Lecture Notes on Verifications

15-317: Constructive Logic
Frank Pfenning

Lecture 5
September 12, 2017

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. These "local" checks pertain only to a single connective at a time.

Under this point of view, what is the meaning of a *proposition*, of course 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 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.

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. Even-

tually 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 limit 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].

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

$$\frac{A\uparrow \quad B\uparrow}{A \wedge B\uparrow}\ \wedge I$$

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.

The informal discussion of proof search strategies earlier, namely to use introduction rules from the bottom up and elimination rules from the top down contains the answer. 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.

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

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

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

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

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

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 2) It should also be clear from the fact that we are not eliminating a connective from A.

$$\dfrac{A \supset B\downarrow \quad A\uparrow}{B\downarrow}\,\supset E$$

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.

Disjunction. The verifications of a disjunction immediately follow from their introduction rules.

$$\dfrac{A\uparrow}{A \vee B\uparrow}\,\vee I_L \qquad \dfrac{B\uparrow}{A \vee B\uparrow}\,\vee I_R$$

A disjunction is used in a proof by cases, called here $\vee E$. This introduces 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 the conclusion, possibly with uses of hy-

potheses. So the conclusion of $\vee E$ should be a verification.

$$\dfrac{\begin{array}{ccc} & \overline{A\downarrow}\,^{u} & \overline{B\downarrow}\,^{w} \\ & \vdots & \vdots \\ A \vee B\downarrow & C\uparrow & C\uparrow \end{array}}{C\uparrow}\ \vee E^{u,w}$$

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

$$\dfrac{}{\top\uparrow}\ \top I$$

A hypothesis $\top\downarrow$ cannot be used because there is no elimination rule for $\top$.

Falsehood. There is no verification of falsehood because we have no introduction rule.

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

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

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 $\vee E$.

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, so we have a rule that lets us use the knowledge of an atomic proposition to construct a verification.

$$\dfrac{P\downarrow}{P\uparrow}\ \downarrow\uparrow$$

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.

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. That is, for arbitrary propositions A and C:

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

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 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:

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

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 state the goal of global completeness.

Because it can often shorten proofs, we implicitly used global completeness in our formulation of verifications in lecture. That is, we allowed

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

for arbitrary A.

Global soundness and completeness are properties of whole deductive systems. Their proof 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.

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. This is rather evident since we have just specialized the introduction and elimination rules, except for the judgmental rule $\downarrow\uparrow$. But under the interpretation of verification and use as truth, this inference becomes redundant.

Significantly more difficult is the 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 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.

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 all 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.

2 A Counterexample

In this section we illustrate how things may go wrong if we do not define the notation of verification correctly.

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

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

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

$$\dfrac{\dfrac{\dfrac{\overline{(A \supset A) \supset B{\downarrow}}\ u \qquad A \supset A{\downarrow}}{B{\downarrow}}\ \supset E?}{B{\uparrow}}\ {\uparrow}{\downarrow}}{((A \supset A) \supset B) \supset B{\uparrow}}\ \supset I^u$$

because there is no rule that applies to $A \supset A{\downarrow}$. In contrast to the successful verification with the correct $\supset E$ rule:

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

3 Normal and Neutral Proof Terms

Any verification is a proof. This very easy to see, because we can traverse a verifcation and replace both $A{\uparrow}$ and $A{\downarrow}$ by A *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 *true*, because otherwise premise and conclusion of the rule would be identical.

These observations suggest that 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 $N : A\uparrow$ (N *is a verification of* A) and $R : A\downarrow$ (R *is a justification for the use of* A). In the language of 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, we obtain the following grammatical characterization of these classes of terms.

Neutral	R	::=	x	Variable	Hyp
		|	$R\,N$	Application	$\supset E$
		|	$\mathsf{fst}\,R \mid \mathsf{snd}\,R$	Projections	$\wedge E_{1,2}$
Normal	N	::=	$\mathsf{fn}\,x \Rightarrow N$	Function	$\supset I$
		|	(N_1, N_2)	Pair	$\wedge I$
		|	$()$	Unit	$\top I$
		|	$\mathsf{inl}\,N \mid \mathsf{inr}\,M$	Injections	$\vee I_{1,2}$
		|	$(\mathsf{case}\,R\,\mathsf{of}\,\mathsf{inl}\,x_1 \Rightarrow N_1 \mid \mathsf{inl}\,x_2 \Rightarrow N_2)$	Case	$\vee E$
		|	$\mathsf{abort}\,R$	Abort	$\bot E$
		|	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 now easy to verify that a normal term (which includes all neutral terms) can never be reduced. This is why this class of terms if called normal which means as much as 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.

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 and elimination is directly below an introduction which is ruled out for verifications. The grammar above just document this on proof terms.

4 Counting Normal Proofs

First, we observe that there 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.

As a second example, how many verifications are there of $A \supset A$, for a propositional variable A? A minute of doodling will tell you there can be only one, namely:

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

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

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

Similarly, there are exactly two verification sof $A \supset (A \supset A)$, as we checked in lecture, and therefore also only two normal proof terms

$$\mathsf{fn}\, u \Rightarrow \mathsf{fn}\, w \Rightarrow u$$
$$\mathsf{fn}\, u \Rightarrow \mathsf{fn}\, w \Rightarrow w$$

Taking things a step further, we see that the normal proofs of type $A \supset (A \supset A) \supset A$ are 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.