Lecture Notes on
Verifications

15-317: Constructive Logic
Frank Pfenning André Platzer

Lecture 5
January 28, 2020

1 Introduction

The verificationist point of view, already introduced earlier in the course, is that the meaning of a *logical connective* should be determined by its introduction rule. From this meaning we derive and then check the soundness and completeness of the elimination rules so that the rules are in harmony. These "local" checks pertain only to a single connective at a time.

Under this point of view, what is then the meaning of a *proposition*, which may well be constructed from multiple logical connectives? We say the meaning of a proposition is determined by its *verifications* [ML83]. In order to be consistent with the explanation of the connectives, a verification should therefore proceed by introduction rules. However, we also need to take the elimination rules into account because they inevitably appear in the proof of a proposition.

Intuitively, a verification should be a proof that only analyzes the constituents of a proposition. This restriction of the space of all possible proofs is necessary so that the definition is well-founded. For example, if we allowed *all* proofs, then in order to understand the meaning of A, we would first have to understand the meaning of $B \supset A$ and B, the whole verificationist approach is in jeopardy because B could be a proposition containing, say, A. But the meaning of A would then in turn depend on the meaning of A, creating a vicious cycle.

To understand what would go wrong, consider a proof of $A \supset A$ *true*:

$$\dfrac{\dfrac{}{A\ \mathit{true}}\,u}{A \supset A\ \mathit{true}}\,{\supset}I^u$$

This seems like the most canonical proof justifying the proposition $A \supset A$. But, using the local expansions from the harmony lecture, the proof could have been expanded by prolonging it with $\supset\! E$ arbitrarily often:

$$\dfrac{\dfrac{\dfrac{\dfrac{}{A\ \mathit{true}}\,u}{A \supset A\ \mathit{true}}\,{\supset}I^u \qquad \dfrac{}{A\ \mathit{true}}\,v}{A\ \mathit{true}}\,{\supset}E}{A \supset A\ \mathit{true}}\,{\supset}I^v$$

The verificationist meaning of $A \supset A$ should depend on the former proof, not on any of the never-ending pile of needlessly expanded proofs.

In this section we will make the structure of verifications more explicit. We write $A\!\uparrow$ for the judgment "*A has a verification*". Naturally, this should mean that A is true, and that the evidence for that has a special form. Eventually we will also establish the converse: if A is true then A has a verification. Verifications also play a helpful role in proof search, because $A\!\uparrow$ limits how a proof of A can look like to a much more canonical form. From the proof search perspective, the notion of verification is called *intercalation* [SB98].

2 Rules for Verifications and Uses

Conjunction is easy to understand. A verification of $A \wedge B$ should exactly consist of a verification of A and a verification of B.

$$\dfrac{A\!\uparrow \quad B\!\uparrow}{A \wedge B\!\uparrow}\,{\wedge}I$$

We reuse here the names of the introduction rule, because this rule is strictly analogous to the introduction rule for the truth of a conjunction.

Implication, however, introduces a new hypothesis which is not explicitly justified by an introduction rule but just a new label. For example, in the proof

$$\dfrac{\dfrac{\dfrac{}{A \wedge B\ \mathit{true}}\,u}{A\ \mathit{true}}\,{\wedge}E_1}{(A \wedge B) \supset A\ \mathit{true}}\,{\supset}I^u$$

the conjunction $A \wedge B$ is *not* justified by an introduction!

Yet $A \wedge B$ *true* did not enter this proof because we tried to verify it, but rather, because it became readily available to us as an assumption (labeled

u) as a result of applying the $\supset I$ introduction rule. This is consistent with our informal discussion of proof search strategies from earlier lectures. We apply introduction rules from the bottom up and elimination rules from the top down. We introduce a second judgment, $A{\downarrow}$ which means "*A may be used*". $A{\downarrow}$ should be the case when either A *true* is a hypothesis, or A is deduced from a hypothesis via elimination rules. Our local soundness arguments provide some evidence that we cannot deduce anything incorrect in this manner. Note that $A{\downarrow}$ does not require us to use A in the proof, it merely gives us a license to assume A if we need it.

