University of Malta
BSc(Hons.) IT Year I

Introduction to Logic and Logic Programming

Lecture 8

Proof Systems

- System L
- Definition of Proof and Deduction
- Natural Deduction
- Fitch System

Department of Computer Science and AI
1988/9

System L

- **The Language**

  A sentence $\mathcal{F}$ is either

  - atomic (denoted by a propositional variable)
  - of the form $-\mathcal{G}$ where $\mathcal{G}$ is a sentence
  - of the form $\mathcal{G} \rightarrow \mathcal{H}$ where $\mathcal{G}$ and $\mathcal{H}$ are sentences

- **The Axiom Schemas**

  A1 $\mathcal{F} \rightarrow (\mathcal{G} \rightarrow \mathcal{F})$

  A2 $(\mathcal{F} \rightarrow (\mathcal{G} \rightarrow \mathcal{H})) \rightarrow (\mathcal{F} \rightarrow \mathcal{G}) \rightarrow (\mathcal{F} \rightarrow \mathcal{H}))$

  A3 $(-\mathcal{F} \rightarrow -\mathcal{G}) \rightarrow (\mathcal{G} \rightarrow \mathcal{F})$

- **Inference Rule.** Modus ponens. Given $\mathcal{F}$ and $\mathcal{F} \rightarrow \mathcal{G}$ we can derive $\mathcal{G}$.

Definitions
Proof, Theorem

Definition. A *proof* in a system is a sequence of formulas of that system such that each formula is either:

- An axiom or an instance of an axiom schema
- Derivable from earlier formulas in the sequence using one of the inference rules.
- An assumption.

Definition. A formula $\mathcal{P}$ is a *theorem of the system* if there is a proof of $\mathcal{P}$ in the system. We write

$$\vdash_\sigma \mathcal{P}$$

To indicate that $\mathcal{P}$ is a theorem within a certain system σ. The subscript will be omitted when the context permits it.

Checkpoint

What is the difference between $\vdash \mathcal{P}$ and $\models \mathcal{P}$ for any sentence $\mathcal{P}$?

- $\vdash \mathcal{P}$ means that $\mathcal{P}$ is a theorem of the system, i.e. can be formally derived from within the system.
- $\models \mathcal{P}$ means that for all possible interpretations, $\mathcal{P}$ comes out true. In other words, $\mathcal{P}$ is logically true (or a tautolology).

Notation for Proofs

A proof is a **sequence of formulas** each of which is annoted with

- a **line number** (so that we can refer to it).
- a justification (which tells us how that formula was derived). This must be one of the following:

  A_n : The line is an instance of axiom n, together with the relevant subsitution.

  MP n,m : the line was obtained as an immediate consequence of lines n and m by MP.

  Ass : that line is an assumption.

Examples of Substitution within Axiom Schemas

A1. $\mathcal{F} \rightarrow (\mathcal{G} \rightarrow \mathcal{F})$
A2. $(\mathcal{F} \rightarrow (\mathcal{G} \rightarrow \mathcal{H})) \rightarrow (\mathcal{F} \rightarrow \mathcal{G}) \rightarrow (\mathcal{F} \rightarrow \mathcal{H}))$

- Substitute $\{\mathcal{F}/P,\ \ \mathcal{G}/P\}$ in A1

  answer $= P \rightarrow (P \rightarrow P)$

- Substitute $\{\mathcal{F}/P,\ \ \mathcal{G}/(P \rightarrow Q)\}$ in A1

  answer $= P \rightarrow ((P \rightarrow Q) \rightarrow P)$

- Substitute $\{\mathcal{F}/P,\ \ \mathcal{G}/(P \rightarrow P),\ \ \mathcal{H}/P\ \}$ in A2.

  answer $=$

  $(P \rightarrow ((P \rightarrow P) \rightarrow P) \rightarrow$
  $((P \rightarrow (P \rightarrow P)) \rightarrow (P \rightarrow P))$

Example Proof 1 (no assumptions)

Below we prove that $\vdash (P \rightarrow P)$

Recall axiom schemata 1 and 2:

A1. $\mathcal{F} \rightarrow (\mathcal{G} \rightarrow \mathcal{F})$
A2. $(\mathcal{F} \rightarrow (\mathcal{G} \rightarrow \mathcal{H})) \rightarrow (\mathcal{F} \rightarrow \mathcal{G}) \rightarrow (\mathcal{F} \rightarrow \mathcal{H}))$

