15-399 Supplementary Notes: Proof Normalization and Normal Proofs

Robert Harper

February 3, 2005

Warning: In this note we confine our attention to the $\top\wedge\supset$ fragment of constructive logic. The results may be generalized to include disjunction and falsehood at the expense of some additional complications that would only distract from the main ideas.

Properties of Normal Proofs

Normal proofs have a restricted form, some aspects of which are captured by the following lemma.

Lemma 0.1 *1. Every normal proof is either neutral, or ends with an application of an introduction rule to other normal proofs.*[1]

2. Every neutral proof is either an assumption, or ends with the application of an elimination rule to another neutral proof.

Proof: By induction on the rules defining normal proofs. □

Every normal proof is a valid proof. This is called the *soundness property* of normal proofs.

Theorem 0.1 *1. If $P_1\downarrow,\ldots,P_n\downarrow\vdash P\uparrow$, then $P_1\,true,\ldots,P_n\,true\vdash P\,true$.*

2. If $P_1\downarrow,\ldots,P_n\downarrow\vdash P\downarrow$, then $P_1\,true,\ldots,P_n\,true\vdash P\,true$.

Proof: Simply replace each occurrence of $P\uparrow$ and of $P\downarrow$ with $P\,true$, and remove all inferences of the form

$$\frac{P\,true}{P\,true}\ (\downarrow\uparrow)$$

which arise from performing this replacement on instances of the $\downarrow\uparrow$ rule. The result is obviously a valid proof. □

[1] In the presence of disjunction and falsehood, this statement must be refined.

The process of replacing arrows by "*true*" used in the proof of the soundness theorem is called *erasure*, because it removes the distinction between normal and neutral proofs. The reverse process, called *decoration*, consists of replacing occurrences of "*true*" by suitable arrows to obtain a normal proof. If the decoration succeeds, then the original proof was already normal, but not every proof can be so decorated!

For example, consider a proof of the following form:

$$\dfrac{\begin{array}{cc}\mathcal{D} & \mathcal{E} \\ \vdots & \vdots \\ Q \supset P\ \mathit{true} & Q\ \mathit{true}\end{array}}{P\ \mathit{true}}\ (\supset\text{-}E)$$

This proof cannot be decorated, because it is not a normal proof. To see why, we may assume by induction that we have decorated $\mathcal{D}$ and $\mathcal{E}$ to obtain normal proofs $\mathcal{D}'$ of $Q \supset P\uparrow$ and $\mathcal{E}'$ of $Q\uparrow$. (If we can't do at least that, then we certainly cannot decorate the whole proof either.) To complete the decoration, we must use $\mathcal{D}'$ and $\mathcal{E}'$ as premises of implication elimination. But to do so requires that we somehow convert the normal proof $\mathcal{D}'$ into a neutral proof so that the implication elimination rule applies:

$$\dfrac{\dfrac{\begin{array}{c}\mathcal{D}' \\ \vdots \\ Q \supset P\uparrow\end{array}}{Q \supset P\downarrow}\ (???) \qquad \begin{array}{c}\mathcal{E}' \\ \vdots \\ Q\uparrow\end{array}}{P\downarrow}\ (\supset\text{-}E)$$

The marked rule would be an instance of the forbidden rule

$$\dfrac{R\uparrow}{R\downarrow}\ (\uparrow\downarrow),$$

which obliterates the distinction between normal and neutral proofs.

This example shows that there are proofs that are not normal proofs. This raises the possibility that there are propositions that have a proof, but no normal proof. However, the *completeness property* of normal proofs states that this is not the case: if a proposition has a proof, then it has a normal proof. We will prove this by showing that every non-normal proof contains "detours" that can be removed, resulting in a normal proof of the same proposition. In the foregoing example, note that the decorated proof $\mathcal{D}'$ might already be neutral (since every neutral proof is normal), in which case the decoration succeeds. But it might also end with an instance of implication introduction, and hence is not neutral. In that case, however, the proof is *reducible* in that we may apply the inversion principle for implications to eliminate the detour.

Non-Provability Using Normal Proofs

The restricted form of normal proofs makes it easy to show that certain propositions have no normal proof. For example, there is no normal proof of the law

of the excluded middle, $P \vee \neg P$. To see why, observe that there are three ways in which we might obtain a proof of $(P \vee \neg P)\uparrow$:

1. Show $(P \vee \neg P)\downarrow$. But this is impossible; for no Q may we derive $Q\downarrow$ from no assumptions.
2. Show $P\uparrow$. This is impossible in general. For example, P might be $\bot$.
3. Show $\neg P\uparrow$. But this is also impossible, because the only way to achieve this is to deduce $\bot\uparrow$ from the assumption $P\downarrow$. Since there is no introduction rule for $\bot$, we have no choice but to derive $\bot\downarrow$ from $P\downarrow$, which is impossible in general. For example, P might be $\top$.

