Constructive First-Order Set Theory with Descriptions

CPSC 509: Programming Language Principles

Ronald Garcia*

1 February 2022
(**Time Stamp**: 21:04, Friday 25th February, 2022)

Syntax

$\Xi \in \textsc{PropConstant}, \quad \Psi \in \textsc{AtomicProp}, \quad \Phi \in \textsc{Prop}, \quad S, A, B, \ldots \in \textsc{SetVar}, \quad \mathcal{E} \in \textsc{SetExp}$
$\ell \in \textsc{Label}, \quad \mathcal{U} \in \textsc{Assumption}, \quad \mathcal{J} \in \textsc{Judgment}, \quad \Gamma \in \textsc{Ctxt}$

$$
\begin{array}{lcl}
\Psi & ::= & \Xi \mid \mathcal{E} = \mathcal{E} \mid \mathcal{E} \in \mathcal{E} \\
\Phi & ::= & \Psi \mid \top \mid \bot \mid \Phi \wedge \Phi \mid \Phi \vee \Phi \mid \Phi \Rightarrow \Phi \mid \forall S.\, \Phi \mid \exists S.\, \Phi \\
\mathcal{E} & ::= & S \mid \wp S.\, \Phi \\
\mathcal{U} & ::= & \ell : \Phi \ \mathsf{use} \mid S \ \mathsf{set} \\
\mathcal{J} & ::= & \mathcal{E} \ \mathsf{set} \mid \Phi \ \mathsf{prop} \mid \Phi \ \mathsf{use} \mid \Phi \ \mathsf{verif} \\
\Gamma & ::= & \mathcal{U}, \ldots, \mathcal{U} \quad \text{(each label } \ell \text{ and set variable } S \text{ unique in } \Gamma\text{)}
\end{array}
$$

$\exists! S.\Phi(S) \equiv (\exists S.\Phi(S)) \wedge (\forall S_1.\, \forall S_2.\, \Phi(S_1) \wedge \Phi(S_2) \Rightarrow S_1 = S_2)$

$\boxed{\Gamma \vdash \mathcal{J}}$ **Entailment**

$$\frac{}{\mathcal{U}_1, \ldots, \ell_i : \Phi_i, \ldots, \mathcal{U}_n \vdash \Phi_i \text{ use}}\ (\text{hyp}^{\ell_i}) \qquad \frac{\Gamma \vdash \Psi \text{ use} \quad \Gamma \vdash \Psi \text{ prop}}{\Gamma \vdash \Psi \text{ verif}}\ (\text{atomic})$$

$$\frac{}{\Gamma \vdash \top \text{verif}}\ (\top\text{I}) \qquad \frac{\Gamma \vdash \bot \text{use} \quad \Gamma \vdash \Phi \text{ prop}}{\Gamma \vdash \Phi \text{ verif}}\ (\bot\text{E})$$

$$\frac{\Gamma \vdash \Phi_1 \text{ verif} \quad \Gamma \vdash \Phi_2 \text{ verif}}{\Gamma \vdash \Phi_1 \wedge \Phi_2 \text{ verif}}\ (\wedge\text{I}) \qquad \frac{\Gamma \vdash \Phi_1 \wedge \Phi_2 \text{ use}}{\Gamma \vdash \Phi_1 \text{ use}}\ (\wedge\text{E1}) \qquad \frac{\Gamma \vdash \Phi_1 \wedge \Phi_2 \text{ use}}{\Gamma \vdash \Phi_2 \text{ use}}\ (\wedge\text{E2})$$

$$\frac{\Gamma \vdash \Phi_1 \text{ verif} \quad \Gamma \vdash \Phi_2 \text{ prop}}{\Gamma \vdash \Phi_1 \vee \Phi_2 \text{ verif}}\ (\vee\text{I1}) \qquad \frac{\Gamma \vdash \Phi_1 \text{ prop} \quad \Gamma \vdash \Phi_2 \text{ verif}}{\Gamma \vdash \Phi_1 \vee \Phi_2 \text{ verif}}\ (\vee\text{I2})$$

$$\frac{\Gamma \vdash \Phi_1 \vee \Phi_2 \text{ use} \quad \Gamma, \ell_1 : \Phi_1 \text{ use} \vdash \Phi_3 \text{ verif} \quad \Gamma, \ell_2 : \Phi_2 \text{ use} \vdash \Phi_3 \text{ verif}}{\Gamma \vdash \Phi_3 \text{ verif}}\ (\vee\text{E}^{\ell_1, \ell_2})$$

