CSE581
Computer Science Fundamentals: Theory

Professor Anita Wasilewska

P1 LOGIC: LECTURE 4 SHORT VERSION

Chapter 4
GENERAL PROOF SYSTEMS

PART 1: General Intoduction; Soundness and Completeness

PART 2: Formal Definition of a Proof System

PART 3: Formal Proofs and Simple Examples

PART 1: General Introduction

Proof Systems - Intuitive Definition

Proof systems are built to prove, it means to **construct formal proofs** of statements formulated in a given language

First component of any proof system is hence its **formal language** $\mathcal{L}$

Proof systems are inference machines with statements called **provable statements** being their final products

Semantical Link

The **starting points** of the inference machine of a proof system S are called its **axioms**

We distinguish two kinds of axioms: **logical axioms** LA and **specific axioms** SA

Semantical link: we usually build a proof systems for a given language and its **semantics** i.e. for

a logic defined semantically

Semantical Link

We always choose as a set of **logical axioms** LA some **subset of tautologies**, under a given **semantics**

We will **consider here** only proof systems with **finite sets** of **logical** or **specific axioms** , i.e we will examine only **finitely axiomatizable** proof systems

Semantical Link

We can, and we often do, consider proof systems with languages **without yet established semantics**

In this case the **logical axioms LA** serve as description of **tautologies** under a future **semantics** yet to be built

Logical axioms LA of a proof system S are hence not only tautologies under an established **semantics**, but they can also guide us how to define a semantics when it is yet **unknown**

Specific Axioms

The **specific axioms** **SA** consist of statements that describe a specific knowledge of an universe we want to use the proof system S to prove facts about

Specific axioms SA are not universally true

Specific axioms SA are true only in the universe we are interested to **describe** and **investigate** by the use of the proof system S

Formal Theory

Given a **proof system** S with **logical axioms** LA

Specific axioms SA of the proof system S is any finite set of formulas that are not **tautologies**, and hence they are always disjoint with the set of **logical axioms LA** of S

The **proof system** S with added set of **specific axioms SA** is called a **formal theory** based on S

Inference Machine

The **inference machine** of a proof system S is defined by a finite set of **inference rules**

The **inference rules** describe the way we are allowed to **transform** the information within the system with **axioms** as a staring point

We depict it informally on the next slide

Inference Machine

AXIOMS

↓ ↓ ↓

RULES applied to AXIOMS

↓ ↓ ↓

RULES applied to any expressions above

↓ ↓ ↓

Provable formulas

Semantical Link

Semantical link:

Rules of inference of a system S have to preserve the truthfulness of what they are being used to prove

The notion of truthfulness is always defined by a given semantics **M**

Rules of inference that preserve the truthfulness are called **sound rules** under a given semantics **M**

Rules of inference can be sound under one semantics and not sound under another

Soundness Theorem

Goal 1

When developing a proof system S the first goal is prove the following theorem about it and its semantics **M**

Soundness Theorem

For any formula A of the language of the system S

If a formula A is **provable** from **logical axioms** LA of S only,

then A is a **tautology** under the semantics **M**

Propositional Proof Systems

We discuss here first only proof systems for propositional languages and call them **proof systems** for different propositional logics

Remember

The notion of **soundness** is connected with a given **semantics**

A proof system S can be sound under **one semantics,** and not sound under the **other**

For example a set of axioms and rules sound under classical logic semantics might not be sound under Ł logic semantics, or K logic semantics, or others

Completeness of the Proof Systems

In general there are many proof systems that are sound under a given **semantics**, i.e. there are many sound proof systems for a given **logic** semantically defined

Given a proof system S with **logical axioms** LA that is **sound** under a semantics **M**.

Notation

Denote by $\mathbf{T}_{\mathbf{M}}$ the set of all tautologies defined by the semantics **M**, i.e. we have that

$$\mathbf{T}_{\mathbf{M}} = \{A \in \mathcal{F} : \models_{\mathbf{M}} A\}$$

Completeness Property

A **natural question** arises:

Are all tautologies i.e formulas $A \in \mathbf{T_M}$ **provable** in the system S ??

We assume that we have already proved that S is sound under the semantics **M**

The positive answer to this question is called **completeness property** of the system S .

