Phil 320
<u>Chapter 14: Proofs and Completeness</u>

Note: Omit 14.3

I. Basic proof concepts. Soundness and completeness.

Proof procedure: A set of *rules* characterizing a *deduction* (finite sequence of steps) from Γ to D.

> *Soundness Theorem*: If D is deducible from Γ, then $\Gamma \models D$.
> *Completeness Theorem*: If $\Gamma \models D$, then D is deducible from Γ.

More generally, "semantic" concepts turn out to line up with "syntactic" (proof-theoretic) concepts:

<u>Semantic</u>	<u>Syntactic</u>
Implication: $\Gamma \models D$	*Deduction*: D is deducible from Γ
Unsatisfiability of Γ	*Inconsistency* (= *refutability*) of Γ
Validity of D	*Demonstrability* of D

- Concepts on the *semantic* side are all special cases of a more general concept, *securing*: Γ *secures* Δ iff each interpretation that makes all sentences in Γ true makes at least one sentence in Δ true.

  Notes:
  1) If Γ is the empty set ϕ, *any* interpretation makes all sentences in Γ true.
  2) If Δ is the empty set ϕ, *no* intepretation makes at least one sentence in Δ true.
  3) Expression of previous concepts in terms of securing:

$\Gamma \models D$	iff	Γ secures $\{D\}$
Γ is unsatisfiable	iff	Γ secures ϕ
D is valid	iff	ϕ secures $\{D\}$

- Concepts on the *syntactic* side are all special cases of the more general concept of *derivation*.

  The primary objects of derivation will be *sequents* of the form $\Gamma \Rightarrow \Delta$, where Γ and Δ are both *finite* sets. Each sequent occupies one line of a derivation. There are inference rules for deriving new sequents from old ones. First, for finite sets:

D is *deducible* from Γ	iff	$\Gamma \Rightarrow \{D\}$ is derivable	
Γ is *inconsistent*	iff	$\Gamma \Rightarrow \phi$ is derivable	[*inconsistent* = *refutable*]
D is *demonstrable*	iff	$\phi \Rightarrow \{D\}$ is derivable	

  Infinite sets: Δ *derivable* from Γ if a finite subset Δ_0 of Δ is derivable from a finite subset Γ_0 of Γ.

- Chapter 14 proves (for finite sets):

  Soundness Theorem: Every derivable sequent is secure.
  Completeness Theorem: Every secure sequent is derivable.

  By **Compactness**, however, the results extend to infinite sets:

  Δ derivable from Γ iff Δ_0 derivable from Γ_0 (as above), some Δ_0, Γ_0
  iff Γ_0 secures Δ_0 (soundness and completeness), for some Γ_0 and Δ_0
  iff Γ secures Δ (using Compactness)

Note: Soundness and completeness can be verified for any correct proof system. Sequents are convenient for doing the metalogical proofs of soundness and completeness, but less convenient in derivations.

II. Sequents and derivation rules

A *derivation* of $\Gamma \Rightarrow \Delta$ is a sequence of lines with the following properties:

(1) Each line is a sequent.
(2) The last line is $\Gamma \Rightarrow \Delta$.

(3) Every line is either of the form $\{A\} \Rightarrow \{A\}$ and justified by (R0), or must follow from previous lines via one of the other *rules of inference*.

Again for convenience, we omit & and $\forall$, assuming only the logical symbols ~, $\vee$, $\exists$, = plus parentheses and commas. The inference rules are as in Table 14-4 and correspond to familiar patterns of reasoning.

Conventions to make life easier:

1) Omit outermost parentheses if meaning is evident: $A \vee B$ instead of $(A \vee B)$.
2) Omit curly brackets: write $A \Rightarrow A, B$ instead of $\{A\} \Rightarrow \{A, B\}$.
3) Empty set (on either side): just put no symbols. Write $\Rightarrow A, {\sim}A$ instead of $\phi \Rightarrow A, {\sim}A$.
4) When combining finite sets, use commas instead of $\cup$: $A, B \Rightarrow A$ instead of $\{A\}\cup\{B\}\Rightarrow A$.
5) Provide a *justification* (rule plus lines) for each step (not 'officially' part of the derivation).