$$\frac{\Gamma \vdash \Phi_1 \text{ prop} \quad \Gamma, \ell_1 : \Phi_1 \text{ use} \vdash \Phi_2 \text{ verif}}{\Gamma \vdash \Phi_1 \Rightarrow \Phi_2 \text{ verif}}\ (\Rightarrow\text{I}^{\ell_1}) \qquad \frac{\Gamma \vdash \Phi_1 \Rightarrow \Phi_2 \text{ use} \quad \Gamma \vdash \Phi_1 \text{ verif}}{\Gamma \vdash \Phi_2 \text{ use}}\ (\Rightarrow\text{E})$$

$$\frac{\Gamma, S_2 \text{ set} \vdash \Phi(S_2) \text{ verif}}{\Gamma \vdash \forall S_1.\, \Phi(S_1) \text{ verif}}\ (\forall\text{I}^{S_2}) \qquad \frac{\Gamma \vdash \forall S.\, \Phi(S) \text{ use} \quad \Gamma \vdash \mathcal{E} \text{ set}}{\Gamma \vdash \Phi(\mathcal{E}) \text{ use}}\ (\forall\text{E})$$

$$\frac{\Gamma, S_2 \text{ set} \vdash \Phi(S_2) \text{ prop} \quad \Gamma \vdash \mathcal{E} \text{ set} \quad \Gamma \vdash \Phi(\mathcal{E}) \text{ verif}}{\Gamma \vdash \exists S_1.\, \Phi(S_1) \text{ verif}}\ (\exists\text{I})$$

$$\frac{\Gamma \vdash \exists S_1.\, \Phi_1(S_1) \text{ use} \quad \Gamma, S_2 \text{ set}, \ell_1 : \Phi_1(S_2) \text{ use} \vdash \Phi_2 \text{ verif}}{\Gamma \vdash \Phi_2 \text{ verif}}\ (\exists\text{E}^{S_2, \ell_1})$$

$$\frac{\Gamma \vdash \mathcal{E} \text{ set}}{\Gamma \vdash \mathcal{E} = \mathcal{E} \text{ verif}}\ (\text{refl}) \qquad \frac{\Gamma \vdash \mathcal{E}_1 = \mathcal{E}_2 \text{ verif} \quad \Gamma \vdash \Phi(\mathcal{E}_1) \text{ verif}}{\Gamma \vdash \Phi(\mathcal{E}_2) \text{ verif}}\ (\text{eq}) \qquad \frac{\Gamma \vdash \exists! S.\, \Phi(S) \text{ verif}}{\Gamma \vdash \Phi(\imath S.\, \Phi(S)) \text{ use}}\ (\text{dd})$$

$$\frac{}{\mathcal{U}_1, \ldots, S_i \text{ set}, \ldots, \mathcal{U}_n \vdash S_i \text{ set}}\ (\text{hypS}^{S_i}) \qquad \frac{\Gamma \vdash \exists! S.\, \Phi(S) \text{ verif}}{\Gamma \vdash \imath S.\, \Phi(S) \text{ set}}\ (\text{ddS})$$

$$\frac{\Gamma \vdash \mathcal{E}_1 \text{ set} \quad \Gamma \vdash \mathcal{E}_2 \text{ set}}{\Gamma \vdash \mathcal{E}_1 = \mathcal{E}_2 \text{ prop}}\ (=\text{P}) \qquad \frac{\Gamma \vdash \mathcal{E}_1 \text{ set} \quad \Gamma \vdash \mathcal{E}_2 \text{ set}}{\Gamma \vdash \mathcal{E}_1 \in \mathcal{E}_2 \text{ prop}}\ (\in\text{P})$$

$$\frac{}{\Gamma \vdash \top \text{ prop}}\ (\top\text{P}) \qquad \frac{}{\Gamma \vdash \bot \text{ prop}}\ (\bot\text{P}) \qquad \frac{\Gamma \vdash \Phi_1 \text{ prop} \quad \Gamma \vdash \Phi_2 \text{ prop}}{\Gamma \vdash \Phi_1 \wedge \Phi_2 \text{ prop}}\ (\wedge\text{P})$$

$$\frac{\Gamma \vdash \Phi_1 \text{ prop} \quad \Gamma \vdash \Phi_2 \text{ prop}}{\Gamma \vdash \Phi_1 \vee \Phi_2 \text{ prop}}\ (\vee\text{P}) \qquad \frac{\Gamma \vdash \Phi_1 \text{ prop} \quad \Gamma, \ell_1 : \Phi_1 \text{ use} \vdash \Phi_2 \text{ prop}}{\Gamma \vdash \Phi_1 \Rightarrow \Phi_2 \text{ prop}}\ (\Rightarrow\text{P})$$

$$\frac{\Gamma, S_2 \text{ set} \vdash \Phi(S_2) \text{ prop}}{\Gamma \vdash \forall S_1.\, \Phi(S_1) \text{ prop}}\ (\forall\text{P}) \qquad \frac{\Gamma, S_2 \text{ set} \vdash \Phi(S_2) \text{ prop}}{\Gamma \vdash \exists S_1.\, \Phi(S_1) \text{ prop}}\ (\exists\text{P})$$

