho \models \psi \perp (\phi\sigma)$ and $\mathfrak{A}, \rho \models p\sigma@\psi$. Further, let R be a fresh variable and $\sigma' = \sigma[R := \psi]$. It follows that $\mathfrak{A}, \rho \models \Gamma'\sigma'$, where $\Gamma' = \Gamma, R \perp \phi, p@R$ and $\mathfrak{A}, \rho \not\models \bigvee \Delta\sigma'$. And so we derive from the validity of the premise of the rule that $\mathfrak{A}, \rho \models q\sigma@(\phi\sigma \cup \psi)$. Since ψ was arbitrarily chosen, by Lemma 3.1.2 again we conclude that $\mathfrak{A}, \rho \models (p\sigma \mathrel{-\!\!*} q\sigma)@\phi\sigma$. □

As a corollary we obtain that $\Gamma \vdash \Delta$ implies $\Gamma \models \Delta$.

Following the completeness proof of first-order logic as described in [108], it suffices to show that every consistent set of formulas is satisfiable (the so-called 'model existence theorem'). A set of formulas Γ is consistent if $\Gamma \nvdash \emptyset$. We first show that every consistent set of formulas can be extended to a maximal consistent set. To this end we assume an infinite set of 'fresh' binary relation symbols R that do not appear in Γ. We construct for any consistent set Γ a maximal consistent extension Γ^∞, assuming an enumeration of all formulas A (which also covers all first-order formulas). We define $\Gamma_0 = \Gamma$ and Γ_{n+1} satisfies the general rule: if $\Gamma_n, A_n \nvdash \emptyset$ then $\Gamma_n \cup \{A_n\} \subseteq \Gamma_{n+1}$, otherwise $\Gamma_{n+1} = \Gamma_n$. Additionally, in case A_n is added and A_n is of the form $\exists x A$ or a rooted assertion $(p * q)@\phi$ or $\neg(p \mathrel{-\!\!*} q)@\phi$, we also include corresponding *witnesses* in Γ_{n+1}:

- If A_n is of the form $\exists x A$ we additionally add $A(y)$, where $A(y)$ results from replacing all free occurrences of x in A by the fresh variable y which does not appear in Γ_n.

Note that $A(y)$ can indeed be added consistently because from $\Gamma_n, A(y) \vdash \emptyset$ we would derive $\Gamma_n, \exists x A \vdash \emptyset$, which contradicts the assumption that $\Gamma_n, \exists x A \nvdash \emptyset$.

- If A_n is of the form $(p * q)@\phi$ we additionally add the formulas $\phi = R_1 \uplus R_2, R_1 \perp R_2, p@R_1$, and $q@R_2$, where R_1 and R_2 are fresh (e.g., not appearing in Γ_n).

  Note that these formulas can indeed be added consistently because from $\Gamma_n, \phi = R_1 \uplus R_2, R_1 \perp R_2, p@R_1, q@R_2 \vdash \emptyset$ we would derive $\Gamma_n, (p * q)@\phi \vdash \emptyset$ (by rule $\mathbf{L}_*$).

- If A_n is of the form $\neg(p \mathrel{-\!\!*} q)@\phi$ (which is equivalent to $\neg((p \mathrel{-\!\!*} q)@\phi)$) we additionally add the formulas $R \perp \phi, p@R(x, y)$, and $\neg q@(\phi \vee R)$, where R is fresh (e.g., not appearing in Γ_n).

  Note that these formulas can indeed be added consistently because from $\Gamma_n, R \perp \phi, p@R(x, y), \neg q@(\phi \vee R) \vdash \emptyset$ we would derive $\Gamma_n \vdash (p \mathrel{-\!\!*} q)@\phi$ (by rule $\mathbf{R}_{-*}$), which contradicts the assumption that $\Gamma_n, \neg(p \mathrel{-\!\!*} q)@\phi \nvdash \emptyset$.

We define $\Gamma^\infty = \bigcup_n \Gamma_n$. By construction Γ^∞ is maximal consistent. Given a maximal consistent set of formulas Γ, let $\mathfrak{A}_\Gamma = (D, I)$, where D is the set of equivalences classes $[x] = \{y \mid x = y \in \Gamma\}$. For any relation symbol R (excluding the points-to relation $\hookrightarrow$) we define

$$\mathcal{I}(R)([x_1], \ldots, [x_n]) = \mathbf{true} \text{ if and only if } R(x_1, \ldots, x_n) \in \Gamma.$$

Given a maximal consistent set of formulas Γ and the structure $\mathfrak{A}_\Gamma = (D, I)$, a corresponding valuation ρ assigns to every variable x an equivalence class $[x]$. However, in the sequel we will represent such a valuation by a *substitution* s which simply assigns to each variable a variable. The value $\mathcal{I}_s(x)$ of a variable x then is given by the equivalence class $[s(x)]$ of the variable $s(x)$.

Given a substitution s and formula A (of the sequent calculus) we denote by ts and As the result of replacing every free occurrence of a (first-order) variable x in t and A by $s(x)$, respectively. Note that $(p@\phi)s = ps@\phi$, because the meaning of $p@\phi$ does not depend on the free variables x and y of the binary formula $\phi(x, y)$.

Given a maximal consistent set of formulas Γ and the structure $\mathfrak{A}_\Gamma = (D, \mathcal{I})$, it follows that $\mathcal{I}_s(x) = [xs]$, for every variable x and substitution s.

Lemma 3.2.3. *Given a maximal consistent set of formulas Γ and the structure $\mathfrak{A}_\Gamma = (D, \mathcal{I})$, we have $\mathfrak{A}, s \models A$ if and only if $As \in \Gamma$, for every formula A and substitution s.*

Proof. The proof proceeds by induction on the following well-founded ordering $A < B$ on formulas of the sequent calculus: Let $\#A = (n, m)$, where n denotes the number of occurrences of the separating connectives and the @-connective of A and m denotes the number of occurrences of the (standard) first-order logical operations of A. Then $A < B$ if $\#A < \#B$, where the latter denotes the lexicographical ordering on $\mathbb{N} \times \mathbb{N}$ (w.r.t. the standard 'smaller than' ordering on the natural numbers). We treat the following main cases (for notational convenience $\mathfrak{A}$ denotes the structure $\mathfrak{A}_\Gamma$).

