Formal Proofs

Computability and Logic

General Idea of Proof

- A sequence of statements, starting with premises, followed by intermediate results, and ended by the conclusion, where each of the intermediate results, and the conclusion itself, is an *obvious* consequence from (some of) the premises and previously established intermediate results.

Inference Rules

- Formal proof systems of logic define a finite set of inference rules that reflect ‘baby inferences’.
- There are many formal systems of logic, each with their own set of inference rules.
- Moreover, there are several different types of formal proof systems:
  - Axiom Systems
  - Sequent Systems
  - Natural Deduction Systems
  - other

Axiom Systems

- Axiom systems most closely mirror the informal definition of a proof as a sequence of statements.
- In axiom systems, a formal proof is exactly that: a sequence of statements
- Each statement in the proof is either an assumption (premise), an instantiation of a general axiom, or the result of applying an inference rule to any of the previous statements.
- The axioms in axiom systems usually express inference principles in conditional format. As a result, axiom systems often come with only 1 rule of inference: Modus Ponens.

Sequent Systems

- In a sequent system, all inferences are the inference of sequents from other sequents.
- A sequent is a structure $\{\varphi_{1\,,}, \ldots ,\varphi_n\} \vDash \phi$ making the claim that ϕ is a logical consequence of the set of statements $\{\varphi_{1\,,}, \ldots ,\varphi_n\}$
- A proof in a sequent system is a sequence of sequents.
- Slate implements a sequent system.

Natural Deduction Proof Systems

- Natural Deduction proof systems try to mirror our 'natural' way of reasoning most closely
- Proofs are structured sequences of statements
  - Many inferences are from statements to other statements, resulting in linear sequences of statements
  - However, sometimes additional assumptions are made ('suppose …'), from which further inferences can be made. Thus one gets linear sequences of statements within linear sequences of statements: subproofs
  - Inference rules infer statements from other statements and from subproofs as a whole

Some Very Basic Inference Rules

$P \wedge Q$

P (or Q)

Simplification

P (or Q)

$P \vee Q$

Addition

P

Q

$P \wedge Q$

Conjunction

What Makes something an Inference Rule?

- A formal system can define any inference from a set of statements to another statement as an inference rule.
  - The rule just needs to be formally defined: “If you have a statement that looks like this, then you can infer a statement that looks like that”
  - They are syntactical
- However, the idea is that:
  - The inference rule reflects a valid inference
  - The inference rule reflects a simple/intuitive inference

Some Other Important (Valid) Inference Patterns

$P \lor Q$

$\neg P$

Q

Disjunctive Syllogism

$P \lor \neg P$

Law Of Excluded Middle

$\neg(P \land Q)$

P

$\neg Q$

Exclusion

Some Invalid Inference Patterns

$$\frac{P \vee Q}{P \wedge Q}$$

Modus Bogus

$$\frac{\quad}{P}$$

Hokus Ponens!

Some Rules Involving Conditionals

$P \rightarrow Q$

P

Q

Modus Ponens

Valid!

$P \rightarrow Q$

$\neg Q$

$\neg P$

Modus Tollens

$P \rightarrow Q$

Q

P

Affirming the Consequent

Invalid!

$P \rightarrow Q$

$\neg P$

$\neg Q$

Denying the Antecedent

Some Other Important Patterns

$P \rightarrow Q$

$Q \rightarrow R$

$P \rightarrow R$

Valid!

Hypothetical Syllogism (or Chain Argument)

$P \rightarrow Q$

$R \rightarrow Q$

$P \rightarrow R$

Invalid!

Undistributed Middle

Some More

Constructive Dilemma	Destructive Dilemma
$P \vee Q$	$\neg R \vee \neg S$
$P \rightarrow R$	$P \rightarrow R$
$Q \rightarrow S$	$Q \rightarrow S$
$R \vee S$	$\neg P \vee \neg Q$

Both Valid!

More Yet …

$P \rightarrow Q$

$(P \wedge R) \rightarrow Q$

Strengthening the Antecedent

$P \rightarrow Q$

$(P \vee R) \rightarrow Q$

Weakening the Antecedent

Valid!

Invalid!

$P \rightarrow Q$

$P \rightarrow (Q \vee R)$

Weakening the Consequent

$P \rightarrow Q$

$P \rightarrow (Q \wedge R)$

Strengthening the Consequent

Reiteration

P

———————

P

Justification

- To make a formal proof readable (consumable), you provide a *justification*.
- Thus, for each statement that you infer, you indicate:
  - which other statements you infer that new statement from
  - which inference rule you use
- To help refer to previous statements, we are going to number the statements.