1 Metatheorems

Our base logic is quite restrictive, which on the downside makes for tedious proofs and a quite forced style, thanks to the use and verif judgments. On the upside, however, the logic embodies the idea of transforming inputs (uses) to outputs (verifs), and the search space for proofs is super-restricted: in some cases where other proof systems have an infinite number of proofs of an entailment, this one may have only one.

This latter property, the small space of proofs, also enables the (relatively) easy establishment of *metatheorems*, proofs *about* our proof system (rather than in it). Some of the first ones ensure that despite its paucity, the system satisfies some of the most important expected properties of a logic. Consistency is the one that is often hard to prove, but here it's nearly a one-liner. Global soundness and completeness are harder to prove than other systems (which take them as built-in rules), but that's the tradeoff for an easy proof of consistency.

We can also use some convenient metatheorems as if they were steps in our proof system, knowing that they can be "compiled" away to the base system. Global soundness and completeness are two such "macros", but there are others as well.

Proposition 1 (Consistency)**.** *There is no proof of* $\bullet \vdash \bot$ verif*.*

This ensures that at the very least our logic is not fundamentally broken. You can only verify falsehood (i.e. output pure garbage) if some of your assumptions make it possible. More generally, what we *really* want to know is that there are *some* propositions that cannot be proven, because if everything can be verified, then your logic is a lawless land. The above proposition plays both roles: it is nice that $\bot$ cannot be verified, but given some other properties (in particular global soundness), it would imply that *every* proposition could be verified (thanks to ($\bot$E)).

Proposition 2 (Global Soundness)**.** *If* $\Gamma \vdash \Phi_1$ verif *and* Γ, Φ_1 use $\vdash \Phi_2$ verif *then* $\Gamma \vdash \Phi_2$ verif

Note. The proof of this proposition is complicated! It's doable but finicky and detailed.

Proposition 3 (Global Completeness)**.** *If* $\Gamma \vdash \Phi$ prop *then* Γ, Φ use $\vdash \Phi$ verif

Proof Sketch. This proposition follows essentially from a proof of "local completeness" for each operator for forming propositional expressions, e.g. $\bot$ use $\vdash \bot$ verif and friends. □

Proposition 4 (Verified Propositions are Meaningful)**.** *If* $\Gamma \vdash \Phi$ verif *then* $\Gamma \vdash \Phi$ prop

Note. This metatheorem ensures that any proof that a proposition can be verified is meaningful: it will never refer to a set variable that has not been accounted for, and all uses of a definite description "the unique set S such that..." will indeed describe sets that, according to assumptions, can be uniquely described by the provided property. Stenlund states this metatheorem categorically, but his discussion of the system makes clear that his proof should work for judgments with antecedents.

Proposition 5 (Weakening)**.** *If* $\Gamma \vdash \mathcal{J}$ *then* $\Gamma, \mathcal{U} \vdash \mathcal{J}$

Proof Sketch. Just add the extra $\mathcal{U}$ assumption throughout, which the proof happens to never appeal to. □

Note. This proposition is called "weakening" because conceptually speaking, an entailment that demands more assumptions is considered weaker than one that demands fewer (because it can be applied in more contexts). In principle there's a stronger entailment hiding in the result of this proposition, but we use weakening to adapt a "strong" entailment to fit in a "weaker" situation.

Some logics do not admit weakening. In particular, *relevance logics* require entailments to use all of their assumptions: none can be dropped silently. Compare this to a programming language where you are expected to free all pointers to memory that you no longer need, lest you leak memory and your program crashes.

Proposition 6 (Contraction)**.** *If* $\Gamma, \ell_1 : \Phi_1$ use, $\ell_2 : \Phi_1$ use $\vdash \mathcal{J}$ *then* $\Gamma, \ell_1 : \Phi_1$ use $\vdash \mathcal{J}$

Proof Sketch. Traverse the proof and replace every use of $(\text{hyp})^{\ell_2}$ with $(\text{hyp})^{\ell_1}$, then remove the $\ell_2 : \Phi_1$ use hypothesis. □

Note. Some logics do not admit contraction. In particular, *affine logics* (I have no idea why they're called that) only allow an assumption to be used at most once, as if it were an exhaustible resource like ice cream. If you need to use a proposition twice then you need license to use two copies. As hinted by the ice cream example, such logics are used to reason about resources.