- For any semi-pure formula p (that is, which does not involve occurrences of the separating connectives) we have:
  $\mathfrak{A}, s \models p@\phi$ if and only if (by definition)
  $\mathfrak{A}, Rel_{\mathfrak{A}}(\phi), s \models p$ if and only if (substitution lemma 3.2.1)
  $\mathfrak{A}, s \models p[\phi/ \hookrightarrow]$ if and only if (induction hypothesis)
  $(p[\phi/ \hookrightarrow])s \in \Gamma$ if and only if
  $(p@\phi)s \in \Gamma$.

  Note that by an application of the points-to rules $(p[\phi/ \hookrightarrow])s \in \Gamma$ implies $\Gamma \vdash (p@\phi)s$, and so $(p@\phi)s \in \Gamma$, by the maximal consistency of Γ. On the other hand, let $(p@\phi)s \in \Gamma$ and assume $(p[\phi/ \hookrightarrow])s \notin \Gamma$, that is, $(\neg p[\phi/ \hookrightarrow])s \in \Gamma$, by the maximal consistency of Γ. By the points-to rules it then follows that $\Gamma \vdash (\neg p@\phi)s$, which contradicts the consistency of Γ.

- Let $\mathfrak{A}, s \models A$, where A denotes the formula $(p * q)@\phi$. By Lemma 3.1.2 there exist ϕ_1 and ϕ_2 such that $\mathfrak{A}, s \models \phi = \phi_1 \uplus \phi_2$, $\mathfrak{A}, s \models p@\phi_1$ and $\mathfrak{A}, s \models q@\phi_2$. From the induction hypothesis it follows that $ps@\phi_1, qs@\phi_2, \phi = \phi_1 \uplus \phi_2 \in \Gamma$ (note that the first-order formula $\phi = \phi_1 \uplus \phi_2$ does not contain free variables, and thus is not affected by the substitution s). So we derive by rule $\mathbf{R}_*$ that $\Gamma \vdash (ps * qs)@\phi$. By maximal consistency of Γ, we then conclude that $(ps * qs)@\phi \in \Gamma$, that is, $As \in \Gamma$.

  On the other hand, let $As \in \Gamma$. That is, $(ps * qs)@\phi \in \Gamma$. By the construction of Γ we have $\phi = R_1 \uplus R_2, ps@R_1, qs@R_2 \in \Gamma$, for some witnesses R_1 and R_2. By the induction hypothesis it then follows that $\mathfrak{A}, s \models p@R_1$ and $\mathfrak{A}, s \models p@R_2$. Further, the induction hypothesis gives $\mathfrak{A}, s \models \phi = R_1 \uplus R_2$ (again, note that the formula $\phi = R_1 \uplus R_2$ has no free variables, and thus is not affected by the substitution s). We conclude by Lemma 3.1.2 that $\mathfrak{A}, s \models (p * q)@\phi$.

- Let $\mathfrak{A}, s \models A$, where A denotes the formula $(p \mathrel{-\!\!*} q)@\phi$. Suppose $As \notin \Gamma$. By the maximal consistency of Γ, we then have $\neg(ps \mathrel{-\!\!*} qs)@\phi \in \Gamma$. By construction $R \perp \phi, ps@R, \neg qs@(\phi \vee R) \in \Gamma$, for some witness R, which contradicts $\mathfrak{A}, s \models (p \mathrel{-\!\!*} q)@\phi$ (after application of the induction hypothesis and using Lemma 3.1.2 again).

  On the other hand, let $As \in \Gamma$. To show that $\mathfrak{A}, s \models (p \mathrel{-\!\!*} q)@\phi$, let $\mathfrak{A}, s \models \phi \perp \psi$ and $\mathfrak{A}, s \models p@\psi$, for some binary formula ψ. By the induction hypothesis we have that $\phi \perp \psi, ps@\psi \in \Gamma$. Suppose that $qs@(\phi \vee \psi) \notin \Gamma$, that is $\neg qs@(\phi \vee \psi) \in \Gamma$ (Γ is maximal consistent), and thus $\Gamma, qs@(\phi \vee \psi) \vdash \emptyset$. Applying rule $\mathbf{L}_{-\!\!*}$ we then derive $\Gamma, (ps \mathrel{-\!\!*} qs)@\phi \vdash \emptyset$, which contradicts the consistency of Γ ($(ps \mathrel{-\!\!*} qs)@\phi \in \Gamma$). So we have that $qs@(\phi \vee \psi) \in \Gamma$, that is, $\mathfrak{A}, s \models q@(\phi \vee \psi)$, by the induction hypothesis. Since ψ is chosen arbitrarily, it follows by Lemma 3.1.2 that $\mathfrak{A}, s \models (p \mathrel{-\!\!*} q)@\phi$.

- Let A be a formula $p@\phi$, where p denotes a semi-pure formula. Let $\mathcal{R} = Rel_{\mathfrak{A}}(\phi)$. We then have:
  $\mathfrak{A}, s \models p@\phi$ iff (by definition)
  $\mathfrak{A}, \mathcal{R}, s \models p$ iff (straightforward induction on p)

$\mathfrak{A}, s \models p[\phi/\hookrightarrow]$ iff (induction hypothesis for $p[\phi/\hookrightarrow]$)
$ps[\phi/\hookrightarrow] \in \Gamma$ iff (by the points-to rules)
$ps@\phi \in \Gamma$.

Note that applying the substitution s to $p@\phi$ and $p[\phi/\hookrightarrow]$ results in $ps@\phi$ and $ps[\phi/\hookrightarrow]$. □

The downward Löwenheim–Skolem property follows. It should be noted that we cannot remove from the constructed model the binary relation symbols which are introduced as witnesses, as these determine the notion of first-order definability.

Theorem 3.2.4 (Completeness)**.** *We have that* $\Gamma \models \Delta$ *implies* $\Gamma \vdash \Delta$.

Compactness follows. We thus derive (by Lindström's theorem [210]) that this interpretation of separation logic is as expressive as first-order logic.

