CS 205 Sections 07 and 08
Supplementary Notes on Proof
Matthew Stone
March 1, 2004
Matthew.Stone@Rutgers.Edu

1 Propositional Natural Deduction

The proof systems that we have been studying in class are called *natural deduction*. This is because they permit the same lines of reasoning and the same form of argument that you see in ordinary mathematics. Students generally find it easier to represent their mathematical ideas in natural deduction than in other ways of doing proofs.

In these systems the proof is a sequence of lines. Each line has a number, a formula, and a justification that explains why the formula can be introduced into the proof. The simplest kind of justification is that the formula is a *premise*, and the argument depends on it. Another common justification is *modus ponens*, which derives the consequent of a conditional in the proof whose antecedent is also part of the proof. Here is a simple proof with these two rules used together.

Example 1

1	$P \rightarrow Q$	*Premise*
2	$Q \rightarrow R$	*Premise*
3	P	*Premise*
4	Q	*Modus ponens 1,3*
5	R	*Modus ponens 2,4*

This proof assumes that P is true, that $P \rightarrow Q$, and that $Q \rightarrow R$. It uses modus ponens to conclude that R must then be true.

Some inference rules in natural deduction allow assumptions to be made *for the purposes of argument*. These inference rules create a *subproof*. A subproof begins with a new assumption. This assumption can be used just within this subproof. In addition, all the assumption made in outer proofs can be used in the subproof. The justification for an assumption that begins a subproof is the kind of argument that the assumption is made for. Formulas in the subproof are indented so you can see that they go together.

Two rules that create subproofs are used very frequently in propositional logic. These are *conditional proof* and *indirect proof*. In conditional proof, you assume some formula A for the purposes of argument. Then you construct a subproof which establishes the conclusion B. This subproof shows that when you make the assumption A, then B follows. From this subproof, you can infer $A \rightarrow B$ in the outer proof.

Here is an example of conditional proof. It also uses modus ponens and the *conjunction rule*: if A is part of a proof and B is part of a proof, then you can infer $A \wedge B$ in the proof, too.

Example 2

1	$P \wedge Q \rightarrow R$		*Premise*
2	$P \rightarrow Q$		*Premise*
3		P	*Premise for Conditional Proof*
4		Q	*Modus ponens 2,3*
5		$P \wedge Q$	*Conjunction 3,4*
6		R	*Modus ponens 1,5*
7	$P \rightarrow R$		*Conditional Proof, 3–6*

This proof assumes that P implies Q and that P and Q together imply R. It shows under these assumptions that in fact P by itself implies R. The proof assumes for the purposes of argument that P is true, and shows that R follows. This is the subproof from steps 3–6. Note that the main assumptions numbered 1 and 2 are used freely within the subproofs, in the modus ponens steps at 4 and 6. Also note that the justification for conditional proof at step 7 appeals to the entire subproof from 3–6.

The other thing you often do is *indirect proof*. This captures reasoning by contradiction. In indirect proof, you begin a subproof by assuming that the conclusion you actually want to prove is false: $\neg A$. In this subproof, you derive the contradiction FALSE. The subproof shows that the assumption $\neg A$ is impossible, so in the outer proof you know that A must be true.

Here is a formal example of indirect proof. It needs the *contradiction rule*: if A is part of a proof and $\neg A$ is part of a proof, then you can infer FALSE there too. It also needs the *disjunction rule*: if A is part of a proof, then you can infer $A \vee B$ there too.

Example 3

1	$\neg P \vee \neg R \rightarrow Q$		*Premise*
2	$\neg Q$		*Premise*
3		$\neg P$	*Premise for Indirect Proof*
4		$\neg P \vee \neg R$	*Disjunction 3*
5		Q	*Modus ponens 1,4*
6		FALSE	*Contradiction 2,5*
7	P		*Indirect Proof, 3–6*

The argument assumes that Q would be true if either P or R was false, but that Q is not true. It uses indirect proof to conclude from this that P must be true. Again we see that the premises of the main proof, numbered 1 and 2, are used freely inside the subproofs, here at steps 5 and 6. And again we see that the rule that needs a subproof, indirect proof, points to the whole subproof in its justification.

2 Mechanical Proofs

Each of the connectives of propositional logic comes with rules that say how to infer that kind of formula and how to use that kind of formula. These simple rules are all you need to build proofs. For that reason, they are often used in computer systems that work with proofs. There is less to put into the computer implementation and the implementation can work with more constrained reasoning problems, which is usually more efficient. Here are all the rules, with explanations.

Example 4

$$\begin{array}{lll} L & A \wedge B & \\ \hline N & A & \textit{Simplification } L \end{array}$$

Example 5

$$\begin{array}{lll} L & A \wedge B & \\ \hline N & B & \textit{Simplification } L \end{array}$$

Example 6

$$\begin{array}{lll} L & A & \\ M & B & \\ \hline N & A \wedge B & \textit{Conjunction } L,M \end{array}$$

If a conjunction is true, each of the conjuncts is true. If each of the conjucts is true, the conjunction is true.