We go through the connectives in turn, defining verifications and uses.

Conjunction. In summary of the discussion above, we obtain:

$$\frac{A{\uparrow} \quad B{\uparrow}}{A \wedge B{\uparrow}}\ \wedge I \qquad\qquad \frac{A \wedge B{\downarrow}}{A{\downarrow}}\ \wedge E_1 \qquad \frac{A \wedge B{\downarrow}}{B{\downarrow}}\ \wedge E_2$$

The first/left elimination rule can be read as: "*If we can use $A \wedge B$ we can use A*", and similarly for the right elimination rule. The directions of the arrows of verifications and uses matches nicely with the direction in which we end up applying the proof rules. The $\wedge I$ rule with all its verifications is applied toward the top: A verification $A \wedge B{\uparrow}$ of $A \wedge B$ will continue to seek a verification $A{\uparrow}$ of A as well as a verification $B{\uparrow}$ of B. In contrast, the elimination rule $\wedge E_1$ with all its uses is applied toward the bottom: If we have license $A \wedge B{\downarrow}$ to use $A \wedge B$, then we also have license $A{\downarrow}$ to use A.

Implication. The implication introduction rule creates a new hypothesis, which we may use in a proof. The assumption is therefore of the judgment $A{\downarrow}$

$$\cfrac{\cfrac{}{A{\downarrow}}\ u \\ \vdots \\ B{\uparrow}}{A \supset B{\uparrow}}\ \supset I^u$$

That is, a verification $A \supset B{\uparrow}$ that A implies B consists of a verification $B{\uparrow}$ of B from an additional assumption u which gives us license $A{\downarrow}$ to use A.

In order to use an implication $A \supset B$ we first require a verification of A. Just requiring that A may be used would be too weak, as can be seen when trying to prove $((A \supset A) \supset B) \supset B{\uparrow}$ (see Section 5). It should also be clear from the fact that we are not eliminating a connective from A.

$$\frac{A \supset B\downarrow \quad A\uparrow}{B\downarrow}\;{\supset}E$$

Verifications and uses meet in ${\supset}I^u$ and ${\supset}E$ due to the direction of the implication. A verification $A \supset B\uparrow$ of $A \supset B$ consists of a verification $B\uparrow$ of B that has license $A\downarrow$ to use the additional hypothesis A. A use $A \supset B\downarrow$ of $A \supset B$ gives license to use $B\downarrow$ but only after launching a verification $A\uparrow$ to verify that A actually holds. This is aligned with the operational intuition of proof search. If we would like to make use of an implication $A \supset B\downarrow$, we first need to verify $A\uparrow$ before we obtain a license to use $B\downarrow$.

Disjunction. The verifications of a disjunction immediately follow from their introduction rules, because verifying a disjunction requires verifying one of its disjuncts.

$$\frac{A\uparrow}{A \lor B\uparrow}\;{\lor}I_L \qquad \frac{B\uparrow}{A \lor B\uparrow}\;{\lor}I_R$$

A disjunction is used in a proof by cases in the elimination rule ${\lor}E$. This rule adds two new hypotheses, and each of them may be used in the corresponding subproof. Whenever we set up a hypothetical judgment we are trying to find a verification of its conclusion, possibly with uses of hypotheses. That is why the conclusion of ${\lor}E$ should be a verification.

$$\frac{A \lor B\downarrow \quad \begin{array}{c}\overline{A\downarrow}^{\,u}\\ \vdots \\ C\uparrow\end{array} \quad \begin{array}{c}\overline{B\downarrow}^{\,w}\\ \vdots \\ C\uparrow\end{array}}{C\uparrow}\;{\lor}E^{u,w}$$

The proof search intuition is again aligned with the fact that the conclusion of ${\lor}E$ is a verification $C\uparrow$, for if it were a license $C\downarrow$ to use C, then we could use rule ${\lor}E$ to go off on a tangent and obtain licenses for all kinds of propositions C that our surrounding proof is never even interested in.