3.3 Natural deduction

The sequent calculus introduced and proven sound and complete in the previous sections was defined in terms of three syntactic categories: the pure first-order formulas, the separation logic formulas, and the rooted formulas closed under propositional connectives and quantification. In this section, we investigate what happens when we consider only a single syntactic category of formulas: those of separation logic closed under the @-connective. We thus introduce the *extended separation logic* formulas by the following abstract grammar:

$$\phi, \psi ::= \bot \mid (x \doteq y) \mid C(x_1, \ldots, x_n) \mid (\phi \to \psi) \mid (\forall x \phi) \mid (\phi * \psi) \mid (\phi \mathrel{-\!\!*} \psi) \mid (\phi @ \psi)$$

The new @-connective can be understood as a binder of $\hookrightarrow$, in the sense that it lets the interpretation of ψ determine the denotation of $\hookrightarrow$ with respect to which the formula ϕ is interpreted. Revisiting Definition A.1.6 (Free and bound variables), we need to add the following clauses:

- $FV(\phi @ \psi) = FV(\phi) \cup (FV(\psi) \setminus \{x, y\})$, and
- $BV(\phi @ \psi) = BV(\phi) \cup BV(\psi) \cup \{x, y\}$.

By abuse of notation, we may think of @ as a *let binding* in the following sense:

$$(\phi @ \psi) = \textbf{let} \hookrightarrow := (\lambda x \lambda y.\ \psi)\ \textbf{in}\ \phi$$

since the interpretation of $\hookrightarrow$ becomes 'bound' in ϕ by the let binding, and the free variables x and y in ψ are 'captured' by the abstraction. Further, for technical convenience, we also have second-order binary variables $R, R_1, \ldots$, but it is not possible to quantify over such second-order variables.

We now give an extension of the natural deduction calculus for classical logic in the following way. The objects of this proof system, called **RSL**, are the above formulas of extended separation logic. Derivability in this proof system is denoted by $\vdash$. We have the usual axioms and proof rules of natural deduction, and add the axioms and proof rules of Figure 3.2.

We have the following example proofs using the above proof system.

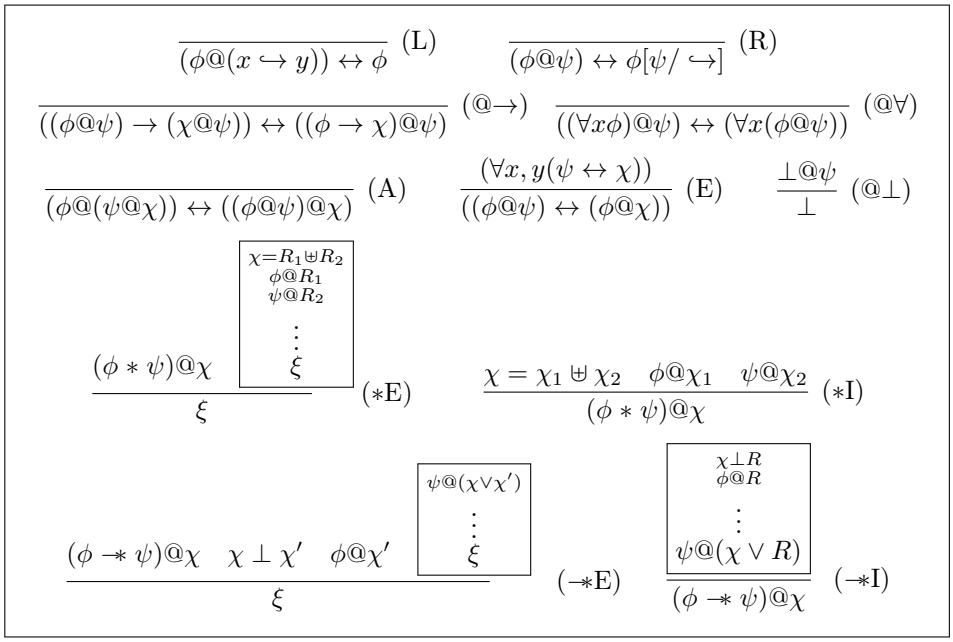

Figure 3.2: Natural deduction system for extended separation logic. In the rule (R) the formula ϕ is semi-pure. In the rule ($*$E), R_1, R_2 do not occur in ξ. In the rule ($-*$I), R does not occur in ϕ, ψ, χ.

Proposition 3.3.1. $\vdash \mathbf{emp}@\bot$.

Proof. Recall that **emp** abbreviates $\forall x, y. \neg(x \hookrightarrow y)$. We apply ($@\forall$) and ($\forall$I) twice, so now it suffices to show $(\neg(x \hookrightarrow y))@\bot$. The logical negation abbreviates $(x \hookrightarrow y) \to \bot$, so we apply ($@\to$) and by ($\to I$) we may assume $(x \hookrightarrow y)@\bot$. From (R) and the new premise we infer $\bot$, and hence by ($\bot$E) we have $\bot@\bot$. □

Proposition 3.3.2. $\vdash \phi * \psi \to \psi * \phi$.

Proof. By (L), it suffices to show $(\phi * \psi \to \psi * \phi)@(x \hookrightarrow y)$, and by ($@\to$) we may assume $(\phi * \psi)@(x \hookrightarrow y)$ and show $(\psi * \phi)@(x \hookrightarrow y)$. We do this by ($*$E), where we assume $(x \hookrightarrow y) = R_1 \uplus R_2$ for fresh R_1, R_2, and $\phi@R_1$ and $\psi@R_2$. It is easy to see we also have $(x \hookrightarrow y) = R_2 \uplus R_1$, and hence by ($*$I) we have $(\psi * \phi)@(x \hookrightarrow y)$, completing the proof. □

Proposition 3.3.3. $\vdash \phi * (\psi * \chi) \leftrightarrow (\phi * \psi) * \chi$.

Proof. We have two directions (classical conjunction). We show $\phi * (\psi * \chi) \to (\phi * \psi) * \chi$ first. By (L) we wrap it under the trivial root, and by ($@\to$) we thus assume $(\phi * (\psi * \chi))@(x \hookrightarrow y)$. We use ($*$E) twice, to obtain $(x \hookrightarrow y) = R_1 \uplus R_2$ and $R_2 = R_3 \uplus R_4$, so that $\phi@R_1$, $\psi@R_3$, $\chi@R_4$. We have $R_1 \perp R_3$, so $R_1 \uplus R_3$ is defined. Further, we have $(R_1 \uplus R_3) \perp R_4$ so $(R_1 \uplus R_3) \uplus R_4$ is also defined. The latter is equivalent to $(x \hookrightarrow y)$. Now by ($*$I) twice, we obtain $(\phi * \psi)@(R_1 \uplus R_3)$ and $((\phi * \psi) * \chi)@(x \hookrightarrow y)$. The other direction goes in a similar way. □

Proposition 3.3.4. $\vdash (\mathbf{emp}@\phi) \leftrightarrow (\forall x, y. \phi \to \bot)$.