Finally, a logic that admits neither weakening nor contraction is called a *linear logic*. In linear logic, you must use all of your resources ("No dessert until you clean up your plate Joey!") and you can only use each once ("You have three wishes, and you may not wish for more!").

Proposition 7 (Conjunction is invertible)**.** *If* $\Gamma \vdash \Phi_1 \wedge \Phi_2$ verif *then* $\Gamma \vdash \Phi_1$ verif *and* $\Gamma \vdash \Phi_2$ verif

Note. Given our informal understanding of words, this metatheorem gives us confidence that $\wedge$ really means "and."

Proposition 8 (Implication is invertible)**.** *If* $\Gamma \vdash \Phi_1 \Rightarrow \Phi_2$ verif *then* Γ, Φ_1 use $\vdash \Phi_2$ verif

Note. This is the reverse of our introduction rule for implication. Note that I accidentally called this "the deduction theorem" previously, but the deduction theorem is the reverse: it coincides with implication introduction, which in some early (and painfully painful) proof theories was not baked in.

Proposition 9 (Universals are invertible)**.** *If* $\Gamma \vdash \forall S_1.\, \Phi(S_1)$ verif *then* Γ, S_2 set $\vdash \Phi(S_2)$ verif.

Note. This is directly analogous to Prop. 9.

Proposition 10 (Closed disjunctions are invertible)**.** *If* $\bullet \vdash \Phi_1 \vee \Phi_2$ verif *then* $\bullet \vdash \Phi_1$ verif *or* $\bullet \vdash \Phi_2$ verif

Note. This proof is similar to Prop. 9, but does *not* hold for arbitrary contexts. For example, consider the entailment $\Psi_1 \vee \Psi_2$ use $\vdash \Psi_1 \vee \Psi_2$ verif. Because of the disjunction among the assumptions, we cannot determine which of the two propositions holds. However, given a context with no disjunctions, we can determine it: there is a more nuanced variant of this metatheorem that makes this precise. But we show this here just to demonstrate that conjunction and implication have some differences.

Another note: this metatheorem *does not* hold for classical logic. That constructive logic "takes disjunction seriously" is part of what makes it "constructive."

Proposition 11 (Closed existentials are invertible)**.** *If* $\bullet \vdash \exists S.\Phi(S)$ verif *then there is some set expression* $\mathcal{E}$ *such that* $\bullet \vdash \mathcal{E}$ set *and* $\bullet \vdash \Phi(\mathcal{E})$ verif.

Note. This is directly analogous to Prop 10, and captures another part of our logic's constructive character: the need to put forth a particular set and a proof that it satisfies a property. And you guessed it: this property does not hold for classical logic!

Proposition 12 (The Law of the Excluded Middle Does Not Categorically Hold)**.**
It is not the case that for all Φ *such that* $\bullet \vdash \Phi$ prop *that* $\bullet \vdash \Phi \vee \neg\Phi$ verif.

Note. This methatheorem is often identified with what makes a logic "constructive". I tend to think this is the wrong way to think about it. To the contrary, Prop. 10 and Prop. 11 get more to the heart of the matter: knowledge of a disjunction or existence proof gives you strong information, that you *know* of a particular set that has the property, not just that "there must be one out there somewhere." In particular, a proof of the form $\forall S_1.\, \Phi_1(S_1) \Rightarrow \exists S_2.\, \Phi_2(S)$ constitutes a "constructive method" for taking knowledge of a set S_1, and knowledge that satisfies Φ_1 and systematically transforming that into another set S_2 that satisfies Φ_2. Typically we call such constructive methods "algorithms."

Proposition 13 (Double-Negation Elimination Does Not Categorically Hold)**.**
It is not the case that for all Φ *such that* $\bullet \vdash \Phi$ prop *that* $\bullet \vdash \neg\neg\Phi \Rightarrow \Phi$ verif.

Note. This metatheorem has similar status to the previous one. It denies "proof by contradiction." as a proof method. Again I prefer to view this one from a positive viewpoint. First, notice that the converse *is* true: if Φ verif then $\neg\neg\Phi$ verif, so a true proposition is "not false". So Prop. 13 shows that our logic distinguishes between being "true" and being "not false." Distinguishing these two states of affair can be advantageous: for starters it makes some theorems more transparent and easier to prove even classically, if you just defer classical reasoning until the end. Also it makes it clear which things you prove classically require the full "power" of classical reasoning. Constructive proofs, when possible, are often more insightful, if you care about the explanation/justification and not just the truth/falsity of the matter. BTW, you may wonder "do these props ever hold?" **Yes!** Set $\Phi \equiv \top$.