Truth. The only verification of truth is the trivial one.

$$\frac{}{\top\uparrow}\;\top I$$

A hypothesis $\top\downarrow$ cannot be used because there is no elimination rule for $\top$. Yet, no useful information was put into a verification of $\top\uparrow$ anyhow.

Falsehood. There is no verification of falsehood because we have no introduction rule (besides, $\bot$ should never be verified in a proof system).

We can use falsehood, signifying a contradiction from our current hypotheses, to verify any conclusion. This is the zero-ary case of a disjunction.

$$\frac{\bot{\downarrow}}{C{\uparrow}}\ \bot E$$

One might argue that a license to use $\bot$ should give us a license to use any arbitrary other C. But the $\bot E$ rule restricts this such that $\bot{\downarrow}$ is only used to show the C we are actually looking to verify, as in conclusion $C{\uparrow}$ of $\lor E$. The verifications and uses judgments make it clearer than the truth judgment that, while we should never verify $\bot{\uparrow}$, we can still read off other information from a license to use $\bot{\downarrow}$ that came from some assumption.

Atomic propositions. How do we construct a verification of an atomic proposition P? We cannot break down the structure of P because there is none, so we can only proceed if we already know P is true. This can only come from a hypothesis (after all, there is no introduction rule for atomic propositions), so we have a rule that lets us use the knowledge of an atomic proposition to construct its verification.

$$\frac{P{\downarrow}}{P{\uparrow}}\ {\downarrow}{\uparrow} \qquad \text{for atomic proposition } P$$

This rule has a special status in that it represents a change in judgments but is not tied to a particular local connective. We call this a *judgmental rule* in order to distinguish it from the usual introduction and elimination rules that characterize the connectives. If we are seeking a verification $P{\uparrow}$ of atomic proposition P, then we succeed if we have a license $P{\downarrow}$ to use P.

For example, we verify $(A \lor B) \supset (B \lor A){\uparrow}$ for atomic propositions A, B:

$$\dfrac{\dfrac{\dfrac{}{A \lor B{\downarrow}}\ u \quad \dfrac{\dfrac{\dfrac{}{A{\downarrow}}\ v}{A{\uparrow}}\ {\downarrow}{\uparrow}}{B \lor A{\uparrow}}\ {\lor}I_2 \quad \dfrac{\dfrac{\dfrac{}{B{\downarrow}}\ w}{B{\uparrow}}\ {\downarrow}{\uparrow}}{B \lor A{\uparrow}}\ {\lor}I_1}{B \lor A{\uparrow}}\ {\lor}E^{v,w}}{(A \lor B) \supset (B \lor A){\uparrow}}\ {\supset}I^u$$

Notice how this verification would never succeed without the judgmental rule ${\downarrow}{\uparrow}$ that makes the verification of the atomic propositions A and

B. Only fairly boring propositions such as $\top\uparrow$ can be verified without the judgmental rule $\downarrow\uparrow$ in which verifications and uses meet.

What if A and B are no atomic propositions, but are themselves abbreviations for larger propositions? Say, A is actually the proposition $C \supset D$. Is the above still a successful proof? If we had used pure natural deduction with the truth judgment to show $(A \vee B) \supset (B \vee A)$ *true* then the same proof would have justified $((C \supset D) \vee B) \supset (B \vee (C \supset D))$ *true* after resolving the abbreviation A. But note that, even after replacing A with $C \supset D$ everywhere, the above is *no* verification of $((C \supset D) \vee B) \supset (B \vee (C \supset D))\uparrow$. The reason is that the inference near assumption v would then look like:

$$\frac{C \supset D\downarrow}{C \supset D\uparrow}\,\downarrow\uparrow$$

But this is not a correct use of the judgmental rule $\downarrow\uparrow$, since $C \supset D$ is no atomic proposition. How could we argue that this inference is acceptable even if not literally by the $\downarrow\uparrow$ rule? We could expand it to a proper verification using the verification and uses proof rules:

$$\dfrac{\dfrac{\dfrac{C \supset D\downarrow \qquad \dfrac{\dfrac{}{C\downarrow}\,t}{C\uparrow}\,\downarrow\uparrow}{D\downarrow}\,\supset\!E}{D\uparrow}\,\downarrow\uparrow}{C \supset D\uparrow}\,\supset\!I^t$$

Obviously this proper verification of $C \supset D\uparrow$ is much larger than if we were allowed to use the judgmental rule $\downarrow\uparrow$ on compound propositions.