Proof. Two classical directions:

- Assume $\mathbf{emp}@\phi$, and take arbitrary x_0, y_0 and assume $\phi(x_0, y_0)$. We need to show $\bot$. Unfold the abbreviation **emp** and we have $(\forall x, y. \neg(x \hookrightarrow y))@\phi$. Specializing this assumption with x_0 and y_0, we obtain $\neg(x_0 \hookrightarrow y_0)@\phi$. To show $\bot$ it is sufficient to show $\bot@\phi$. We apply our assumption, so it suffices to show $(x_0 \hookrightarrow y_0)@\phi$. But that follows from our assumption $\phi(x_0, y_0)$.

- Assume $(\forall x, y. \phi \to \bot)$. Unfold the abbreviation **emp**, and take arbitrary x_0, y_0, and assume $(x_0 \hookrightarrow y_0)@\phi$. We need to show $\bot@\phi$, but it suffices to show $\bot$. From our assumption, we know $\phi(x_0, y_0)$ holds. But that contradicts our earliest assumption. □

Proposition 3.3.5. $\vdash \phi * \mathbf{emp} \leftrightarrow \phi$.

Proof. There are two directions (classically).

- We assume $(\phi * \mathbf{emp})@(x \hookrightarrow y)$ and need to show $\phi@(x \hookrightarrow y)$. From our assumption we have $\phi@R_1$ and $\mathbf{emp}@R_2$ and $(x \hookrightarrow y) = R_1 \uplus R_2$. Since $\mathbf{emp}@R_2$ we know $R_2 = \bot$ (by previous proposition), and hence $(x \hookrightarrow y) = R_1$. So by $\phi@R_1$ we then have $\phi@(x \hookrightarrow y)$.

- We assume $\phi @ (x \hookrightarrow y)$ and need to show $(\phi * \mathbf{emp}) @ (x \hookrightarrow y)$. To show the latter it suffices to show $(x \hookrightarrow y) = (x \hookrightarrow y) \uplus \epsilon$ where $\epsilon = \bot$. Clearly the disjoint union of those two relations is defined, and we already have $\phi(x \hookrightarrow y)$. Also we have $\mathbf{emp} @ \epsilon$ (by our previous proposition). □

Proposition 3.3.6. *The following holds:*

- $\vdash (\phi \vee \psi) * \chi \leftrightarrow \phi * \chi \vee \psi * \chi$,
- $\vdash (\phi \wedge \psi) * \chi \to \phi * \chi \wedge \psi * \chi$,
- $\vdash (\exists x \phi(x)) * \psi \leftrightarrow \exists x (\phi(x) * \psi)$,
- $\vdash (\forall x \phi(x)) * \psi \to \forall x (\phi(x) * \psi)$,
- $\vdash \phi * (\phi \mathrel{-\!\!*} \psi) \to \psi$.

Proof. Left as exercises for the reader, as their proofs are not long. The proofs are also formalized, see Appendix D. □

Note that distributivity of conjunction (universal quantification) and separating conjunction only works in one direction.

Proposition 3.3.7. *The following holds:*

- $\vdash \blacksquare \phi \to \phi$,
- $\vdash \blacksquare \phi \to (\phi @ \psi)$,
- $\vdash \blacksquare(\phi \to \psi) \to \phi @ \chi \to \psi @ \chi$,
- $\vdash \blacksquare(\phi \to \phi') \to \blacksquare(\psi \to \psi') \to \phi * \psi \to \phi' * \psi'$,
- $\vdash (x \hookrightarrow y) \leftrightarrow (x \mapsto y) * \top$,
- $\vdash \neg(x \hookrightarrow -) \to (((x \mapsto y) \mathrel{-\!\!*} (x \mapsto y) * \phi) \leftrightarrow \phi)$.

Proof. Left as exercises for the reader, as their proofs are not long. The proofs are also formalized, see Appendix D. □

Proposition 3.3.8. *If $\phi @ \psi$ is deducible for every ψ, then $\vdash \blacksquare \phi$.*

Proof. If $\phi @ \psi$ is deducible for every heap description, then ϕ cannot depend on the heap and as such it holds in every heap. The proof is formalized, see Appendix D. □

Proposition 3.3.9. *If $\phi \leftrightarrow \psi$ is deducible, and we have a deduction of χ from premises Γ then we may replace any occurrence of ϕ by ψ in any of the premises in Γ and the conclusion χ.*

We again investigate the weakest precondition of the postcondition $(v \hookrightarrow z)$ and the program $[u] := 0$. As before, let p denote the weakest precondition $(u \hookrightarrow -) \wedge (z = 0 \triangleleft u = v \triangleright v \hookrightarrow z)$, where again $\phi \triangleleft b \triangleright \psi$ abbreviates $(b \wedge \phi) \vee (\neg b \wedge \psi)$. Let p' denote the weakest precondition $(u \mapsto -) * (u \mapsto 0 \mathrel{-\!\!*} v \hookrightarrow z)$.

Proposition 3.3.10. $\vdash p \to p'$.

Proof. The proof can be formalized, see Appendix D. □

Lemma 3.3.11. $\vdash p' \to p$.

Proof. The proof can be formalized, see Appendix D. □

Note that it is not needed to assume functionality of the heap (since the separating implication speaks of all disjoint relational heaps, including those that satisfy functionality).

3.4 Soundness and completeness

We shall give a general relational semantics to these extended separation logic formulas, but to do so we need to construct the satisfaction relation in two stages.

Definition 3.4.1. A *general relational structure* $\mathfrak{H} = (\mathfrak{A}, H)$ consists of a structure $\mathfrak{A} = (A, \mathcal{I})$ with domain A and a set of binary relations $H \subseteq \mathcal{P}(A \times A)$.

In the first stage, we give a general relational semantics **GRSL** which is suitable for interpreting the let binding. We shall use valuations ρ that assign both the first-order and binary second-order variables. The binary second-order variables are not constrained and ranges over *arbitrary* binary relations between elements of the domain of the underlying structure. Also the relation $\mathcal{R}$ is not constrained and ranges over arbitrary relations, whereas in the interpretation of the separating connectives quantification *is* restricted to the set of relations of the general relational structure.

