1 Proofs in propositional logic

1.1 A warm-up puzzle

Consider the following two rules:

$$\frac{A \wedge B \to C \qquad A}{B \to C}$$

$$\frac{A \wedge B \to C \qquad \neg A}{B \to C}$$

Are either of these rules sound? Why or why not?

It is not too difficult to answer this question if you just take a moment to think about what the rules are saying, intuitively.

Exercise 1. *Do this.*

1.2 A harder puzzle

Next consider the following two rules. Which of them is sound?

$$\frac{A \to B \vee C \qquad \neg C \wedge D \to C \qquad D \to C \vee A}{D \to B}$$

$$\frac{A \to B \vee C \qquad C \wedge D \to \neg C \qquad D \to C \vee A}{D \to B}$$

This question certainly looks much harder!

Of course, we could create a truth table for each rule and definitively answer the question. But with four variables and four compound formulas, it will be a pretty big truth table.

Instead, let's try to think about these rules logically.

Let's focus on the first rule:

$$\frac{A \to B \vee C \qquad \neg C \wedge D \to C \qquad D \to C \vee A}{D \to B}$$

If this rule is *not* sound, there must be some assignment to variables that makes the assumptions true, and the conclusion false.

The only way the conclusion $D \to B$ can be false is if $D = \top$ and $B = \bot$.

Substituting $D = \top$ into the second assumption gives $\neg C \wedge \top \to C$, which simplifies to $\neg C \to C$: if C is false, then C is true! This is a contradiction, so C cannot be false, C must be true, so that $C = \top$.

With $C = \top$, both other assumptions become true, regardless of what A is. So the rule is *unsound*, and we have an actual truth assignment that shows this.

Exercise 2. *Substitute the assignment $A = \bot$, $B = \bot$, $C = \top$, $D = \top$ into the first rule, and verify that it simplifies into* $\frac{\top \quad \top \quad \top}{\bot}$.

Next, let's look at the other rule:

$$\frac{A \to B \vee C \qquad C \wedge D \to \neg C \qquad D \to C \vee A}{D \to B}$$

In order for this rule to be unsound, we again need $D = \top$ and $B = \bot$ to make the conclusion false.

But this time, the second assumption becomes $C \wedge \top \to \neg C$, which simplifies to $C \to \neg C$: If C is true, then C is false. So C can't be true; we must have $C = \bot$.

With $C = \bot$, the third assumption becomes $\top \to \bot \vee A$, which simplifies to $\top \to A$, meaning A must be true. So $A = \top$.

But now the first assumption becomes $\top \to \bot \vee \bot$, which simplifies to $\top \to \bot$, which is false.

So there is no way that the conclusion can be false when all the assumptions are true.

Indeed, this rule is sound, and we have just proved this.

1.3 A better proof

The above argument showed the soundness of a rule without using proof tables. However, it was quite informal, tracking our intuitive thought process rather directly. In computer science, arguments should be given with maximum precision. Here is a better presentation of the same idea, written in "mathematical style".

Assumptions:
1. $A \to B \vee C$
2. $C \wedge D \to \neg C$
3. $D \to C \vee A$

Goal: $D \to B$

Proof. To show that $D \to B$ follows from the above assumptions, we will show that, if D is true, then B must also be true.

To that end, assume D is true. (We will now show that B is true.)

By the third assumption, since D is true, then $C \vee A$ is also true.

That is, either C is true or A is true.

Case 1: C is true. If C is true then, since D is true, so is the conjunction $C \wedge D$.

Then by the second assumption, C is false, which is a contradiction.

So this case is impossible.

Case 2: A is true. If A is true, then by the first assumption, $B \vee C$ must be true.

That is, either B is true, or C is true.

But we have already seen in the previous case that C can't be true.

The only remaining possibility is that B is true.

So in any circumstance, if D is true, then B must also be true.

That is, we have shown that $D \to B$ is true.

This was the goal, so our proof is complete.

Notice how reading the "mathematical proof" leaves no doubt about the claim that the conclusion follows from the assumptions. Every step is justified by the previous steps using small, unquestionable logical inferences.

Writing good proofs is an art. A theorem can have many different proofs. It often takes insight to find the right sequence of steps. In the above example, this insight came from the "intuitive" argument we discovered when we tried to see whether the rule was sound in the first place. The hard part, which requires a lot of practice to become good at, is to translate this intuitive understanding into "watertight" proof of the claim.

