8.6: Proving Theorems

Definition: A *theorem* is a statement that can be proved independently of any premises.

Recall that the a *tautology* is a statement that is true on every assignment of truth values to its atomic components (hence true in every row of its truth table). It can be shown that our system of proof is *complete* in the following sense: every statement that is logically true is a theorem of our system of natural deduction.

But: how does one prove anything without any premises?

To prove a theorem you must use either CP or RAA.

If the theorem to be proved is a conditional, you will typically want to use CP (although, as always, RAA would also work):

Example 1: A proof of $\sim A \rightarrow ((A \vee B) \rightarrow B)$.

If the theorem to be proved isn't a conditional, use RAA:

Example 2: A proof of $\sim P \vee P$.

Note that, alternatively, we could have used CP to prove $P \rightarrow P$ (try it!) and then derived $\sim P \vee P$ directly by MI. There is always more than one way to do it!

In some cases, a combination of RAA and CP works best.

Example 3: A proof of $[(F \rightarrow G) \rightarrow F)] \rightarrow F$.

Other cases still might require embedding multiple assumptions one within the other to prove a theorem.

***Example 4*:** A proof of $[A \rightarrow (B \rightarrow C)] \rightarrow [(A \rightarrow B) \rightarrow (A \rightarrow C)]$.

Corresponding conditionals

There is an important connection between valid arguments and theorems. To understand it, we need the concept of a *corresponding conditional* for an argument.

If an argument has a single premise, the corresponding conditional is formed simply by taking the premise to be the antecedent and the conclusion to be the consequent. For example:

Argument: $\sim(\mathrm{A} \vee \sim\mathrm{B}) \;\therefore\; \mathrm{B}$

Corresponding conditional: $\sim(\mathrm{A} \vee \sim\mathrm{B}) \rightarrow \mathrm{B}$

If an argument has multiple premises, the corresponding conditional is formed by simply by taking the *conjunction* of the premises (in their given order) to be the antecedent and the conclusion to be the consequent. For example:

Argument: $\mathrm{P} \rightarrow \sim\mathrm{Q}, \mathrm{S} \vee \mathrm{Q}, \;\sim\mathrm{S} \;\therefore\; \sim\mathrm{P}$

Corresponding conditional: $(((\mathrm{P} \rightarrow \sim\mathrm{Q}) \bullet (\mathrm{S} \vee \mathrm{Q})) \bullet \sim\mathrm{S}) \rightarrow \sim\mathrm{P}$

Definition: If $p \therefore q$ is an argument with a single premise, then its corresponding conditional is $p \rightarrow q$. And if $p_1, \dots, p_n \therefore q$ is an argument with n premises (where $n > 1$), then its corresponding conditional is $r \rightarrow q$, where r is the conjunction of $p_1, \dots, p_n$.

Definition (sorta): The conjunction of two formulas p_1 and p_2 is of course $(p_1 \bullet p_2)$. The conjunction of three formulas p_1, p_2, p_3 is the conjunction of $(p_1 \bullet p_2)$ with p_3, i.e., $((p_1 \bullet p_2) \bullet p_3)$; the conjunction of four formulas p_1, p_2, p_3, p_4 is the conjunction of $((p_1 \bullet p_2) \bullet p_3)$ with p_4, i.e., $(((p_1 \bullet p_2) \bullet p_3) \bullet p_4)$; and so on.

It is easy to show that an argument is valid if and only if its corresponding conditional is a theorem. Hence, one can show an argument to be valid by proving its corresponding conditional.

Example 5: A proof that $\sim A \vee \sim B, C \rightarrow A, D \rightarrow B \therefore \sim C \vee \sim D$ is valid via a proof of its corresponding conditional.

$$\therefore (((\sim A \vee \sim B) \bullet (C \rightarrow A)) \bullet (D \rightarrow B)) \rightarrow (\sim C \vee \sim D)$$

1.	$((\sim A \vee \sim B) \bullet (C \rightarrow A)) \bullet (D \rightarrow B)$	Assume
2.	$(\sim A \vee \sim B) \bullet (C \rightarrow A)$	1 Simp
3.	$\sim A \vee \sim B$	2 Simp
4.	$C \rightarrow A$	2 Simp
5.	$D \rightarrow B$	1 Simp
6.	$\sim A \rightarrow \sim C$	4 Cont
7.	$\sim B \rightarrow \sim D$	5 Cont
8.	$\sim C \vee \sim D$	3, 6, 7 CD
9.	$(((\sim A \vee \sim B) \bullet (C \rightarrow A)) \bullet (D \rightarrow B)) \rightarrow (\sim C \vee D)$	1-8 CP

However, just because you *can* show that an argument is valid in this way doesn't mean that you *should*! For, typically, a proof for the argument is going to be shorter — indeed, typically, a proof for the argument will be *embedded* in the proof for its corresponding conditional! In particular, in the above proof, it is easy to see that lines 3-8 by themselves (appropriately renumbered and re-annotated) constitute a proof of the given argument.