By the completeness property of normal proofs, the law of the excluded middle has no proof at all.

It is instructive to observe that this argument breaks down for *general* proofs, precisely because it does not account for the possibility that the proof of $P \vee \neg P$ has the form

$$\dfrac{\begin{array}{cc}\mathcal{D} & \mathcal{E} \\ \vdots & \vdots \\ Q \supset P \vee \neg P\ true & Q\ true\end{array}}{P \vee \neg P\ true}\ (\supset\text{-}E),$$

which, as we saw earlier, is not a normal proof.

Thus, the above argument that the law of the excluded middle has no *normal* proof does not immediately imply that it has no *general* proof. To take this step requires that we prove completeness, which assures us that if a proposition has no normal proof, then it has no proof at all.

0.1 Proof Reduction

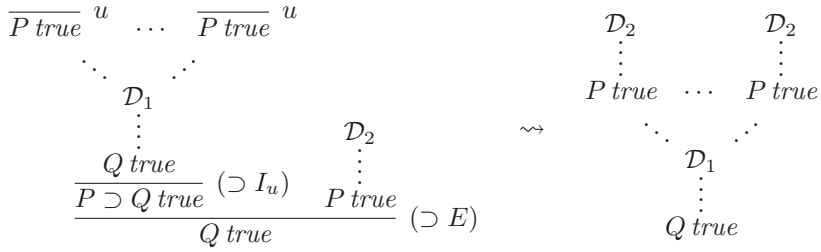
A *digression*, or *detour*, in a proof consists of the application of an elimination rule for a connective to an instance of an introduction rule for the same connective. The inversion principle states that such a digression can be eliminated by applying one of the following *reduction*, or *simplification*, steps. If no simplification can be made, we say that the proof is *irreducible*.

Here are the two proof reduction steps for conjunction:

$$\dfrac{\dfrac{\begin{array}{cc}\mathcal{D}_1 & \mathcal{D}_2 \\ \vdots & \vdots \\ P\ true & Q\ true\end{array}}{P \wedge Q\ true}\ (\wedge I)}{P\ true}\ (\wedge E_L) \quad \rightsquigarrow \quad \begin{array}{c}\mathcal{D}_1 \\ \vdots \\ P\ true\end{array}$$

$$\dfrac{\dfrac{\begin{array}{cc}\mathcal{D}_1 & \mathcal{D}_2 \\ \vdots & \vdots \\ P\ true & Q\ true\end{array}}{P \wedge Q\ true}\ (\wedge I)}{Q\ true}\ (\wedge E_R) \quad \rightsquigarrow \quad \begin{array}{c}\mathcal{D}_2 \\ \vdots \\ Q\ true\end{array}$$

Here is the proof reduction step for implication:



The proof $\mathcal{D}_2$ may be replicated many times (or no times at all) in the right-hand side.

Plugging $\mathcal{D}_2$ into $\mathcal{D}_1$ can introduce new digressions that did not previously exist. For example, suppose that $P = R \wedge S$ and that in $\mathcal{D}_1$ we have an inference of the form

$$\dfrac{\dfrac{}{R \wedge S\ true}\ u}{R\ true}\ (\wedge E_L)$$

Once we plug in $\mathcal{D}_2$ for this use of the assumption u we obtain the proof

$$\dfrac{\begin{array}{c}\mathcal{D}_2\\ \vdots\\ R \wedge S\ true\end{array}}{R\ true}\ (\wedge E_L).$$

Now if $\mathcal{D}_2$ ends, as it may, with $\wedge I$,

$$\dfrac{\begin{array}{cc}\mathcal{D}_{2,1} & \mathcal{D}_{2,2}\\ \vdots & \vdots\\ R\ true & S\ true\end{array}}{R \wedge S\ true}\ (\wedge I),$$

then we have created the digression

$$\dfrac{\dfrac{\begin{array}{cc}\mathcal{D}_{2,1} & \mathcal{D}_{2,2}\\ \vdots & \vdots\\ R\ true & S\ true\end{array}}{R \wedge S\ true}\ (\wedge I)}{R\ true}\ (\wedge E_L),$$

which must be reduced on the way to a normal proof. Since u may be used many times in $\mathcal{D}_1$, we may obtain many copies of such a digression after reducing the implication digression.

0.2 Normal Proofs and Irreducible Proofs

It is easy to see that a normal proof is irreducible. For a proof reduction step to be applicable, we must have an introduction rule for a connective followed

immediately by an elimination rule for the same connective. But all introduction rules end with $P\uparrow$, and all elimination rules require their "main" premise (the one with the connective to be eliminated) to be of the form $P\downarrow$. Since we cannot pass from $P\uparrow$ to $P\downarrow$, there can be no reductions of a normal proof.

It is not much harder to see that an irreducible proof is normal. More precisely, we may prove the following lemma.