Definition 3.4.2 (Satisfaction relation)**.** Given a general relational structure $\mathfrak{H} = (\mathfrak{A}, H)$ with domain A and interpretation $\mathcal{I}$, a valuation ρ of $\mathfrak{A}$, a binary relation $\mathcal{R} \subseteq A \times A$, and an extended separation logic formula ϕ. The satisfaction relation $\mathfrak{H}, \mathcal{R}, \rho \models^{\mathbf{GRSL}} \phi$ is defined inductively on the structure of ϕ:

- $\mathfrak{H}, \mathcal{R}, \rho \models^{\mathbf{GRSL}} \bot$ never holds,
- $\mathfrak{H}, \mathcal{R}, \rho \models^{\mathbf{GRSL}} (x \doteq y)$ iff $\rho(x) = \rho(y)$,
- $\mathfrak{H}, \mathcal{R}, \rho \models^{\mathbf{GRSL}} (x \hookrightarrow y)$ iff $(\rho(x), \rho(y)) \in \mathcal{R}$,
- $\mathfrak{H}, \mathcal{R}, \rho \models^{\mathbf{GRSL}} R(x_1, x_2)$ iff $(\rho(x_1), \rho(x_2)) \in \rho(R)$,
- $\mathfrak{H}, \mathcal{R}, \rho \models^{\mathbf{GRSL}} C(x_1, \ldots, x_n)$ iff $(\rho(x_1), \ldots, \rho(x_n)) \in C^{\mathcal{I}}$,
- $\mathfrak{H}, \mathcal{R}, \rho \models^{\mathbf{GRSL}} \phi \to \psi$ iff $\mathfrak{H}, \mathcal{R}, \rho \models^{\mathbf{GRSL}} \phi$ implies $\mathfrak{H}, \mathcal{R}, \rho \models^{\mathbf{GRSL}} \psi$,
- $\mathfrak{H}, \mathcal{R}, \rho \models^{\mathbf{GRSL}} \forall x \phi$ iff $\mathfrak{H}, \mathcal{R}, \rho[x := a] \models^{\mathbf{GRSL}} \phi$ for every $a \in A$,
- $\mathfrak{H}, \mathcal{R}, \rho \models^{\mathbf{GRSL}} \phi * \psi$ iff $\mathfrak{H}, \mathcal{R}_1, \rho \models^{\mathbf{GRSL}} \phi$ and $\mathfrak{H}, \mathcal{R}_2, \rho \models^{\mathbf{GRSL}} \psi$ for some $\mathcal{R}_1, \mathcal{R}_2 \in H$ such that $\mathcal{R} = \mathcal{R}_1 \cup \mathcal{R}_2$ and $\mathcal{R}_1 \perp \mathcal{R}_2$,

- $\mathfrak{H}, \mathcal{R}, \rho \models^{\mathbf{GRSL}} \phi \mathrel{-\!\!*} \psi$ iff $\mathfrak{H}, \mathcal{R}', \rho \models^{\mathbf{GRSL}} \phi$ implies $\mathfrak{H}, \mathcal{R} \cup \mathcal{R}', \rho \models^{\mathbf{GRSL}} \psi$ for every $\mathcal{R}' \in H$ such that $\mathcal{R} \perp \mathcal{R}'$,
- $\mathfrak{H}, \mathcal{R}, \rho \models^{\mathbf{GRSL}} \phi @ \psi$ iff $\mathfrak{H}, \mathcal{R}', \rho \models^{\mathbf{GRSL}} \phi$ for $\mathcal{R}' = Rel_{\mathfrak{H},\mathcal{R},\rho}(\psi)$.

where $Rel_{\mathfrak{H},\mathcal{R},\rho}(\psi)$ denotes $\{\langle d_x, d_y\rangle \mid \mathfrak{H}, \mathcal{R}, \rho[x, y := d_x, d_y] \models^{\mathbf{GRSL}} \psi\} \subseteq A \times A$.

Note that if one takes H to be the set of all finite relations and restrict to the (non-extended) formulas of separation logic, we obtain weak relational separation logic, and similarly if one takes H to be the set of all relations, we obtain full relational separation logic.

For the second stage, we define the following class of general relational structures. This class captures *semantic comprehension* by means of a closure condition on the set of relations, that constraints the range of second-order quantifiers implicitly used for giving semantics to the separating connectives, in the sense that every binary relation that can be expressed by an extended formula of separation logic must be in the set of binary relations of the general structure too.

Definition 3.4.3. A *comprehensive relational structure* $\mathfrak{H} = (\mathfrak{A}, H)$ is a general relational structure such that for every relation $\mathcal{R} \in H$, valuation ρ of $\mathfrak{A}$ where $\rho(R) \in H$ for every second-order variable R, and extended formula of separation logic ψ, we have $Rel_{\mathfrak{H},\mathcal{R},\rho}(\psi) \in H$.

We then define our intended semantics as follows.

Definition 3.4.4 (Satisfaction relation)**.** Given a comprehensive relational structure $\mathfrak{H} = (\mathfrak{A}, H)$, a relation $\mathcal{R} \in H$, and valuation ρ of $\mathfrak{A}$ where $\rho(R) \in H$ for every second-order variable R, we define the satisfaction relation $\mathfrak{H}, \mathcal{R}, \rho \models^{\mathbf{RSL}} \phi$ with the same conditions as given before in Definition 3.4.2.

Notice how in this satisfaction relation, compared to the previous stage, the relation $\mathcal{R}$ and the value of second-order variables are constrained to be in H. Since the semantic comprehension condition imposed on comprehensive relational structures is expressed using the first stage semantics, there is no circularity in the condition that $\mathcal{R}$ (and the value of any second-order variable) needs to be in H.

Again, note that if one takes H to be the set of all finite relations, to obtain weak relational separation logic, we may fail to make a comprehensive relational structure out of it: there is a formula, such as $\top$, that express that infinitely many locations are related to a value, but that contradicts the requirement that we restrict to finite relations. There is no problem for structures with finite domain, since there weak relational separation logic and full relational separation logic coincide. If one takes H to be the set of all relations on a structure with infinite domain, we obtain full relational separation logic, which is also trivially a comprehensive relational structure. It does seem possible to construct a comprehensive relational structure out of a set H consisting of all finite and cofinite relations, but we leave that structure for the reader to investigate further.