Fortunately, logic provides us with a small set of rules which in combination can be used to prove the soundness of any valid rule. Moreover, these rules are connected to the logical structure of the formula we are trying to prove, so they can also guide us in finding the right sequence of steps, based on the structure of the formula.

1.4 The structure of proofs

Let us look again at how the above proof was organized.

It started by clearly stating what the assumptions are, and what is the conclusion that we are trying to prove from these assumptions.

This is a general pattern, which you should always follow when writing proofs.

RULE 1. *Start every proof by stating the assumptions, and then stating the conclusion that is to be proved from these assumptions.*

Notice that, while the "goal" of the overall proof was $D \to B$, after the first step, we added a new assumption — *and a different goal.*

Afterwards, every step of the proof generated a new piece of knowledge (that a certain proposition is true) from the previous information.

Thus, after we assumed that D is true in the first step, in the next step we used the third assumption to generate the fact that $C \vee A$ is true.

The rule we used to generate this fact was *Modus Ponens*:

$$\frac{X \to Y \qquad X}{Y}\,\mathrm{MP}$$

(In words, Modus Ponens says that, if you know that $X \to Y$ is true, and you know that X is true, then you can conclude that Y is true. When we used this rule, we had $X = D$ and $Y = C \vee A$. We knew that $X \to Y$ is true from the third assumption, and we knew that X was true because we just assumed it in the previous step.)

Later, in Case 1, we used the fact that C is true and D is true to generate another fact, that $C \wedge D$ is true. The rule we used to generate this was *Conjunction Introduction*:

$$\frac{X \qquad Y}{X \wedge Y}$$

(In words, Conjunction Introduction says that if you know that X is true and you know that Y is true, then you also know that $X \wedge Y$ is true. When we used this rule, we had $X = C$ and $Y = D$. We knew that X was true because we were in Case 1, and we knew that Y is true because we assumed it at the beginning of the proof.)

A proof is basically a sequence of steps like this, where at every step a new fact is derived using one of the basic rules of logic. The point is to derive the fact that exactly matches the goal that was stated at the beginning.

RULE 2. *In every step of the proof, a new fact is generated from previous ones using one of the basic inference rules of logic. Every use of a rule needs to specify why the assumptions to the rule are satisfied, by pointing to the earlier place in the proof in which the corresponding formula above the line was shown to be true.*

For example, when we used Modus Ponens again in Case 2 (we used it with $X = A$ and $Y = B \vee C$), we pointed to the assumption 1 as satisfying the formula $X \to Y$ in the rule MP. The other formula needed for the rule, X, was generated immediately before using the rule, so we didn't need to point to any earlier place.

The rules of inference

Here are the most important rules of Propositional Logic:

Introduction Rules	Elimination Rules
$\wedge\text{-intro}\ \dfrac{X \quad Y}{X \wedge Y}$	$\dfrac{X \wedge Y}{X} \quad \dfrac{X \wedge Y}{Y}\ \wedge\text{-elim}$
$\vee\text{-intro}\ \dfrac{X}{X \vee Y} \quad \dfrac{Y}{X \vee Y}$	$\dfrac{X \vee Y \quad X \to Z \quad Y \to Z}{Z}\ \vee\text{-elim}$
$\to\text{-intro}\ \dfrac{\boxed{\begin{matrix} X \\ \vdots \\ Y \end{matrix}}}{X \to Y}$	$\dfrac{X \to Y \quad X}{Y}\ \to\text{-elim}$
$\bot\text{-intro}\ \dfrac{X \quad \neg X}{\bot}$	$\dfrac{\bot}{X}\ \bot\text{-elim}$

The names of the rules reflect how these rules are used in practice.

The introduction rules tell us how to *generate* (introduce) formulas of a specific shape. The elimination rules tell us how we can *consume* (eliminate) formulas of a specific shape.

For example, we used $\wedge$-introduction rule in order to generate the formula $C \wedge D$ (which we needed so that we could use the second assumption). This formula is a conjunction, and the introduction rule tells us how we can generate a formula of such shape $X \wedge Y$: we must first generate X and also generate Y.

Having generated the formula $C \wedge D$, we could now make use of the second assumption, which is an implication $X \to Y$ (with $X = C \wedge D$ and $Y = \neg C$).

The $\to$-elimination rule tells us how we can consume a formula of such shape $X \to Y$: to consume such a formula, we must first generate X — and the rule will generate Y.