1. $(P \rightarrow ((P \rightarrow P) \rightarrow P) \rightarrow$
   $((P \rightarrow (P \rightarrow P)) \rightarrow (P \rightarrow P))$
   [A2 $\mathcal{F}/P; \mathcal{H}/P;$ $\mathcal{G}/P \rightarrow P$]

2. $P \rightarrow ((P \rightarrow P) \rightarrow P)$ [A1 $\mathcal{F}/P,$ $\mathcal{G}/P \rightarrow P$]

3. $((P \rightarrow (P \rightarrow P)) \rightarrow (P \rightarrow P))$ [MP 1,2]

4. $(P \rightarrow (P \rightarrow P))$ [A1 $\mathcal{F}/P; \mathcal{G}/P$]

5. $(P \rightarrow P)$ [MP 3,4]

Definition: Deduction

A notion closely related to proof is that of *deduction*. A proof is derived only from the axioms. A deduction allows the possibility of *additional assumptions*.

Definition. A deduction in a system is a sequence of formulas such that each formula is either

- an axiom or instance of an axiom schema
- derivable from earlier formulas in the sequence using an inference rule.
- an assumption

To indicate that $\mathcal{P}_n$ is derived from assumptions $\mathcal{P}_1\mathcal{P}_2,\ldots,\mathcal{P}_{n-1}$ we write

$$\mathcal{P}_1\mathcal{P}_2,\ldots,\mathcal{P}_{n-1} \vdash \mathcal{P}_n$$

Notation

Where appropriate, we employ the notation

$$\Gamma \vdash \mathcal{P}$$

to mean that $\mathcal{P}$ is deducible from the assumptions Γ. Note that Γ is a set, so that if we wanted to indicate $\mathcal{P}$ was derivable from a set of assumptions including a particular formula f, we might write

$$\Gamma \cup \{f\} \vdash \mathcal{P}$$

If Γ is the empty set, we write

$$\vdash \mathcal{P}$$

to indicate that p is a theorem. Strictly, we should write $\vdash_\sigma$ to show that the corresponding proof is carried out within System σ.

Remarks on System L

- System is simple to specify, therefore easy to prove things about.

- In particular, it is easy to show that System L is *complete* and *sound*. These two properties make it legitimate and useful from the logical point of view.

- One way to show that other systems are complete and sound is to show that they are equivalent, in some sense, to System L.

- It is very difficult to carry out proofs within System L

Natural Deduction Systems

- Natural deduction systems have the opposite properties to System L
- They employ a richer language with a full set of connectives.
- They employ a large set of inference rules that correspond, in principle, to "natural" patterns of reasoning.

Patterns of Reasoning in Natural Deduction Systems

Each connective in the language gives rise to a legitimate pattern of reasoning associated with its introduction or elimination. We distinguish between:

1. **Valid inference steps:** simple entailments between pairs of sentences. Examples of such steps are: double negation, conjunction elimination.

2. **Proof Methods:** longer patterns of inference that are allowed by the new expressions. Examples of such steps are proof by cases, proof by contradiction.

Valid Inference Steps

- **Double Negation:** from --P infer P or vice versa.
- **Conjunction Elimination:** if we have already proved a conjunction such as P & Q , infer any of the conjuncts alone (e.g. Q) from the same premises. The reason is obvious: the conjunction cannot be true without all the conjuncts being true as well.
- **Conjunction introduction:** Suppose we have proved P and proved Q. Then infer P & Q: in general, if we want to prove a conjunction, we can go about it by proving each conjunct separately.
- **Disjunction introduction:** Suppose we have proved P. Then we can infer *any* disjunction, such as (P v Q v R), that has P as one of its disjuncts.

Proof Methods: 1. Proof by Cases

A Simple Example

Given (A & B) v (A & C), prove A. We have two cases corresponding to the two disjuncts.

- **case 1**: A & B. Clearly A follows by conjunction elimination.

- **case 2**: A & C. Clearly A follows by conjunction elimination.

Therefore A follows in either case.

> To prove S from $P_1 \vee \ldots \vee P_n$
> prove S from each of $P_1, \ldots, P_n$

Proof Methods:
1. Proof By Cases

Show that there are irrational numbers b and c such that b^c is rational.

Assume $\sqrt{2}$ is irrational. Consider the number $\sqrt{2}^{\sqrt{2}}$.

$\sqrt{2}^{\sqrt{2}}$ is either (i) rational or (ii) irrational.