From the definition above, we can see that the formula ψ in the let binding $(\phi @ \psi)$ is a type with free variables among x and y. In particular, we have the properties (L)eft-root, (R)ight-root, (A)ssociative-root, and (E)quivalent-root:

Lemma 3.4.5 (Soundness I)**.**

(L) $\mathfrak{H}, \mathcal{R}, \rho \models^{\mathbf{RSL}} (\phi @ (x \hookrightarrow y)) \leftrightarrow \phi$,

(R) $\mathfrak{H}, \mathcal{R}, \rho \models^{\mathbf{RSL}} (\phi @ \psi) \leftrightarrow \phi[\psi/ \hookrightarrow]$ *where* ϕ *is semi-pure,*

(A) $\mathfrak{H}, \mathcal{R}, \rho \models^{\mathbf{RSL}} (\phi @ (\psi @ \chi)) \leftrightarrow ((\phi @ \psi) @ \chi)$,

(E) $\mathfrak{H}, \mathcal{R}, \rho \models^{\mathbf{RSL}} (\forall x, y (\psi \leftrightarrow \chi)) \rightarrow ((\phi @ \psi) \leftrightarrow (\phi @ \chi))$.

Proof. (L) Suppose $\mathfrak{H}, \mathcal{R}, \rho \models^{\mathbf{RSL}} (\phi @ (x \hookrightarrow y))$ holds, then we know that also $\mathfrak{H}, \mathcal{R}, \rho \models^{\mathbf{RSL}} \phi$ holds, since $Rel_{\mathfrak{H},\mathcal{R},\rho}(x \hookrightarrow y) = \mathcal{R}$. The converse is similar.

(R) Suppose $\mathfrak{H}, \mathcal{R}, \rho \models^{\mathbf{RSL}} (\phi @ \psi)$ holds, then by definition we know that also $\mathfrak{H}, \mathcal{R}', \rho \models^{\mathbf{RSL}} \phi$ holds for $Rel_{\mathfrak{H},\mathcal{R},\rho}(\psi) = \mathcal{R}'$. Since ϕ is semi-pure, in the evaluation of ϕ we never change $\mathcal{R}'$. Hence we can replace $(z \hookrightarrow w)$ by $\psi(z, w)$ in ϕ and we have that $\mathfrak{H}, \mathcal{R}, \rho \models^{\mathbf{RSL}} \phi[\psi/ \hookrightarrow]$ holds. Note how the free variables of ψ (other than x, y which are replaced by the variables z, w) are still evaluated with respect to ρ. The converse is similar.

(A) Suppose $\mathfrak{H}, \mathcal{R}, \rho \models^{\mathbf{RSL}} (\phi @ (\psi @ \chi))$ holds, then we know that $\mathfrak{H}, \mathcal{R}', \rho \models^{\mathbf{RSL}} \phi$ holds for $Rel_{\mathfrak{H},\mathcal{R},\rho}(\psi @ \chi) = \mathcal{R}'$. We then also know that for every pair $\langle d_x, d_y \rangle \in \mathcal{R}'$ we have that $\mathfrak{H}, \mathcal{R}'', \rho[x := d_x, y := d_y] \models^{\mathbf{RSL}} \psi$ where we take $Rel_{\mathfrak{H},\mathcal{R},\rho[x:=d_x,y:=d_y]}(\chi) = \mathcal{R}''$. Note that we have $\mathcal{R}'' = Rel_{\mathfrak{H},\mathcal{R},\rho}(\chi)$, since x and y are bound, and thus we have $\mathfrak{H}, \mathcal{R}'', \rho \models^{\mathbf{RSL}} \phi @ \psi$ since we have that $\mathfrak{H}, \mathcal{R}''', \rho \models^{\mathbf{RSL}} \phi$ where $Rel_{\mathfrak{H},\mathcal{R}'',\rho}(\psi) = \mathcal{R}'''$, from $\mathfrak{H}, \mathcal{R}', \rho \models^{\mathbf{RSL}} \phi$ and knowing that $\mathcal{R}' = \mathcal{R}'''$.

(E) Similar to the cases before. □

The following properties describe the interactions between connectives:

Lemma 3.4.6 (Soundness II)**.**

(@⊥) $\mathfrak{H}, \mathcal{R}, \rho \models^{\mathbf{RSL}} (\bot @ \psi) \rightarrow \bot$,

(@→) $\mathfrak{H}, \mathcal{R}, \rho \models^{\mathbf{RSL}} ((\phi @ \psi) \rightarrow (\chi @ \psi)) \leftrightarrow ((\phi \rightarrow \chi) @ \psi)$,

(@∀) $\mathfrak{H}, \mathcal{R}, \rho \models^{\mathbf{RSL}} ((\forall x \phi) @ \psi) \leftrightarrow (\forall x (\phi @ \psi))$ *where* x *is not free in* ψ,

(∗E) $\mathfrak{H}, \mathcal{R}, \rho \models^{\mathbf{RSL}} ((\phi * \psi) @ \chi) \wedge (\chi = R_1 \uplus R_2 \wedge (\phi @ R_1) \wedge (\psi @ R_2) \rightarrow \xi) \rightarrow \xi$ *where* R_1, R_2 *do not occur in* ξ,

(∗I) $\mathfrak{H}, \mathcal{R}, \rho \models^{\mathbf{RSL}} \chi = \chi_1 \uplus \chi_2 \wedge (\phi @ \chi_1) \wedge (\psi @ \chi_2) \rightarrow ((\phi * \psi) @ \chi)$,

(−∗E) $\mathfrak{H}, \mathcal{R}, \rho \models^{\mathbf{RSL}} ((\phi \mathrel{-\!\!*} \psi) @ \chi) \wedge \chi \perp \chi' \wedge (\phi @ \chi') \wedge ((\psi @ (\chi \vee \chi') \rightarrow \xi)) \rightarrow \xi$,

(−∗I) $\mathfrak{H}, \mathcal{R}, \rho \models^{\mathbf{RSL}} (\chi \perp R \wedge (\phi @ R) \rightarrow (\psi @ (\chi \vee R))) \rightarrow ((\phi \mathrel{-\!\!*} \psi) @ \chi)$
where R *does not occur in* ϕ, ψ, χ.

We also have the following derived properties:

Corollary 3.4.7.

- $\mathfrak{A}, \mathcal{R}, \rho \models^{\mathbf{RSL}} (\phi @ \psi) \leftrightarrow \phi$ *where* ϕ *is a pure formula,*
- $\mathfrak{A}, \mathcal{R}, \rho \models^{\mathbf{RSL}} ((\phi @ \psi) \wedge (\chi @ \psi)) \leftrightarrow ((\phi \wedge \chi) @ \psi)$,
- $\mathfrak{A}, \mathcal{R}, \rho \models^{\mathbf{RSL}} ((\phi @ \psi) \vee (\chi @ \psi)) \leftrightarrow ((\phi \vee \chi) @ \psi)$,
- $\mathfrak{A}, \mathcal{R}, \rho \models^{\mathbf{RSL}} ((\exists x \phi) @ \psi) \leftrightarrow (\exists x (\phi @ \psi))$ *where* x *is not free in* ψ,
- $\mathfrak{A}, \mathcal{R}, \rho \models^{\mathbf{RSL}} \blacksquare \phi \rightarrow (\phi @ \chi)$.