3 Global Soundness and Completeness

With some care in modifying the judgments, the local soundness and completeness notions from the harmony lecture could be carried over to verifications and uses. Verifications and uses, however, also enable us to ask even more interesting global counterparts that concern the entire proof.

Global soundness. Local soundness is an intrinsic property of each connective, asserting that the elimination rules for it are not too strong given the introduction rules. Global soundness is its counterpart for the whole system of inference rules. It says that if an arbitrary proposition A has a verification then we may use A without gaining any information. Whatever $C{\uparrow}$ we can verify using $A{\downarrow}$, we can already verify $C{\uparrow}$ without $A{\downarrow}$, because we can verify $A{\uparrow}$ itself. That is, for arbitrary propositions A and C:

$$\begin{array}{cccccc} & & & A{\downarrow} & & \\ & & & \vdots & & \\ \textit{If} & A{\uparrow} & \textit{and} & C{\uparrow} & \textit{then} & C{\uparrow}. \end{array}$$

We would want to prove this using a substitution principle, except that the judgment $A{\uparrow}$ and $A{\downarrow}$ do not match. In the end, the arguments for local soundness will help us carry out this proof later in this course when we have progressed to sequent calculus.

Global soundness also implies that we can (fortunately) never verify $\bot{\uparrow}$ except possibly from assumptions that are themselves contradictory and unprovable. For if we could, global soundness would imply the existence of a direction verification of $\bot{\uparrow}$, which has no introduction rule.

Global completeness. Local completeness is also an intrinsic property of each connective. It asserts that the elimination rules are not too weak, given the introduction rule. Global completeness is its counterpart for the whole system of inference rules. It says that if we may use A then we can construct from this a verification of A. That is, for arbitrary propositions A:

$$\begin{array}{c} A{\downarrow} \\ \vdots \\ A{\uparrow}. \end{array}$$

Global completeness follows from local completeness rather directly by induction on the structure of A. Note how crucial it is to distinguish the verification judgment $A{\uparrow}$ from the use judgment $A{\downarrow}$ to be able to clearly even state the goal of global completeness.

For atomic propositions P, the ${\downarrow}{\uparrow}$ rule directly justifies the above. Because it can often shorten proofs, one may sometimes implicitly use global completeness by allowing

$$\frac{A{\downarrow}}{A{\uparrow}}\;{\uparrow}{\downarrow}$$

for arbitrary propositions A.

Global soundness and completeness are properties of whole deductive systems. Their proofs must be carried out in a mathematical *metalanguage* which makes them a bit different than the formal proofs that we have done so far within natural deduction. Of course, we would like them to be correct as well, which means they should follow the same principles of valid inference that we have laid out so far.

4 Relating Verifications and Uses to Truth

There are two further properties we would like, relating truth, verifications, and uses. The first is that if A has a verification or A may be used, then A is true, e.g.:

$$\text{If } A\!\uparrow \text{ then } A \ \mathit{true}$$

Indeed, any verification is a proof. We have just specialized the introduction and elimination rules (except for the judgmental rule $\downarrow\uparrow$ which becomes redundant under the interpretation of verification and use as truth). We can traverse a verification and replace both $A\!\uparrow$ and $A\!\downarrow$ by $A\ \mathit{true}$ and obtain a proof. The minimal required change is to collapse instances of the rule

$$\frac{A\!\downarrow}{A\!\uparrow}\ {\downarrow\uparrow}$$

into simply $A\ \mathit{true}$, because otherwise premise and conclusion of the rule would be identical.

Significantly more difficult is the converse property that if A is true then A has a verification. Since we justified the meaning of the connectives from their verifications, a failure of this property would be devastating to the entire verificationist program. Fortunately it holds and can be proved by exhibiting a process of *proof normalization* that takes an arbitrary proof of A *true* and constructs a verification of $A\!\uparrow$.

