MAT 1361: Notes on Formal Proofs[1]

P. J. Scott January, 1997

1 What is a Formal Proof?

In its crudest form, a formal proof is a finite list of formulas where each formula in the list has to be one of the following two things: it is either (i) *an hypothesis* (of some kind) or (ii) it arises from previous formulas in the list by a rule of inference. Hence every formula in a proof has to have a "reason" or "justification" written beside it : this tells us whether the formula is an hypothesis or else which rule it arises from (using previous formulas in the list).

In our course, we use Natural Deduction for Propositional Calculus, which closely corresponds to ordinary mathematical reasoning. Our natural deduction proofs have specific geometric shapes, similar to block, structured programming languages. The rules are divided into two kinds: *Introduction* and *Elimination* rules for each connective in Propositional Calculus. *It is important that you see how to connect these rules with correct, informal logical reasoning (say the reasoning done in ordinary mathematics.)*

Notation: A logical argument

$$\begin{array}{c} H_1 \\ H_2 \\ \vdots \\ H_n \\ \hline C \end{array}$$

from (global) hypotheses or premisses $H_1 \cdots H_n$ and with conclusion C is sometimes written $H_1, \cdots, H_n \vdash C$.

Let $\Gamma = \{H_1, \cdots, H_n\}$ be the set of global hypotheses (or premisses) in the above argument. A natural deduction proof of this argument has the form

$$\begin{array}{|l} \Gamma \quad \textit{Hypotheses} \\ \hline \vdots \\ C \end{array}$$

The formula C appears to the immediate right, at the bottom of a vertical line, called the *spine* of the proof of C. The set of hypotheses $\Gamma = \{H_1, \cdots, H_n\}$ is put at the top of the spine of the proof, immediately to its right. Note: we always make a small horizontal line under hypotheses to set them apart from the rest of the proof.

Each line of the proof starting with the set Γ must be justified by a reason: it is either a (global) hypothesis, a local hypothesis of some rule of inference, or else it arises by using

[1]These notes are a supplement to the following two sets of notes which I assume you have read carefully: (i) My Hints on Natural Deduction in the Introductory Sections of the Text for Mat1361 (Alberta Notes), (ii) The discussion on Natural Deduction in the text, Chapter 3. Further examples may be found in the books on reserve in the library.

some rule of inference applied to (formulas in) preceeding lines of the proof.

Let's examine each rule:

Conjunction ($\wedge$) In ordinary mathematics, we certainly use the following kind of reasoning:

- *Introduction of Conjunction*: Suppose we have proved A and we have proved B, for any two statements A, B . Then of course we can immediately conclude A *and* B, since we already have a proof of each component. This corresponds to the following rule of $\wedge$-Introduction for natural deduction:

$$\begin{array}{r|l} & \vdots \\ k & A \\ & \vdots \\ l & B \\ & \vdots \\ & A \wedge B \quad \wedge - I,\ k - l \end{array}$$

  Actually, we don't care whether A or B comes first: so there's a similar rule where A and B come in the opposite order:

$$\begin{array}{r|l} & \vdots \\ k & B \\ & \vdots \\ l & A \\ & \vdots \\ & A \wedge B \quad \wedge - I,\ k - l \end{array}$$

  Observe that in the $\wedge$-introduction rule, the formulas $A, B, A \wedge B$ lie on the spine of the proof: they are at the same "level" or "distance from the spine" .

- *Elimination of Conjunction*: Suppose we have proven A *and* B. Then of course we can infer A and also infer B. Essentially, that's because we have simple tautologies $(A \wedge B) \to A$ and $(A \wedge B) \to B$. To formalize this, we use the following rules of $\wedge$-Elimination:

$$\begin{array}{r|l} & \vdots \\ k & A \wedge B \\ & \vdots \\ & A \qquad\quad \wedge - E,\ k \end{array} \qquad\qquad \begin{array}{r|l} & \vdots \\ k & A \wedge B \\ & \vdots \\ & B \qquad\quad \wedge - E,\ k \end{array}$$

  Again, notice in the $\wedge$-Elimination rule that all formulas used in the rule are on the spine of the proof: they are on the same "level" .