Example Formal Proof

1.	$H \vee B$	A.
2.	$H \rightarrow A$	A.
3.	$\sim A$	A.
4.	$\sim H$	2, 3 MT
5.	B	1, 4 DS

Natural Deduction: Subproofs

- At any time during a proof, a subproof may be started by making an additional assumption which can then be used to draw further inferences.
- The subproof may be ended at any time. When it is ended, the *individual* statements from the subproof can no longer be used to infer others.
- Subproofs demonstrate that certain statements can be inferred when an additional assumption is made, and this result can be used in the proof itself. That is, the subproof *as a whole* can be used to infer other statements.

Important Uses of Subproofs

- Subproofs are used to formalize the following important proof techniques we commonly use:
  - Proof by Contradition: Assume something P. Show that this assumption leads to a contradiction. Conclude P is not true
  - Proof by Cases: When you know that one of a finite set of cases applies, assume eah of the cases individually. If something Q follows in each case, then infer Q.
  - Conditional Proof: If something Q can be inferred by making assumption P, then we can conclude ‘If P then Q’

Proof by Contradiction

$$
\begin{array}{l}
\quad P \\
\quad \vdots \\
\quad \bot \\
\neg P
\end{array}
$$

Proof by Cases

$P_1 \vee \ldots \vee P_i \vee \ldots \vee P_n$

P_1

$\vdots$

Q

$\Downarrow$

P_n

$\vdots$

Q

Q

Conditional Proof

$$
\begin{array}{|l}
\begin{array}{|l}
P \\ \hline
\vdots \\
Q
\end{array} \\
P \rightarrow Q
\end{array}
$$

Subproofs and Scope

- An additional line is used to indicate the start and end of the subproof.
- The line can also be seen as the *scope* of the additional assumption made at the start of the subproof: every statement within that scope is inferred from the truth of that assumption and all previous assumptions.
- The line of the proof itself can be seen in exactly this way as well. Therefore, there is no real difference between subproofs and proofs.

Subproofs within Subproofs

- Within any subproof, another subproof can be started.
- Subproofs within subproofs must be ended before the original subproof is ended.
- The general rule is: one can use as justification all and only statements that is either one of the assumptions whose scope one is working in, or some statement inferred from those.

F: A 'Fitch'-style Natural Deduction Proof System

- The formal system that our book uses is called *F*.
- *F* has 2 inference rules for each connective:
  - *Introduction*: A rule to infer a statement with that connective as its main connective
  - *Elimination*: A rule to infer something from a statement with that connective as its main connective.
- Formal systems with these two types of inference rules are called 'Fitch'-style systems.

How to Do Modus Tollens in F

Pattern:

$\varphi \rightarrow \psi$

$\neg\psi$

$\neg\varphi$

Proof:

1.	$\varphi \rightarrow \psi$	
2.	$\neg\psi$	
3.	$\quad \varphi$	
4.	$\quad \psi$	1,3 $\rightarrow$ Elim
5.	$\quad \bot$	2,4 $\bot$ Intro
6.	$\neg\varphi$	3-5 $\neg$ Intro

$\wedge$ Elim

$$P_1 \wedge P_2 \wedge \ldots \wedge P_n$$

$$\vdots$$

$$P_i$$

$\wedge$ Intro

P_1

$\Downarrow$

P_n

$P_1 \wedge P_2 \wedge \ldots \wedge P_n$

$\vee$ Intro

$$\begin{array}{|l} P_i \\ \vdots \\ P_1 \vee \ldots \vee P_i \vee \ldots \vee P_n \end{array}$$

$\vee$ Elim

$P_1 \vee \ldots \vee P_i \vee \ldots \vee P_n$

P_1

$\vdots$

Q

$\Downarrow$

P_n

$\vdots$

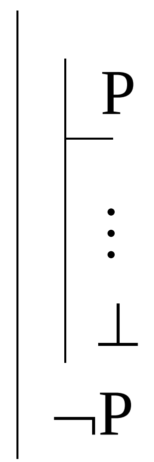
Q

Q

¬ Elim

$$\begin{array}{|l} \neg\neg P \\ \vdots \\ P \end{array}$$

¬ Intro



⊥ Elim

	$\bot$
	$\vdots$
	P

⊥ Intro

$$\left|\begin{array}{l} P \\ \Downarrow \\ \neg P \\ \vdots \\ \bot \end{array}\right.$$

$\rightarrow$ Elim

$$
\begin{array}{|l}
P \rightarrow Q \\
\Downarrow \\
P \\
\vdots \\
Q
\end{array}
$$

$\rightarrow$ Intro

P

$\vdots$

Q

$P \rightarrow Q$

$\leftrightarrow$ Elim

$P \leftrightarrow Q$ (or $Q \leftrightarrow P$)

$\Downarrow$

P

$\vdots$

Q

↔ Intro

P

⋮

Q

⇓

Q

⋮

P

$P \leftrightarrow Q$