All these properties in concert show that our rules are well constructed, locally as well as globally. Experience with many other logical systems indicates that this is not an isolated phenomenon: we can employ the verificationist point of view to give coherent sets of rules not just for constructive logic, but for classical logic, temporal logic, spatial logic, modal logic, and many other logics that are of interest in computer science. Taken together, these constitute strong evidence that separating judgments from propositions and taking a verificationist point of view in the definition of the logical connectives is indeed a proper and useful foundation for logic.

Finally observe how verifications play a role in informing proof search by reducing the proof search space. The direction of the arrows indicates in which direction a judgment should be expanded during proof search. A verification $A\uparrow$ needs to be verified upwards by applying its appropriate introduction rule. A license to use $A\downarrow$ can be used downwards by applying its appropriate elimination rule. Verifications and uses meet in the judgmental rule $\downarrow\uparrow$. In fact, when you carefully examine the example deductions we have conducted so far, you will see that they already ended up following the proof search order that verifications and uses mandate. What needed our creativity in proof search so far has no become systematic thanks to a distinction of whether A needs to be verified or whether A can be assumed to hold.

5 A Counterexample

In this section we illustrate how things may go wrong if we do not define verifications correctly.

If the $\supset\!E$ elimination rule would be modified to have a second premise giving license to use $A{\color{red}\downarrow}$ instead of a verification $A\uparrow$:

$$\frac{A \supset B\downarrow \quad A{\color{red}\downarrow}}{B\downarrow}\supset\!E?$$

Then the verification of $((A \supset A) \supset B) \supset B\uparrow$ would be stuck:

$$\cfrac{\cfrac{\cfrac{\cfrac{}{(A \supset A) \supset B\downarrow}u \qquad A \supset A{\color{red}\downarrow}}{B\downarrow}\supset\!E?}{B\uparrow}\uparrow\downarrow}{((A \supset A) \supset B) \supset B\uparrow}\supset\!I^u$$

because there is no rule that applies to $A \supset A{\color{red}\downarrow}$ (another $\supset\!E?$ is not applicable because it is missing the license $A\downarrow$ for its second premise).

Contrast this to the successful verification with the correct $\supset\!E$ rule:

$$\cfrac{\cfrac{\cfrac{\cfrac{}{(A \supset A) \supset B\downarrow}u \qquad \cfrac{\cfrac{\cfrac{}{A\downarrow}w}{A\uparrow}\uparrow\downarrow}{A \supset A\uparrow}\supset\!I^w}{B\downarrow}\supset\!E}{B\uparrow}\uparrow\downarrow}{((A \supset A) \supset B) \supset B\uparrow}\supset\!I^u$$

6 Normal and Neutral Proof Terms

Any verification is a proof. Hence, we should not need to devise a new notation for *proof terms*, just reuse them and distinguish those that constitute verifications. Indeed, we need two classes of terms, so that $N : A\!\uparrow$ is for "*N is a verification of A*" and $R : A\!\downarrow$ for "*R is a justification for the use of A.*" In the language of functional programs, these already happen to have names coming from a different tradition: terms N are called *normal* and terms R are called *neutral*. By annotating the inference rules for verifications and uses with proof terms, we obtain the following grammatical characterization of these classes of terms.

Neutral	$R ::= x$	Variable	Hyp
	$\mid\ R\,N$	Application	$\supset E$
	$\mid\ \mathsf{fst}\,R \mid \mathsf{snd}\ R$	Projections	$\wedge E_{1,2}$
Normal	$N ::= \mathsf{fn}\ x \Rightarrow N$	Function	$\supset I$
	$\mid\ (N_1, N_2)$	Pair	$\wedge I$
	$\mid\ (\,)$	Unit	$\top I$
	$\mid\ \mathsf{inl}\,N \mid \mathsf{inr}\,M$	Injections	$\vee I_{1,2}$
	$\mid\ (\mathsf{case}\ R\ \mathsf{of}\ \mathsf{inl}\,x_1 \Rightarrow N_1 \mid \mathsf{inl}\,x_2 \Rightarrow N_2)$	Case	$\vee E$
	$\mid\ \mathsf{abort}\ R$	Abort	$\bot E$
	$\mid\ R$	Normal Term	$\downarrow\uparrow$

At first glance, the case and abort construct appear to be in the wrong place, but then we look back at the rules and see that they do indeed construct a verification of some C.