Implication ($\to$) Implication is the fundamental concept in logical reasoning. Let's examine the two rules:

- *Introduction of Implication* This rule is based on the following simple concept: in order to prove $A \to B$, we must *assume* A and prove B from this assumption. Note that A is a "local" assumption for this inference only: we make this assumption and then based on it, we prove B . Then from this entire subproof (or subprogram) we can infer $A \to B$. The general form is:

$$\begin{array}{r|lll}
 & \vdots & & \\
k & & \begin{array}{|l}\underline{A}\end{array} & Hyp(\to -I) \\
 & & \begin{array}{|l}\vdots\end{array} & \\
l & & \begin{array}{|l}B\end{array} & \\
l+1 & A \to B & & \to -I, k-l
\end{array}$$

  There are some important comments to make about this rule.
  (i) The spine of the proof is the vertical line to the left of the formula $A \to B$. The subproof on lines $k - l$ above is "one level inwards" from the main body of the proof–that is, it is nested inwards one level (i.e. it is distance one from the spine). This subproof is a complete proof in its own right: it has its own spine, which starts with hypothesis A and ends with final formula B. Each line within this subproof must be justified by a rule, as usual.
  (ii) You can reiterate any formula X on lines $1, \cdots, (k-1)$ into this subproof *provided the formula X is on the spine of the proof.* For a more general discussion, see the section on Reiteration.
- *Elimination of Implication* This is the major rule of logical inference, going back thousands of years. It is based on the simple rule called *modus ponens*: $\dfrac{A \quad A \to B}{B}$.
  This rule says: if we assume A and $A \to B$, then we can infer B. Of course, this rule is valid: by examining the truth table, we see that if A is true, and $A \to B$ is true, then of course B is true.

  In natural deduction, *modus ponens* is captured by the $\to$-Elimination rule, which is the following (we give two versions, so it doesn't depend on the order of the assumptions):

$$\begin{array}{r|ll}
 & \vdots & \\
k & A & \\
 & \vdots & \\
l & A \to B & \\
 & \vdots & \\
 & B & \to -E,\ k, l
\end{array}
\qquad\qquad
\begin{array}{r|ll}
 & \vdots & \\
k & A \to B & \\
 & \vdots & \\
l & A & \\
 & \vdots & \\
 & B & \to -E,\ k, l
\end{array}$$

  Observe that the formulas $A, B, A \to B$ mentioned in the $\to$-Elimination rule occur on the spine of the proof.

Disjunction ($\vee$) In ordinary mathematics we sometimes use the following kind of reasoning:

- *Introduction of Disjunction*: Suppose we have proved a statement A. Then we can infer A *or* B for any B whatsoever, no matter how complicated B is. One justification for this is that we know that there are tautologies $A \rightarrow (A \vee B)$ and $B \rightarrow (A \vee B)$, so from A we can certainly infer $A \vee B$, and similarly from B we can infer $A \vee B$. Motivated by this idea, we introduce the following rules:

$$\begin{array}{r|ll} & \vdots & \\ k & A & \\ & \vdots & \\ & A \vee B & \vee - I,\ k \end{array} \qquad\qquad \begin{array}{r|ll} & \vdots & \\ k & B & \\ & \vdots & \\ & A \vee B & \vee - I,\ k \end{array}$$

- *Elimination of Disjunction* This is one of the harder rules. It is based on the idea of *Case Analysis.* Mathematicians often argue by looking at the different possible cases. This should be familiar to you, based on the Knights and Knaves logic puzzles. Here is the general form. Suppose we know A *or* B. There are two cases: Case 1: suppose A is true. Case 2: Suppose B is true. Now suppose we know that *in each case* the hypothesis for that case logically implies C. That is, In Case 1, suppose we know that from A we can infer C, and in Case 2, suppose we know that from B we can infer C. Since in either case we can infer C, then overall we can conclude C, since we assumed globally that A *or* B is true. In natural deduction we have:

$$\begin{array}{r|lll} & \vdots & & \\ k & A \vee B & & \\ k+1 & & \underline{A} & Hyp(\vee - Elim) \\ & & \vdots & \\ l & & C & \\ l+1 & & \underline{B} & Hyp(\vee - Elim) \\ & & \vdots & \\ m & & C & \\ m+1 & C & & \vee - Elim, k, k+1-l, l+1-m. \end{array}$$

Notice that each case is actually a little subproof (= subprogram): Case 1 assumes A and then eventually proves C, Case 2 assumes B and eventually proves C. The assumptions in each of the subproofs are *local hypotheses* for those cases only. Since we assume $A \vee B$ on line k (so $A \vee B$ is kind of a global hypothesis for all later lines) then together with each of the two subcases (subprograms), we can conclude C on line $m+1$.

This reasoning really corresponds to the following tautology (do you see why?):

$$[(A \vee B) \rightarrow C] \leftrightarrow [(A \rightarrow C) \wedge (B \rightarrow C)]$$

Comments:

1. Both subproofs in $\vee$-Elimination are at the same inner "level", 1 unit from the spine (the same level of nesting as in $\rightarrow$-Introduction). We think of them as parallel programs, corresponding to each case of the disjunction $A \vee B$.
2. In the two subproofs of $\vee$-Elimination, you **cannot** reiterate a formula from one case (subproof) into the other case (subproof) *because they are separate proofs at the same level.* When we argue by cases, each case is a separate proof, happening simultaneously but independently from the other case. So cases cannot share information between themselves. But you *can reiterate* from a global formula on the spine at line k into any subproof after line $k+1$.