The proof system **RSL** is sound with respect to the semantics **RSL**.

Lemma 3.4.8 (Soundness)**.** $\Gamma \vdash^{\mathbf{RSL}} \phi$ *implies* $\Gamma \models^{\mathbf{RSL}} \phi$.

Proof. By induction on the structure of a deduction. Note that the semantics of **RSL** follows that of classical logic for all logical connectives, hence the proof rules involving classical connectives are sound via their usual argument. For the additional axioms and proof rules, see Lemma 3.4.5 and Lemma 3.4.6. □

We now investigate a proof reduction technique. Every deduction in the natural deduction proof system can be reduced to a deduction with only rooted formulas of a particular shape, by introducing additional fresh binary variables. The shape of rooted formulas we wish to obtain are precisely those that can be worked with in our previous sequent calculus, i.e. rooted assertions with a pure right-side. The purpose of the procedure is as follows. Suppose we are given a set of premises Γ and a conclusion ϕ. Our goal is to obtain an equisatisfiable set of premises Γ' and conclusion ϕ' in which every occurrence of a rooted formula does not have any roots occurring the left, has a first-order formula on the right, and is not nested under separating connectives. Such equi-satisfiable set of premises then allows us to obtain a proof using our previous sequent calculus, and that proof is straightforwardly mapped to a proof in natural deduction.

We sketch out the following provability-preserving and semantics-preserving operations on the premises and conclusion:

1. For all formula occurrences $\psi @ \chi$ that are nested on the left under a top-level root $(\ldots(\psi @ \chi)\ldots) @ \xi$, we 'push down' the outer root until it reaches the nested root, and we perform an associative root swap so that from $(\ldots(\psi @ \chi)\ldots) @ \xi$ we obtain $(\ldots(\psi @ (\chi @ \xi))\ldots)$. For the classical connectives this 'pushing down' is straightforward. For $(x \hookrightarrow y)$, we can simply substitute using the right root rule. For an occurrence that is a separating conjunction $(\psi_1 * \psi_2) @ \xi$ we introduce fresh binary variables R_1, R_2, replace the occurrence with $(\psi_1 @ R_1) \wedge (\psi_2 @ R_2)$, add the premise $\xi = R_1 \uplus R_2$, and proceed with pushing down in the occurrences $\psi_1 @ R_1$ and $\psi_2 @ R_2$. A similar construction happens for separating implication, but we leave one fresh variable open for interpretation. We repeat this step until no longer we have roots nested under the left.

2. For each formula occurrence $\psi @ \chi$ that does not occur on the left under a root and where χ is not first-order, in some formula of Γ or in the conclusion ϕ, we introduce a fresh binary variable R. We add a premise on the top level $(\forall x, y.\, R(x, y) \leftrightarrow \chi)$, and replace χ in the occurrence $\psi @ \chi$ by $R(x, y)$.

3. For any rooted formula $\psi @ \chi$ that occurs under a separating connective, we dissolve the separating connective in a similar matter as described above.

Now we can show completeness of the natural deduction proof system by reduction to the completeness of the sequent calculus.

Lemma 3.4.9 (Completeness)**.** $\Gamma \models^{\mathbf{RSL}} \phi$ *implies* $\Gamma \vdash^{\mathbf{RSL}} \phi$.

Proof. The proof goes along the following lines, and mostly uses standard techniques from interpretational proof theory [212]. We adapt the premises and conclusion in an equisatisfiable way, as sketched out above. We then obtain a sequent $\Gamma' \Rightarrow \phi'$ for which, by the completeness result of the sequent calculus established previously, we can obtain a deduction. Every deduction in sequent calculus can be mapped to a deduction in natural deduction. The operations to obtain the adapted premises and conclusion can be reversed to obtain a proof of the original conclusion ϕ with the original premises Γ in the natural deduction proof system. □

We gloss over the details comparing the semantics **RSL** and **FORSL**. However, these details are not essential to the completeness result above: it is also possible to prove the completeness of the proof system **RSL** directly, by replicating much of the work done previously to show completeness of the sequent calculus (the model existence theorem): again by constructing a maximal consistent set of formulas of (extended) separation logic out of a given set of formulas, and constructing a model out of it to show the satisfiability of the given set of formulas. After doing such a direct proof of completeness, one also establishes a relation between the two semantics.

3.5 Discussion

One may think of relational separation logic to be an abstraction of (functional) separation logic in the following sense: suppose, in an object-oriented setting, we would have a functional 'points to' relation for each field of an object. In the abstract view of (one-step) reachability, it does not matter by which field an object points to another object, what only matters is that another object is reachable through *some* field. Reachability is thus modeled as a points-to relation that is not necessarily functional, and interpreting the separating conjunction thus involves a partition of objects. In particular, we have that the formula $(x \hookrightarrow -) * (x \hookrightarrow -)$ should be equivalent to **false**, because an object x cannot be in both separate parts at the same time. With the condition on the disjointedness of the domains of $\mathcal{R}_1$ and $\mathcal{R}_2$ this equivalence indeed holds.

However, and contrary to our intuition of separation, it is possible to satisfy $(x \hookrightarrow -) * (x \hookrightarrow -)$ if we merely require the relations $\mathcal{R}_1$ and $\mathcal{R}_2$ to be disjoint

	Narrow	Wide
Strict	$(x \rightharpoonup y)$	$(x \mapsto y)$
Loose	$(x \hookrightarrow y)$	$(x \hookrightarrow y)$

Table 3.1: The four points-to relations.

(since one part can assign the location x to a different value than the other part). But then what does *separate* mean if an object x can be in both separate parts at the same time?