Example: Addition. Derive: $A \Rightarrow A \vee B$

1.	$A \Rightarrow A$	(R0)
2.	$A \Rightarrow A, B$	(R1), 1
3.	$A \Rightarrow A \vee B$	(R3), 2

III. Examples of derivations

Example 2: Duplication. Derive: $A \vee A \Rightarrow A$

1.	$A \Rightarrow A$	(R0)
2.	$A \vee A \Rightarrow A$	(R4), 1, 1

Example 3: Simplification. Derive: $A\&B \Rightarrow B$ (**Work bottom-up**)

1.	$B \Rightarrow B$	(R0)
2.	$A, B \Rightarrow B$	(R1), 1
3.	$A \Rightarrow {\sim}B, B$	(R2a), 2
4.	$\Rightarrow {\sim}A, {\sim}B, B$	(R2a), 3
5.	$\Rightarrow ({\sim}A \vee {\sim}B), B$	(R3), 4
6.	${\sim}({\sim}A \vee {\sim}B) \Rightarrow B$	(R2b), 5

Example 4: Modus ponens. Derive: $A, A \rightarrow B \Rightarrow B$ (Clue: derive two sequents needed for (R4).)

1.	$A \Rightarrow A$	(R0)
2.	$A \Rightarrow A, B$	(R1), 1
3.	$A, {\sim}A \Rightarrow B$	(R2b), 2
4.	$B \Rightarrow B$	(R0)
5.	$A, B \Rightarrow B$	(R1), 4
6.	$A, {\sim}A \vee B \Rightarrow B$	(R4), 3, 5

Example 5: Quantifier rules. Derive: $\exists xFx, \forall x(Fx \rightarrow Gx) \Rightarrow \exists xGx$

…

6.	$Fc, {\sim}Fc \vee Gc \Rightarrow Gc$	(R4), 3, 5 (Exactly as for MP, above)
7.	$Fc \Rightarrow {\sim}({\sim}Fc \vee Gc), Gc$	(R2a)
8.	$Fc \Rightarrow {\sim}({\sim}Fc \vee Gc), \exists xGx$	(R5)
9.	$Fc \Rightarrow \exists x{\sim}({\sim}Fx \vee Gx), \exists xGx$	(R5)
10.	$\exists xFx \Rightarrow \exists x{\sim}({\sim}Fx \vee Gx), \exists xGx$	(R6)
11.	$\exists xFx, {\sim}\exists x{\sim}({\sim}Fx \vee Gx) \Rightarrow \exists xGx$	(R2b)

Note: There are some important 'tricks' that help here – e.g., do the right side quantifier introductions first in order to be able to apply (R6) – but we won't dwell on this. The text contains many additional examples, including some using the rules for =.

IV. Soundness

Theorem 14.1: If $\Gamma \Rightarrow \Delta$ is derivable, then Γ secures Δ.

Proof: Every (R0) sequent $\{A\} \Rightarrow \{A\}$ is secure: if Γ makes A true, then Γ makes A true.

We have to show that each of (R1) - (R9) is sound, i.e., 'preserves' security. Then at every step in our derivation, we have a secure sequent. It follows that the final step is secure. The proof is almost entirely straightforward, because the rules were constructed with soundness in mind. I will only do a few steps.

(R1) is sound: if $\Gamma \Rightarrow \Delta$ is secure, then $\Gamma' \Rightarrow \Delta'$ is secure. For if $M \models \Gamma'$, then $M \models \Gamma$ (since M makes each sentence of Γ' true and Γ is a subset of Γ'), and so $M \models D$ for some D in Δ and hence in Δ' (since Δ is a subset of Δ').

(R2a) is sound: suppose $\Gamma, A \Rightarrow \Delta$ is secure. Suppose $M \models \Gamma$. If $M \models \sim A$, then we have the result that M makes true a sentence D in $\{\sim A\} \cup \Delta$. Otherwise, we must have $M \models A$ and hence it follows that $M \models D$ for some D in Δ. But then D is in $\{\sim A\} \cup \Delta$. So either way, the sequent $\Gamma \Rightarrow \{\sim A\} \cup \Delta$ is secure.