Goal 2

Given for a **sound** proof system S under its semantics **M**, our the second goal is to prove the following theorem about S

Completeness Theorem

For any formula A of the language of S

A **is provable** in S iff A is a **tautology** under the semantics **M**

We write the **Completeness Theorem** symbolically as

$$\vdash_S A \quad \text{iff} \quad \models_{\mathbf{M}} A$$

Completeness Theorem is composed of two parts:

Soundness Theorem and the **Completeness Part** that proves the completeness property of a sound proof system

Proving Soundness and Completeness

Proving the Soundness Theorem for S under a semantics **M** is usually a straightforward and not a very difficult task

We **first prove** that all **logical axioms** LA are **tautologies**,

and then we **prove** that all inference rules of the system S preserve the notion of the truth

Proving the completeness part of the **Completeness Theorem** is always a crucial, difficult and sometimes impossible task

BOOK PLAN

We present two proofs of the **Completeness Theorem** for **classical propositional** proof system in Chapter 5

We also present a constructive proofs of **Completeness Theorem** for two different Gentzen style automated theorem proving systems for **classical Logic** in Chapter 6

We discuss the **Inuitionistic Logic** in Chapter 7

Predicate Logics proof of the **Completeness Theorems** and Automated Theorem proving systems,land Goedel Theorems Chapters 8, 9, 10, 11

PART 2

PROOF SYSTEMS: Formal Definitions

Proof System S

In this section we present **formal definitions** of the following notions

Proof system S

Formal proof from **logical axioms** in a proof system S

Formal proof from **specific axioms** in a proof system S

Formal Theory based on a proof system S

We also give **examples** of different simple proof systems

Components: Language

Language $\mathcal{L}$ of a **proof system** S is any formal language $\mathcal{L}$

$$\mathcal{L} = (\mathcal{A}, \mathcal{F})$$

We assume as before that both sets $\mathcal{A}$ and $\mathcal{F}$ are enumerable, i.e. we deal here with enumerable languages

The **Language** $\mathcal{L}$ can be **propositional** or **first order** (predicate) but we discuss propositional languages first

Components: Expressions

Expressions $\mathcal{E}$ of a proof system S

Given a set $\mathcal{F}$ of well formed formulas of the language $\mathcal{L}$ of the system S

We often extend the set $\mathcal{F}$ to some set $\mathcal{E}$ of **expressions** build out of the language $\mathcal{L}$ and some extra symbols, if needed

In this case all other components of S are also defined on basis of elements of the set of **expressions** $\mathcal{E}$

In particular, and **most common case** we have that $\mathcal{E} = \mathcal{F}$

Expressions Examples

Automated theorem proving systems usually use as their basic components different sets of **expressions** build out of formulas of the language $\mathcal{L}$

In Chapters 6 and 10 we consider finite sequences of formulas instead of formulas, as basic expressions of the proof systems **RS** and **RQ**

We also present there proof systems that use yet other kind of expressions, called original **Gentzen sequents** or their modifications

Some systems use yet other expressions such as clauses, sets of clauses, or sets of formulas, others use yet still different expressions

Semantical Link

We always have to **extend** a given semantics **M** for the language $\mathcal{L}$ of the system S to the set $\mathcal{E}$ of all **expression** of the system S

Sometimes, like in case of **Resolution** based proof systems we have also to **prove** a semantic equivalency of new created expressions $\mathcal{E}$ (sets of clauses in Resolution case) with appropriate formulas of $\mathcal{L}$

Components: Logical Axioms

Logical axioms LA of S form a **non-empty** subset of the set $\mathcal{E}$ of **expressions** of the proof system S, i.e.

$$LA \subseteq \mathcal{E}$$

In particular, LA is a non-empty subset of **formulas**, i.e.

$$LA \subseteq \mathcal{F}$$

We **assume here** that the set LA of **logical axioms** is always **finite** , i.e. that we consider here finitely axiomatizable systems

Components: Axioms

Semantical link

Given a semantics **M** for $\mathcal{L}$ and its **extension** to the set $\mathcal{E}$ of all expressions

We extend the notion of **tautology** to the expressions and write

$$\models_{\mathbf{M}} E$$

to denote that the **expression** $E \in \mathcal{E}$ is a **tautology** under semantics **M** and we put

$$\mathbf{T}_{\mathbf{M}} = \{E \in \mathcal{E} : \ \models_{\mathbf{M}} E\}$$

Logical axioms LA are always a subset of expressions that are **tautologies** of under the semantics **M**, i.e.

$$LA \subseteq \mathbf{T}_{\mathbf{M}}$$

Components: Rules of Inference

Rules of inference $\mathcal{R}$

We **assume** that a proof system contains only a finite number of **inference rules**