Example 7

$$\begin{array}{lll} L & A & \textit{Premise for Conditional Proof} \\ & \vdots & \\ M & B & \\ \hline N & A \rightarrow B & \textit{Conditional Proof L–M} \end{array}$$

Example 8

$$\begin{array}{lll} L & A \rightarrow B & \\ M & A & \\ \hline N & B & \textit{Modus Ponens L,M} \end{array}$$

If the consequent of a conditional would follow from the assumption of the antecedent, then the conditional must be true. If the antecedent of a true conditional is true, the consequent must be true.

Example 9

$$\begin{array}{lll} L & A & \textit{Premise for Indirect Proof} \\ & \vdots & \\ M & \text{FALSE} & \\ \hline N & \neg A & \textit{Indirect Proof L–M} \end{array}$$

Example 10

$$\begin{array}{lll} L & \neg A & \textit{Premise for Indirect Proof} \\ & \vdots & \\ M & \text{FALSE} & \\ \hline N & A & \textit{Indirect Proof L–M} \end{array}$$

Example 11

$$\begin{array}{lll} L & A & \\ M & \neg A & \\ \hline N & \text{FALSE} & \textit{Contradiction L,M} \end{array}$$

Example 12

$$\begin{array}{lll} M & \text{FALSE} & \\ \hline N & A & \textit{False L} \end{array}$$

If the assumption of A would lead to a contradiction, $\neg A$ must be true. If the assumption of $\neg A$ would lead to a contradiction, A must be true. A contradiction is A and $\neg A$. From a contradictory proof, anything follows.

Example 13

$$\begin{array}{lll} L & A & \\ \hline N & A \vee B & \textit{Disjunction L} \end{array}$$

Example 14

$$\begin{array}{lll} L & B & \\ \hline N & A \vee B & \textit{Disjunction L} \end{array}$$

Example 15

D	$A \vee B$		
L_1		A	*Premise for Case Analysis D*
	$\vdots$		
M_1		C	
L_2		B	*Premise for Case Analysis D*
	$\vdots$		
M_2		C	
N	C		*Case Analysis D,L_1–M_1,L_2–M_2.*

If A is true, $A \vee B$ must be true, and if B is true, $A \vee B$ must be true. If $A \vee B$ is true, and some conclusion C must be true if A is true, and must be true if B is true, then C must be true no matter what.

3 More relaxed proofs

What's important when people write down proofs formally is not to use a specific proof system. What's important is to be able to demonstrate correct conclusions. You can use any correct rule that is intuitively obvious—that nobody would doubt. For example, there are some derived rules involving negation that come in very handy for indirect proofs.

Example 16

L	$A \rightarrow B$	
M	$\neg B$	
N	$\neg A$	*Modus tollens L,M*

If A is true only when B is true, and B is false, then A must also be false.

Example 17

L	$A \vee B$	
M	$\neg B$	
N	A	*Disjunctive syllogism L,M*

If either A or B is true, but B is not true, then A must be true.

More generally, you can use results that you have derived earlier, or even results that you have derived by other methods. For example, since De Morgan's law gives you the logical equivalence between $\neg(A \vee B)$ and $\neg A \wedge \neg B$, you can reason this way in a proof:

Example 18

L	$\neg(A \vee B)$	
N	$\neg A \wedge \neg B$	*De Morgan's Law L*

We've seen examples where you use results from algebra and definitions of concepts, as well as logical equivalences in derivations.

4 Quantifiers

There are four quantifier rules.

Example 19

L	$P(a)$	
N	$\forall x P(x)$	*Universal generalization L*

You can only use universal generalization when no *premises* in the proof mention a. That means that a is arbitrary, and the same reasoning would go through for any object. So the universal statement must be true.

Example 20

L	$\forall x P(x)$	
N	$P(t)$	*Universal instantiation L*

There are no restrictions on t here. Because $P(x)$ holds for all objects t can be anything.

Example 21

L	$P(t)$	
N	$\exists x P(x)$	*Existential generalization L*

Again there is no restriction on t here. Once you know that $P(t)$ holds you know that $P(x)$ holds for some x, and that is enough to infer the existential statement.

Example 22

D	$\exists x P(x)$	
L	$\quad P(a)$	*Premise for Existential Instantiation*
	$\vdots$	
M	$\quad C$	
N	C	*Existential instantiation D,L–M.*

This has two restrictions. You can't make any assumptions about a other than $P(a)$ in the proof. That makes a an arbitrary individual. So whatever the thing is that turns out to have $P(x)$, the argument will work for it. And a can't occur in C either. That means that the conclusion doesn't depend on a, so it holds whatever it is that turns out to have $P(x)$. Since some x has $P(x)$, C must be true.