1.5 Generating implications

The rule $\to$-intro, which tells us how to generate formulas of shape $X \to Y$, deserves a special discussion. This is the only rule for which the input (the stuff above the line) is not previously generated facts, but it is a *mini-proof*: a block of steps, which show how to generate Y if one adds a new assumption X.

Notice that this rule was used as the last step in the above proof. The goal had the shape $D \to B$; the only possible way to generate this formula was to use the $\to$-intro rule. This explains why the proof started by assuming that D was true, and then proving that B was true as well: this was simply giving the input to the $\to$-intro rule, with $X = D$ and $Y = B$.

The final step took as input the whole block of steps before it, starting from "To that end, assume D is true..." and ending in "...B must also be true." It is customary to mark the beginning and end of the block when using this rule, either by drawing a box around the block, or by placing some other kind of marker.

The most important thing to keep in mind in using this rule is that, *after a block is closed by using the $\to$-rule, no subsequent steps can ever make use of the assumption X or any other facts generated within the block.*

Basically, after the $\to$-intro rule is used, everything inside the box becomes locked off to the rest of the proof. This is because it might depend on the new assumption X, which is only relevant in proving the formula $X \to Y$, and is irrelevant in the rest of the proof.

Rule 3. *To prove an implication $X \to Y$, assume X and prove Y. If you have any other goals left to prove, no subsequent steps in the proof can refer to any facts generated under this assumption.*

1.6 Consuming disjunctions

Another rule that was used implicitly in the above proof is disjunction elimination. This occurred when we split into cases: we consumed the fact that $C \vee A$ is true, and as input we provided separate proofs that $C \to B$ and $A \to B$ are true, where B was the goal we were trying to prove when consuming the disjunction.

So really, the "proof by cases" part of the proof is nothing but an instance of the $\vee$-elim rule, with $X = C$, $Y = A$, and $Z = B$.

However, it should be noted that to use this rule, we had to briefly change our goal to $C \to B$ and $A \to B$, which we immediately unpacked by assuming C and proving B, and then assuming A and proving B again.

Rule 4. *To consume a disjunction, split the proof into cases.*

1.7 Using contradictions

You might object that in Case 1, we didn't really prove B, we simply showed that the case was impossible.

However, the $\perp$-rules show that, when one can find a contradiction, one can complete *any* goal. Here is a way to rewrite Case 1 so that it ends in the goal B:

Case 1: C is true. If C is true then, since D is true, so is the conjunction $C \wedge D$.

By the second assumption, $\neg C$ is true.

By the $\bot$-intro rule (with $X = C$), since C and $\neg C$ are true, $\bot$ is true.

By the $\bot$-elim rule (with $X = B$), B is true.

RULE 5. *If you managed to derive a contradiction, your proof of the current goal is finished.*

1.8 Excluded Middle

The final rule of propositional logic states that every proposition is either true or false:

$$\text{EM}\ \frac{}{X \vee \neg X}$$

This rule has *no assumptions*, which means that you can invoke it at any point in the proof, on any formula you want. Sometimes, you might want to use it on the goal. This is equivalent to doing *proof by contradiction*: in order to prove A, you may assume $\neg A$, and derive $\bot$.

This principle is motivated as follows. First, use excluded middle to derive $A \vee \neg A$. Next, use disjunction elimination on this, with $X = A, Y = \neg A, Z = A$ (the goal is still A). In the first case, if we assume A, we can certainly get A. In the second case, if we assume $\neg A$, and derive $\bot$, we can use $\bot$-elim to again get A. In either case, we get A, so disjunction elimination shows that A must be true.

Proofs by contradiction can be very efficient. However, it is generally advisable to avoid them whenever possible. The reason is that the principle which justifies it, the Excluded Middle rule, is not in any way connected to the structure of the formula. So it may be difficult to discover when is a good time to use it.

In contrast, all other inference rules correspond precisely to the logical structure of the formula involved. Thus, they can help guide us toward the right sequence of steps.

RULE 6. *To generate the goal from the assumptions, alternate between consuming the assumptions using the corresponding elimination rules, and generating the goal using the corresponding introduction rules. When the goal is an implication or a conjunction, use the introduction rule first. When the goal is a disjunction, use the introduction rule at the very end.*

EXERCISE 3. *Rewrite the above proof, numbering and explicitly stating which inference rule is being used at every step, and where the information needed to use the rule was first generated.*

EXERCISE 4. *Prove the soundness of the following rule, with the same level of precision as in the previous question:*

$$\frac{A \wedge B \to C \qquad D \vee (B \wedge \neg C) \qquad D \vee B \to A}{B \to D}$$