We discuss the consequence of the fact that in relational separation logic the points-to relation is no longer functional. We previously have seen the following two concepts:

- We have that the primitive formula $(x \hookrightarrow y)$ expresses 'x points to y' or 'location x has value y'. In the relational setting, we no longer have that if $(x \hookrightarrow y)$ holds that y is the *only* value that x points to, since it is possible that there are other values that x points to as well.
- We have that $(x \mapsto y)$ abbreviates $((x \hookrightarrow y) \wedge \forall z, w((z \hookrightarrow w) \rightarrow x = z))$, which expresses that '$x$ strictly points to y' or 'x points to y and only x is allocated'. Similarly, in the relational setting, we also no longer have that if $(x \mapsto y)$ holds that y is the *only* value that x points to, since it is also possible that there are other values that the location x points to. However, we do have that x is the only allocated location.

In the relational setting, that a location points to a value does not necessarily mean that this location points to only one value. Thus it is warranted that we introduce the following abbreviations:

$$(x \hookrightarrow y) \text{ abbreviates } ((x \hookrightarrow y) \wedge \forall z((x \hookrightarrow z) \rightarrow y = z))$$
$$(x \rightharpoonup y) \text{ abbreviates } ((x \hookrightarrow y) \wedge \forall z, w((z \hookrightarrow w) \rightarrow x = z \wedge y = w))$$

where z is a fresh variable. We speak about these formulas in the following way:

- for $(x \hookrightarrow y)$ we say 'x points to y' or 'location x has value y',
- for $(x \rightharpoonup y)$ we say 'x points to y alone' or 'location x has (and only has) value y',
- for $(x \mapsto y)$ we say 'strictly x points to y' or 'x points to y and only x is allocated',
- for $(x \rightharpoonup y)$ we say 'strictly x points to y alone' or 'x points to y alone and only x is allocated' or 'the one and only location-value pair is (x, y)'.

Strictness (resp. looseness) indicates exactly one (resp. at least one) location on the heap, and narrowness (resp. wideness) indicates precisely one (resp. at least

one) value is associated to that location. The four points-to relations can be systematized as in Table 3.1. The following sentences are valid:

$$\forall x, y.\ (x \mapsto y) \leftrightarrow (x \mapsto y) \wedge (x \hookrightarrow y),$$
$$\forall x, y.\ (x \mapsto y) \vee (x \hookrightarrow y) \rightarrow (x \hookrightarrow y),$$

and $(x \mapsto y)$ and $(x \hookrightarrow y)$ are themselves incomparable. If we have

$$\forall x, y.\ (x \hookrightarrow y) \rightarrow (x \hookrightarrow y)$$

then the points-to relation must be functional. This is the case in (functional) separation logic as introduced in the previous chapter, but no longer for relational separation logic. The latter formula is equivalent to $\mathit{fun}(\hookrightarrow)$.

In this chapter we have investigated relational separation logic, but how much work does it take to adapt the semantics and the proof system to (functional) separation logic?[1] Both the semantics and the proof system of relational separation logic rely on the fact that we can express relations using arbitrary binary formulas. We can not simply use the proof system but restrict to functional interpretations of the binary variables: the problem lies in that rooted assertions $p@\phi$ allow any binary formula ϕ, which may denote non-functional relations as well. And the same problem happens when considering comprehensive relational structures. However, without a lot of effort we can overcome this problem, by introducing additional notational conventions, obligations, and assumptions.

Similar to how terms can be added to a first-order logic that only has constant symbols such as predicate and relation symbols, by *declaring* constant symbols as individual symbols and function symbols, we can also keep track of a subclass of binary formulas for which we declare the property of functionality holds. By writing such binary formulas $\hat{\phi}$, to mean that ϕ must be functional, then we can keep track for which formulas we have additional obligations to show functionality, or assumptions that witness their functionality.

We can then adapt the proof system **RSL** to obtain the proof system **SL**: additional proof obligations are required for the introduction rule of separating conjunction (because the disjoint union of two functional relations is not necessarily functional) and the elimination rule of separating implication (where also the disjoint union is not necessarily functional). In the case of the elimination rule of separating conjunction, we already know that splitting a functional relation always results in two functional relations, leading to additional assumptions. In the case of the introduction rule of separating implication we can add functionality (of the relation representing the extension, and of the disjoint union of the outer heap and the extension) as an additional assumptions.

Adapting **GRSL** to **GSL** involves restricting to partial functions h instead of relations $\mathcal{R}$, to obtain general heap structures. We then have the set $\mathit{Fun}_{\mathfrak{H},h,\rho}(\hat{\psi})$

[1] Many respectable colleagues have told the author that 'nobody reads Ph.D. theses'—in the interest of their reputation it is best to leave them anonymous. The full description of the proof system **SL** and its soundness and completeness proof remain to be published in a forthcoming journal article. However, from the sketch provided here, it is not difficult for a reader to come up with it themselves.

that denotes a partial function based on the formula ψ for which we know it has the property of functionality. Consequently, we can consider closed heap structures in a similar way, to obtain **SL**.

Finally, notice how in the rooted assertion $\phi@\psi$ the @-connective is related to the binding operator $(\downarrow R\phi)$ of the previous chapter, by comparing their semantics:

- $\mathfrak{A}, \mathcal{R}, \rho \models^{\mathbf{FRSL}\downarrow} (\downarrow R\phi)$ if and only if $\mathfrak{A}, \mathcal{R}, \rho[R := \mathcal{R}] \models^{\mathbf{FRSL}\downarrow} \phi$,
- $\mathfrak{H}, \mathcal{R}, \rho \models^{\mathbf{GRSL}} \phi@\psi$ iff $\mathfrak{H}, \mathcal{R}', \rho \models^{\mathbf{GRSL}} \phi$ for $\mathcal{R}' = Rel_{\mathfrak{H},\mathcal{R},\rho}(\psi)$.

In some sense, the binding operator 'captures' the current interpretation of $\mathcal{R}$, whereas in the interpretation of the @-connective we replace the current interpretation of $\mathcal{R}$. The connection is interesting from the perspective of Henkin models of second-order logic, which satisfy a comprehension axiom, by which we know that every formula also denotes a relation over which one can quantify. If we would add second-order variables to **GRSL**, the connection may become more obvious:

- $\mathfrak{A}, \mathcal{R}, \rho \models^{\mathbf{FRSL}\downarrow} (\downarrow R\phi)$ if and only if $\mathfrak{A}, \mathcal{R}, \rho[R := \mathcal{R}] \models^{\mathbf{FRSL}\downarrow} \phi$,
- $\mathfrak{H}, \mathcal{R}, \rho \models^{\mathbf{GRSL}} \phi@R$ if and only if $\mathfrak{H}, \rho(R), \rho \models^{\mathbf{GRSL}} \phi$.