(R2b) is sound: suppose $\Gamma \Rightarrow \{A\} \cup \Delta$ is secure. Suppose $M \models \Gamma \cup \{\sim A\}$. Since $M \models \Gamma$, M makes true some D in $\{A\} \cup \Delta$. But not A, since $M \models \sim A$. Hence, D must be in Δ. So $\Gamma \cup \{\sim A\} \Rightarrow \Delta$ is secure.

(R4) is sound: suppose the two sequents $\Gamma, A \Rightarrow \Delta$ and $\Gamma, B \Rightarrow \Delta$ are secure. Suppose now that $M \models \Gamma, A \vee B$. Then $M \models \Gamma$ and either $M \models A$ or $M \models B$. In either case, M must make true some sentence in Δ, and thus $\Gamma, A \vee B \Rightarrow \Delta$ is secure.

(R6) is sound: suppose $\Gamma, A(c) \Rightarrow \Delta$ where c is a constant not in Γ or Δ or $A(x)$. Suppose that $M \models \Gamma, \exists x A(x)$. Then $M \models \Gamma$, and $M \models \exists x A(x)$. This means that for some m in the domain, if we pick any c not in $A(x)$ we have $M^c{}_m \models A(c)$. If in addition c is not in Γ or Δ, then Extensionality tells us $M^c{}_m$ does not change the truth-values of sentences in Γ and Δ from what M assigns them. In particular, $M^c{}_m \models \Gamma$ and we have $M^c{}_m \models A(c)$, so that $M^c{}_m \models D$ for some D in Δ. But then $M \models D$ as well, and thus $\Gamma, \exists x A(x) \Rightarrow \Delta$ is secure.

This illustrates the idea; none of the remaining steps is harder than the proof for (R6). ■

V. Completeness

Theorem 14.2: Every secure sequent $\Gamma \Rightarrow \Delta$ is derivable.

Preliminaries: Γ and Δ are finite sets, but the result extends to infinite sets, as noted earlier. So suppose $\Gamma=\{C_1,\ldots,C_m\}$ and $\Delta=\{D_1,\ldots,D_n\}$. Write $\sim\Delta$ for the set of *negated* members of Δ, i.e., $\sim\Delta=\{\sim D_1,\ldots,\sim D_n\}$.

First:	Γ secures Δ	iff	Γ implies $D_1 \vee \ldots \vee D_n$	
		iff	$\Gamma \cup \{\sim(D_1 \vee \ldots \vee D_n)\}$ is unsatisfiable	
		iff	$\Gamma \cup \sim\Delta$ is unsatisfiable	
	$\Gamma \Rightarrow \Delta$ is derivable	iff	$C_1,\ldots,C_m \Rightarrow D_1,\ldots,D_n$	
		iff	$C_1,\ldots,C_m,\sim D_1 \Rightarrow D_2,\ldots,D_n$	(R2a $\rightarrow$ and R2b $\leftarrow$)
		iff	$C_1,\ldots,C_m,\sim D_1, \sim D_2 \Rightarrow D_3,\ldots,D_n$	(same justification)
		…		
		iff	$C_1,\ldots,C_m, \sim D_1,\ldots,\sim D_n \Rightarrow$	(same justification)
		iff	$\Gamma \cup \sim\Delta$ is inconsistent (i.e., refutable)	

So to prove that "Γ secures Δ implies $\Gamma \Rightarrow \Delta$ is derivable", it's good enough to prove that any unsatisfiable set is inconsistent, or equivalently, any consistent set is satisfiable.

Next: Recall the **Model Existence Lemma (Lemma 13.3)** of chapter 13: Suppose L is a language and L+ is obtained by adding infinitely many constants to L. If S^* is a set of sets of sentences of L+ having the satisfaction properties (S0) - (S8), then every set of sentences of L in S^* has a model in which each element of the domain is the denotation of some closed term of L+.

We used this to prove **Compactness**, and we use it again. We need only show that if S is the set of all *consistent* sets in a language, then S has the satisfaction properties. For Lemma 13.3 then tells us that every consistent set has a model, i.e., is satisfiable. So we verify (S0) - (S8) for S.

Proof: [In each case, we show that if the property failed for some Γ in S, then $\Gamma \Rightarrow \phi$ would be derivable, violating the consistency of Γ. Note that we sometimes write $\Gamma \Rightarrow \phi$ as just $\Gamma \Rightarrow$.]