We **assume** that each rule has a finite number of **premisses** and one **conclusion**

Components: Rules of Inference

We write the **inference rules** in a following convenient way

One premiss rule

$$(r) \quad \frac{P_1}{C}$$

Two premisses rule

$$(r) \quad \frac{P_1 \;;\; P_2}{C}$$

m premisses rule

$$(r) \quad \frac{P_1 \;;\; P_2 \;;\; .... \;;\; P_m}{C}$$

Semantic Link: Sound Rules of Inference

Given some **m** premisses rule

$$(r) \qquad \frac{P_1 \;\; ; \;\; P_2 \;\; ; \;\; .... \;\; ; \;\; P_m}{C}$$

Semantical link

Given a semantics **M** for the language $\mathcal{L}$ and for the set of expressions $\mathcal{E}$

We want the **rules of inference** $r \in \mathcal{R}$ to preserve truthfulness i.e. to be **sound** under the semantics **M**

Propositional Definition: Sound Rule of Inference

Definition (Shorthand Notation)

An inference rule $r \in \mathcal{R}$, such that

$$(r) \quad \frac{P_1 \;\; ; \;\; P_2 \;\; ; \;\; .... \;\; ; \;\; P_m}{C}$$

is sound under a semantics **M** f and only if

ifrom that **assumption** that $P_1 = T, \; P_2 = T, .P_m = T$,

we prove $C = T$

Example

Given a rule of inference

$$(r) \quad \frac{(A \Rightarrow B)}{(B \Rightarrow (A \Rightarrow B))}$$

Prove that (r) is **sound** underclassical semantics

Assume that $A \Rightarrow B) = T$

We **evaluate** logical value of the **conclusion** as follows

$$(B \Rightarrow (A \Rightarrow B)) = B) \Rightarrow T = T$$

This proves the **soundness** of (r)

Formal Definition: Proof System

Definition

By a **proof system** we understand a quadruple

$$S = (\mathcal{L}, \mathcal{E}, LA, \mathcal{R})$$

where

$\mathcal{L} = \{\mathcal{A}, \mathcal{F}\}$ is a **language** of S with a set $\mathcal{F}$ of formulas

$\mathcal{E}$ is a set of **expressions** of S formed out of the set $\mathcal{F}$ of formulas of $\mathcal{L}$

In particular case $\mathcal{E} = \mathcal{F}$

$LA \subseteq \mathcal{E}$ is a **non- empty, finite set** of logical axioms of S

$\mathcal{R}$ is a **non- empty, finite set** of rules of inference of S

PART 3: Formal Proofs
Simple Examples of Proof Systems

Provable Expressions

A **final product** of a single or multiple use of the **inference rules** of S, with axioms taken as a **starting point** are called **provable expressions** of the proof system S

A single use of an inference rule is called a **direct consequence**

A multiple application of rules of inference with axioms taken as a starting point is called a **proof**

Definition: Direct Consequence

Formal definitions are as follows

Direct consequence

For any rule of inference $r \in \mathcal{R}$ of the form

$$(r) \quad \frac{P_1 \; ; \; P_2 \; ; \; .... \; ; \; P_m}{C}$$

C is called a **direct consequence** of $P_1, ...P_m$ by virtue of the rule $r \in \mathcal{R}$

Definition: Formal Proof

Formal Proof of an expression $E \in \mathcal{E}$ in a proof system

$$S = (\mathcal{L}, \mathcal{E}, LA, \mathcal{R})$$

is a sequence

$$A_1, A_2, , A_n \quad \text{for} \quad n \geq 1$$

of expressions from $\mathcal{E}$, such that

$$A_1 \in LA, \qquad A_n = E$$

and for each $1 < i \leq n$, either $A_i \in LA$ or A_i is a **direct consequence** of some of the **preceding expressions** by virtue of one of the rules of inference

$n \geq 1$ is the **length of the proof** $A_1, A_2, , A_n$

Formal Proof Notation

We write

$$\vdash_S E$$

to denote that $E \in \mathcal{E}$ **has a proof** in S

When the proof system S is **fixed** we write $\vdash E$

Any $E \in \mathcal{E}$, such that $\vdash_S E$ is called a **provable expression** of S

The set of **all provable expressions** of S is denoted by $\mathbf{P}_S$, i.e. we put

$$\mathbf{P}_S = \{E \in \mathcal{E} : \ \vdash_S E\}$$

Given a proof system:

$$S = (\mathcal{L}_{\{\neg,\Rightarrow\}}, \mathcal{F}, \{(A \Rightarrow A), (A \Rightarrow (\neg A \Rightarrow B))\}, (r) \ \frac{(A \Rightarrow B)}{(B \Rightarrow (A \Rightarrow B))})$$

Problem 3.