Negation Again, there are two rules.

- $\neg$-*Introduction* This rule is simply based on *proof by contradiction.* In words: "to prove $\neg A$, assume (in a subproof) A and get a contradiction . Since from A we get a contradiction, then it must be the case that $\neg A$." In natural deduction, it has the following form:

$$\begin{array}{r|l l}
 & \vdots & \\
k & \quad \underline{A} & Hyp(\neg - I) \\
 & \quad \vdots & \\
l & \quad C & \\
 & \quad \vdots & \\
m & \quad \neg C & \\
m+1 & \neg A & \neg - I, k - m(l, m)
\end{array}
\qquad
\begin{array}{r|l l}
 & \vdots & \\
k & \quad \underline{A} & Hyp(\neg - I) \\
 & \quad \vdots & \\
l & \quad \neg C & \\
 & \quad \vdots & \\
m & \quad C & \\
m+1 & \neg A & \neg - I, k - m(l, m)
\end{array}$$

Comments:

1. The contradiction is written in parentheses in line $m+1$ after the rule name $\neg - I$. There are two rules, since we don't care whether C precedes $\neg C$ or vice versa.
2. Notice that the subproof containing the contradiction is "nested 1 level inwards" from the spine of the main proof.
3. To simplify the subproof, we allow A itself to be one of C or $\neg C$. So if starting from local hypothesis A we derive $\neg A$ then that counts as a contradiction. This special case looks like, for example:

$$\begin{array}{r|l l}
 & \vdots & \\
k & \quad \underline{A} & Hyp(\neg - I) \\
 & \quad \vdots & \\
m & \quad \neg A & \\
m+1 & \neg A & \neg - I, k - m(k, m)
\end{array}$$

- $\neg\neg$-*Elimination* This rule, sometimes just called $\neg$-Elimination, is the easiest rule of all. It is based on the fact that two negations cancel, that is $\neg\neg A$ equals A, in terms of truth values. In words, it says "in a proof, whenever we have derived

$\neg\neg A$, then at any later time we can immediately conclude A." Of course this rule is obviously logically valid. Formally, we have the following rule:

$$\begin{array}{r|ll}
 & \vdots & \\
k & \neg\neg A & \\
 & \vdots & \\
 & A & \quad \neg\neg - E,\, k
\end{array}$$

Reiteration This rule allows us to reuse a formula we have already proved (or assumed, if it is an hypothesis of some kind) later in a proof. The idea is that if we have already derived A in a proof, we can use it later in the proof. Here is an example:

$$\begin{array}{r|l}
 & \underline{\Gamma} \\
 & \vdots \\
k & D \qquad\qquad \text{some reason} \\
 & \vdots \\
 & \begin{array}{|l}
 \underline{A} \\
 \vdots \\
 \begin{array}{|l}
 \underline{B} \\
 \vdots \\
 D \quad \textit{Reiteration}, k
 \end{array} \\
 \vdots
 \end{array} \\
 & \vdots
\end{array}$$

Comments:

1. The above is just an illustration of reiterating into a later subproof nested at level 2. Note: D can be any formula, possibly one of the hypotheses
2. You can reiterate D in one step into any depth of *proper* nested subproof (*provided the subproof occurs after the formula D and has greater nesting level than D).*
3. *In $\vee -$ Elim you cannot reiterate between the two cases: each case is a separate subproof.*

2 General facts about proofs

It is important to remember the following:

1. You may only use the rules given in class. You can use supplementary Lemmas (if you prove them) but I strongly discourage it–all proofs can be done quite easily directly.
2. The basic strategy is to reason bottom-up (that is, start at the bottom from the formula you are trying to prove), although there are some rules (e.g. $\vee$-Elim) where you may

wish to reason top-down. In more advanced proofs, we use a mixture of the two kinds of strategies.

3. We can only prove tautologies. More generally, every line of a proof is either (i) an hypothesis of some kind, or (ii) a formula which is a tautological consequence of all the previous lines. That is, a formula at line k which is not a hypothesis is implied by the set of all formulas "above" it, on lines $1, \cdots, (k-1)$ (actually, we can be more precise here, but this suffices for our purposes).
4. The reason we can only prove tautologies, or tautological consequences of the global hypotheses, is the following: *all rules preserve truth.* That is, *if we apply a rule of inference to true formulas, we get true formulas.* Hence, we can only prove true statements. In particular, before you try to prove something, I recommend you check that it is either a tautology or a valid argument.