It is easy to verify that a normal term (which includes all neutral terms) can never be reduced. This is why these terms are called *normal* alias *irreducible*. For example, the general proof term $\mathsf{fst}\,(M_1, M_2)$ does not fit this grammar, because only $\mathsf{fst}\,R$ is allowed, and a neutral term R cannot be a pair. Indeed, $\mathsf{fst}\,(M_1, M_2)$ could still be reduced to just M_1.

If we go back to local reductions, this should not be surprising. A local reduction arises if an elimination is applied to the result of an introduction, but this means an elimination is *directly* below an introduction which is ruled out for verifications. The grammar above just documents this fact on proof terms. If an elimination for a connectives follows right after the introduction for the same connective, then a location reduction is possible. If this happens nowhere, then the proof term is irreducible alias normal.

7 Consistency and Counting Normal Proofs

First, we observe that there (fortunately!) is no introduction rule for $\bot$ and therefore no verification of $\bot$. In other words, not every proposition has a verification. If we assume global soundness (yet to be proved), then this implies the consistency of the logic. The reason is that, by global soundness, indirect verifications of $\bot{\uparrow}$ from extra uses $C{\downarrow}$ could be normalized to a direct verification $C{\uparrow}$, which has no introduction rule.

As a second example, how many proofs are there of $A \supset A$ *true* for a propositional variable A? There are infinitely many by the local expansions from the harmony lecture. How many verifications are there of $A \supset A{\uparrow}$? A minute of doodling will tell you there can be only one, namely:

$$\dfrac{\dfrac{\dfrac{}{A{\downarrow}}\,u}{A{\uparrow}}\,{\downarrow}{\uparrow}}{A \supset A{\uparrow}}\,{\supset}I^u$$

This also means there is exactly one normal term of type $A \supset A$:

$$\mathsf{fn}\,u \Rightarrow u : A \supset A$$

There is any number of unnecessarily complicated terms of type $A \supset A$ that come from proof-term-assigned natural deduction proofs such as those obtained by locally expanding $\mathsf{fn}\,u \Rightarrow u$. But there is only one normal such term because there is only one verification. Similarly, there are exactly two verifications of $A \supset (A \supset A)$, which differ by which of the two different available assumptions of $A{\downarrow}$ are used to verify $A{\uparrow}$. Therefore there are also only two normal proof terms:

$$\begin{array}{l} \mathsf{fn}\,u \Rightarrow \mathsf{fn}\,w \Rightarrow u : A \supset (A \supset A) \\ \mathsf{fn}\,u \Rightarrow \mathsf{fn}\,w \Rightarrow w : A \supset (A \supset A) \end{array}$$

Obviously, none of the corresponding proofs used all their available assumptions. Taking things a step further, we see that the normal proofs of type $A \supset (A \supset A) \supset A$ are in bijection with the natural numbers:

$$\begin{array}{lcl} \mathsf{zero} & = & \mathsf{fn}\,z \Rightarrow \mathsf{fn}\,s \Rightarrow z \\ \mathsf{one} & = & \mathsf{fn}\,z \Rightarrow \mathsf{fn}\,s \Rightarrow s(z) \\ \mathsf{two} & = & \mathsf{fn}\,z \Rightarrow \mathsf{fn}\,s \Rightarrow s(s(z)) \\ \ldots & & \end{array}$$

References

[ML83] Per Martin-Löf. On the meanings of the logical constants and the justifications of the logical laws. Notes for three lectures given in Siena, Italy. Published in *Nordic Journal of Philosophical Logic*, 1(1):11-60, 1996, April 1983.

[SB98] Wilfried Sieg and John Byrnes. Normal natural deduction proofs (in classical logic). *Studia Logica*, 60(1):67–106, January 1998.