Write a **formal proof** of your choice in S with 2 applications of the rule (r)

Solution

There many of such proofs, of different length, with different choice if axioms - here is my choice: A_1, A_2, A_3, where

$A_1 = (A \Rightarrow A)$

(Axiom)

$A_2 = (A \Rightarrow (A \Rightarrow A))$

Rule (r) application 1 for $A = A,\ B = A$

$A_3 = ((A \Rightarrow A) \Rightarrow (A \Rightarrow (A \Rightarrow A)))$

Rule (r) application 2 for $A = A, B = (A \Rightarrow A)$

Formal Proof

Given a proof system:

$$S = (\mathcal{L}_{\{\neg,\Rightarrow\}}, \mathcal{F}, \{(A \Rightarrow A), (A \Rightarrow (\neg A \Rightarrow B))\}, (r)\ \frac{(A \Rightarrow B)}{(B \Rightarrow (A \Rightarrow B))})$$

Problem 4

1. Prove, by constructing a **formal proof** that

$$\vdash_S ((\neg A \Rightarrow B) \Rightarrow (A \Rightarrow (\neg A \Rightarrow B)))$$

Solution Required formal proof is a sequence A_1, A_2, where

$A_1 = (A \Rightarrow (\neg A \Rightarrow B))$

Axiom

$A_2 = ((\neg A \Rightarrow B) \Rightarrow (A \Rightarrow (\neg A \Rightarrow B)))$

Rule (r) application for $A = A, B = (\neg A \Rightarrow B)$

Definition: Sound S

Definition

Given a proof system

$$S = (\mathcal{L}, \mathcal{E}, LA, \mathcal{R})$$

We say that the system S is **sound** under a semantics **M** iff the following conditions hold

1. $LA \subseteq \mathbf{T_M}$
2. Each rule of inference $r \in \mathcal{R}$ is **sound**

Example

Given a proof system:

$$S = (\mathcal{L}_{\{\neg, \Rightarrow\}}, \ \mathcal{F}, \ \ \{(A \Rightarrow A), (A \Rightarrow (\neg A \Rightarrow B))\}, \ \ (r) \ \frac{(A \Rightarrow B)}{(B \Rightarrow (A \Rightarrow B))})$$

1. Prove that S is **sound** under **classical semantics**
2. Prove that S is **not sound** under **K** semantics

Example

1. Both **axioms** of S are basic classical **tautologies** and we have just proved that the rule of inference (r) is **sound**, hence S is **sound**

2. Axiom $(A \Rightarrow A)$ is not a **K** semantics tautology

Any truth assignment v such that $v^*(A) = \perp$ is a **counter-model** for it

This proves that S is **not sound** under **K** semantics

Soundness Theorem

Let $\mathbf{P}_S$ be the set of all provable expressions of S i.e.

$$\mathbf{P}_S = \{A \in \mathcal{E} : \ \vdash_S A\}$$

Let $\mathbf{T_M}$ be a set of all expressions of S that are tautologies under a semantics **M**, i.e.

$$\mathbf{T_M} = \{A \in \mathcal{E} : \ \models_{\mathbf{M}} A\}$$

Soundness Theorem for S and semantics **M**

$$\mathbf{P}_S \subseteq \mathbf{T_M}$$

i.e. for any $A \in \mathcal{E}$, the following implication holds

If $\vdash_S A$, then $\models_{\mathbf{M}} A$.

Exercise: prove by Mathematical Induction over the length of a proof that if S is sound, the Soundness Theorem holds for S

Completeness Theorem

Completeness Theorem for S and semantics **M**

$$\mathbf{P}_S = \mathbf{T}_{\mathbf{M}}$$

i.e. for any $A \in \mathcal{E}$, the following holds

$$\vdash_S A \quad \text{if and only if} \quad \models_{\mathbf{M}} A$$

The **Completeness Theorem** consists of two parts:

Part 1: **Soundness Theorem**

$$\mathbf{P}_S \subseteq \mathbf{T}_{\mathbf{M}}$$

Part 2: **Completeness Part** of the Completeness Theorem

$$\mathbf{T}_{\mathbf{M}} \subseteq \mathbf{P}_S$$