Lemma 0.2

1. *If $\mathcal{D}$ is an irreducible proof of P true ending with an introduction rule, then $\mathcal{D}$ is normal.*
2. *If $\mathcal{D}$ is an irreducible proof of P true ending with either a hypothesis or an elimination rule, then $\mathcal{D}$ is neutral.*

Proof: By induction on proofs of P *true*, with a case analysis on the last rule applied.

- Suppose that $\mathcal{D}$ ends as follows:

$$\dfrac{\begin{array}{cc}\mathcal{D}_1 & \mathcal{D}_2 \\ \vdots & \vdots \\ P\ true & Q\ true\end{array}}{P \wedge Q\ true}\ (\wedge I)$$

  By induction both $\mathcal{D}_1$ and $\mathcal{D}_2$ are normal (perhaps even neutral), and hence can be transformed into normal proofs

$$\begin{array}{c}\mathcal{D}_1' \\ \vdots \\ P\uparrow\end{array}$$

  and

$$\begin{array}{c}\mathcal{D}_2' \\ \vdots \\ Q\uparrow.\end{array}$$

  These may be combined to yield the normal proof $\mathcal{D}'$

$$\dfrac{\begin{array}{cc}\mathcal{D}_1' & \mathcal{D}_2' \\ \vdots & \vdots \\ P\uparrow & Q\uparrow\end{array}}{P \wedge Q\uparrow}\ (\wedge I).$$

- Suppose that $\mathcal{D}$ ends as follows:

$$\dfrac{\begin{array}{c}\mathcal{D}_1 \\ \vdots \\ P \wedge Q\ true\end{array}}{P\ true}\ (\wedge E_L).$$

Since $\mathcal{D}$ is irreducible, it cannot end with $(\wedge I)$, and so, by induction, can be transformed into the neutral proof

$$\begin{array}{c} \mathcal{D}'_1 \\ \vdots \\ P \wedge Q \downarrow. \end{array}$$

This may be used with $(\wedge E_L)$ to obtain the neutral proof

$$\dfrac{\begin{array}{c} \mathcal{D}'_1 \\ \vdots \\ P \wedge Q \downarrow \end{array}}{P \downarrow}\ (\wedge E_L).$$

The other cases are handled similarly.

□

Theorem 0.2 *A proof is normal iff it is irreducible.*

0.3 Normalization

It is not at all obvious that the process proof reduction terminates. Two important theorems, which we do not prove here, show that this is indeed the case.

The normalization theorem states that there is always a way to simplify a proof to obtain an irreducible, hence normal, proof of the same result.

Theorem 0.3 (Normalization) *For every proof there is a sequence of reductions leading to a normal proof of the same proposition.*

Proof: (Sketch)

The idea is to assign a *measure* in some well-founded ordering to digressions and to derivations in such a way that if we reduce a digression of maximal measure, then the resulting proof has smaller measure than the original. Since the ordering on measures is well-founded, we cannot go on forever obtaining smaller and smaller measures — the process must eventually terminate.

A suitable measure of a derivation $\mathcal{D}$ is the pair (d, n), ordered lexicographically,[2] where d is the *degree* of the derivation $\mathcal{D}$ and n is the *number* of digressions in $\mathcal{D}$ of degree d. The degree of a derivation is defined to be the maximum of the degrees of the digressions occurring in it; the degree of a digression is defined to be the degree of the proposition being eliminated. Finally, the degree of the proposition $\top$ is zero, and the degree of $P \supset Q$ and $P \wedge Q$ is one more than the sum of the degrees of P and Q.

The crux of the remainder of the proof is to show that if we reduce a digression of maximal degree in a derivation, then the resulting derivation has a

[2]This means that $(d, n) < (d', n')$ iff $d < d'$ or $d = d'$ and $n < n'$.

strictly smaller measure — either the maximal degree of digressions has gone down (*even if* their count has gone up!), or the maximal degree remains the same, but their count has gone down.

□

Corollary 0.1 *If P true has a proof, then it has a normal proof.*

Proof: Let $\mathcal{D}$ be a derivation of P *true*. Using the normalization theorem, apply simplifications to $\mathcal{D}$ until it is irreducible, and hence normal. □

The strong normalization theorem states that we may apply proof reductions in *any order at all* without fear of reducing forever.

Theorem 0.4 (Strong Normalization) *There is no infinite sequence of reductions starting from any proof. Every sequence of reductions obtained by repeatedly simplifying digressions must terminate in a normal proof of $P\uparrow$.*

Proof: (Sketch)

The proof requires a technique known as *Tait's Method*, also known as the method of *logical relations*. The main idea is to prove an apparently stronger property of proofs, called *reducibility*, which implies strong normalization. The reducibility property is chosen so that we may prove by induction on proofs that every proof is reducible. We may then prove separately that every reducible proof is strongly normalizable.

□