(S0) [If Γ in S, Γ_0 a subset of Γ, then Γ_0 in S.] This means: if we can't derive $\Gamma \Rightarrow \phi$, then we can't derive $\Gamma_0 \Rightarrow \phi$.

This follows, since if we could derive $\Gamma_0 \Rightarrow \phi$, then $\Gamma \Rightarrow \phi$ would be derivable by applying (R1).

(S1) [If Γ in S, for no A are both A and $\sim A$ in Γ.] If A and $\sim A$ were in Γ, we would be able to derive $\Gamma \Rightarrow \phi$, contradicting Γ in S:

$A \Rightarrow A$	(R0)
$A, \sim A \Rightarrow$	(R2b)
$\Gamma \Rightarrow$	(R1)

(S2) [If Γ is in S and $\sim\sim B$ in Γ, then $\Gamma \cup \{B\}$ in S.] For if not, then we could derive

$\Gamma, B \Rightarrow \phi$	and hence	
$\Gamma \Rightarrow \sim B$	(R2a)	
$\Gamma, \sim\sim B \Rightarrow \phi$	(R2b)	contradicting $\sim\sim B$ in Γ and NOT $\Gamma \Rightarrow \phi$.

(S3) [If Γ is in S and $B \vee C$ is in Γ, then either $\Gamma \cup \{B\}$ is in S or $\Gamma \cup \{C\}$ is in S.] If not, then we have the derivation

$\Gamma, B \Rightarrow \phi$	
$\Gamma, C \Rightarrow \phi$	
$\Gamma, B \vee C \Rightarrow \phi$	(R4), contradiction (since $B \vee C$ is in Γ).

(S4) [If Γ is in S and $\sim(B \vee C)$ is in Γ, then both $\Gamma \cup \{\sim B\}$ and $\Gamma \cup \{\sim C\}$ are in S.] Suppose that $\Gamma \cup \{\sim B\}$ is not in S (a similar argument for $\sim C$). Then we have the derivation:

$\Gamma, \sim B \Rightarrow \phi$	
$\Gamma \Rightarrow B$	(R9a)
$\Gamma \Rightarrow B, C$	(R1)
$\Gamma \Rightarrow B \vee C$	(R3)
$\Gamma, \sim(B \vee C) \Rightarrow$	(R2b), contradiction (since $\sim(B \vee C)$ is in Γ).

(S5) [If Γ is in S and $\exists xB(x)$ is in Γ, and c does not appear in Γ or $\exists xB(x)$, then $\Gamma \cup \{B(c)\}$ is in S.] Suppose not. Then:

$\Gamma, B(c) \Rightarrow$	
$\Gamma \cup \{\exists xB(x)\} \Rightarrow$	(R6), contradiction (since $\exists xB(x)$ is in Γ).

(S6) [If Γ is in S and $\sim\exists xB(x)$ is in Γ, then for every closed term t, $\Gamma \cup \{\sim B(t)\}$ is in S.] Suppose not. Then for some closed term t:

$\Gamma, \sim B(t) \Rightarrow$	
$\Gamma \Rightarrow B(t)$	(R9a)
$\Gamma \Rightarrow \exists xB(x)$	(R5)
$\Gamma, \sim\exists xB(x) \Rightarrow$	(R2b), contradiction (since $\sim\exists xB(x)$ is in Γ).

(S7) [If Γ is in S, then $\Gamma \cup \{t = t\}$ is in S for any closed term t.] Suppose not. Then for some such t,

$\Gamma, t{=}t \Rightarrow$	
$\Gamma \Rightarrow$	(R7), contradiction.

(S8) [If Γ is in S and $B(s)$ and $s{=}t$ are in Γ, then $\Gamma \cup \{B(t)\}$ is in S.] Suppose not. Then

$\Gamma, B(t) \Rightarrow$	
$\Gamma \Rightarrow \sim B(t)$	(R2a)
$\Gamma \cup \{s = t\} \Rightarrow \sim B(s)$	(R8a)
$\Gamma, s{=}t, B(s) \Rightarrow$	(R9b), contradiction (since $s{=}t$ and $B(s)$ are in Γ). ■