If (i), then b=$\sqrt{2}$, c =$\sqrt{2}$, Q.E.D.

If (ii) , then let b=$\sqrt{2}^{\sqrt{2}}$, c=$\sqrt{2}$

$b^c = (\sqrt{2}^{\sqrt{2}})^{\sqrt{2}} = \sqrt{2}^{\sqrt{2}.\sqrt{2}} = \sqrt{2}^2 = 2$, Q.E.D

So the proposition holds in either case, and this spans all possibilities. So the proposition holds.

To prove S from $P_1 \vee \ldots \vee P_n$ prove S from each of $P_1, \ldots, P_n$

Proof Methods:
2. Proof by Contradiction

Suppose you want to prove -S from some premises, say P and Q, that are known to be consistent.

- Temporarily assume S
- Show that a contradiction follows. This implies that P, Q and S cannot possibly be true simultaneously.
- Infer -S

$\sqrt{2}$ is irrational
Proof by Contradiction

Prove S: $\sqrt{2}$ is irrational

1. Assume -S, i.e. that $\sqrt{2}$ is rational.

2. Draw Inferences:

   Then $\sqrt{2} = \frac{p}{q}$ where at least one of p, q is odd. Squaring,

   $\frac{p^2}{q^2} = 2$ so $p^2 = 2q^2$

   p^2 is even.
   p is even,
   p^2 is divisible by 4.

   Given $p^2 = 2q^2$, q^2 is divisible by 2
   q is even

   contradiction

3. Therefore --S $\equiv$ S

Natural Deduction
Fitch-Style Systems

A proof in the system $\mathcal{F}$ from premises P,Q,R of a conclusion S takes the following form:

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

Notice:

- The vertical line indicates a single proof comprising several steps
- The horizontal line ("Fitch bar"), indicates a division between *assumptions* and things that follow from them.
- The vertical dots would normally be replaced by intermediate conclusions necessary to derive S.

Example of a Fitch-style Proof

1.	A & B & C	
2.	B	& Elim: 1
3.	C	& Elim: 1
4.	C & B & C	& Intro: 3,2,3

Notice:

- Line numbers have been added so we can refer to proof steps explicitly.
- Each line below the Fitch bar has a justification comprising (a) the name of an inference rule and (b) the lines to which it applies.
- The rule used in lines 2 and 3 is "& Elimination" operating on line 1.
- The rule used in line 4 is "& Introduction". Notice the line numbers it is applied to are repeated to yield the silly conclusion.

Inference Rules: Conjunction Elimination Conjunction Introduction

Conjunction Elimination

$$\begin{array}{r|l} & P_1 \& \ldots \& P_i \& \ldots \& P_n \\ & \vdots \\ \triangleright & P_i \end{array}$$

Conjunction Introduction

$$\begin{array}{r|l} & P_1 \\ & \Downarrow \\ & P_n \\ & \vdots \\ \triangleright & P_1 \& \ldots \& P_n \end{array}$$

- The $\Downarrow$ indicates that $P_1 \ldots P_n$ must appear before the conjunction can be asserted and in any order.
- In the justification, the line numbers of the conjuncts should be cited in the order they appear in the conjunction.
- The symbol $\triangleright$ indicates the step which is licenced by the rule.

Disjunction Rules

Disjunction Introduction

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

Disjunction Elimination

$$
\begin{array}{r|l}
 & P_1 \vee \ldots \vee P_n \\
 & \vdots \\
 & \begin{array}{|l} P_1 \\ \hline \vdots \\ \mathsf{S} \end{array} \\
 & \Downarrow \\
 & \begin{array}{|l} P_n \\ \hline \vdots \\ \mathsf{S} \end{array} \\
 & \vdots \\
\rhd & \mathsf{S}
\end{array}
$$

Disjunction Elimination introduces the notion of a *subproof* – a proof within a proof which may begin with assumptions and a Fitch bar.

Proof Using Disjunction Elimination

```
| 1. (A & B) v (C & D)
|—
| | 2. A & B
| |—
| | 3. B         & Elim: 2
| | 4. B v D     v Intro: 3
|
| | 5. C & D
| |—
| | 6. D         & Elim: 5
| | 7. B v D     v Intro: 6
|
| 8. B v D                      v Elim 1,2-4,5-7
```

Checkpoint

Give Fitch-style proofs of the following

1. P v Q from the premise P & Q
2. C v B from the premise (A & B) v C
3. (A & B) v (A & C) from the premises A and B v C.