Here is a typical example of how the quantifier rules are used in combination.

Example 23

1	$\forall x(P(x) \rightarrow Q(x))$	*Premise*
2	$\exists x(P(x))$	*Premise*
3	$\quad P(a)$	*Premise for Existential Instantiation 2*
4	$\quad P(a) \rightarrow Q(a)$	*Universal Instantiation 1*
5	$\quad Q(a)$	*Modus ponens 4,3*
6	$\quad \exists x(Q(x))$	*Existential generalization 5*
7	$\exists x(Q(x))$	*Existential instantiation 2,3–6.*

If every P is a Q, and there is a P, then there is a Q. The inference says: let a be a P. It must also be a Q, so there is a Q.

5 Proof Terms (Optional)

Let's generalize the idea of a proof. Let's think instead about pieces of information about the world. Then the rules of proof give you ways of putting information together to draw conclusions. For example, if x is some information that guarantees that A is true, and y is some information that guarantees that B is true, then x and y together make up a piece of information that guarantees that $A \wedge B$ is true.

More interestingly, what kind of information do you need for $A \rightarrow B$? You can think of it as a function. If you give the function a piece of information that says that A is true, your proof of $A \rightarrow B$ will give you back a piece of information that says that B is true.

You can use this idea to give *terms* that spell out the content of the proof. Assumptions correspond to variables.

Example 24

1	$P \rightarrow Q$	*Premise*	f
2	$Q \rightarrow R$	*Premise*	g
3	P	*Premise*	x
4	Q	$mp(1,3)$	$mp(f,x)$
5	R	$mp(2,4)$	$mp(g,mp(f,x))$

Conditional proof corresponds to specifying an algorithm. The hypothesis is a variable for a new fact that could be supplied. The subproof constructs a new piece of information as a function of this variable. When you reason from the subproof to extend the main proof, you use this function as part of the inference.

Example 25

1	$P \wedge Q \rightarrow R$		*Premise*	f
2	$P \rightarrow Q$		*Premise*	g
3		P	*Premise*	z
4		Q	$mp(2,3)$	$mp(g,z)$
5		$P \wedge Q$	$cj(3,4)$	$cj(z,mp(g,z))$
6		R	$mp(1,5)$	$mp(f,cj(z,mp(g,z)))$
7	$P \rightarrow R$		$cp(3 \Rightarrow 6)$	$cp(z \Rightarrow mp(f,cj(z,mp(g,z))))$

When you build large proofs, you can sometimes build intermediate results that you don't really need. You can simplify these proofs to get rid of the extra steps. For example look at this proof.

Example 26

1	$P \wedge Q \rightarrow R$		*Premise*	f
2	$P \rightarrow Q$		*Premise*	g
3		P	*Premise*	z
4		Q	$mp(2,3)$	$mp(g,z)$
5		$P \wedge Q$	$cj(3,4)$	$cj(z,mp(g,z))$
6		R	$mp(1,5)$	$mp(f,cj(z,mp(g,z)))$
7	$P \rightarrow R$		$cp(3 \Rightarrow 6)$	$cp(z \Rightarrow mp(f,cj(z,mp(g,z))))$
8	P		*Premise*	w
9	R		$mp(7,8)$	$mp(cp(z \Rightarrow mp(f,cj(z,mp(g,z)))),w)$

This proof has P as an assumption. But it uses this assumption to prove R indirectly. First we prove $P \to R$ using conditional proof. And then we use modus ponens to derive R from this using the assumption of P.

We didn't really need to do conditional proof in this case. We could have just started from our main assumption of P, and derived R directly. The proof-term tells us how to get this simple proof. We have a term of the form:

$$mp(cp(F), a)$$

We've used a conditional proof made up of some function F, and then reasoned from this and another proof a using modus ponens. The proof we need should just be

$$F(a)$$

In other words, we should take the function F that we built and apply it to the argument a. In this case our overall proof term is:

$$mp(cp(z \Rightarrow mp(f, cj(z, mp(g, z)))), w)$$

So the simple proof should be

$$[z \Rightarrow mp(f, cj(z, mp(g, z)))](w)$$

or

$$mp(f, cj(w, mp(g, w)))$$

We can take this proof term and use it to reconstruct the whole proof that goes with it. Here it is:

Example 27

1	$P \wedge Q \to R$	*Premise*	f
2	$P \to Q$	*Premise*	g
3	P	*Premise*	w
4	Q	$mp(2,3)$	$mp(g, w)$
5	$P \wedge Q$	$cj(3,4)$	$cj(w, mp(g, w))$
6	R	$mp(1,5)$	$mp(f, cj(w, mp(g, w)))$