Discrete Mathematics

Yi Li

Software School
Fudan University

April 18, 2012

Review

- Atomic tableaux
- CST and properties

Outline

- Syntax and semantics
- Soundness theorem
- Completeness theorem

Syntax & Semantics

Example

Give you two Chinese characters "更衣", what's it mean?

- It means **change clothes** in modern Chinese.
- It means **go to washroom** in ancient Chinese.

Example

Give an acronym "IP", what's it mean?

- **Internet Protocol** in network.
- **Integer Programming** in operation research.
- **Interactive proof** in complexity.

Syntax & Semantics

Example

Give you the following programming segments:

1. in C, printf("Hello World!");
2. in Java, system.print("Hello World!");
3. in C++, cout<<"Hello World!";

All of them just output "Hello World!" on the screen.

Syntax & Semantics in PL

- What's syntax?
- What's semantic?
- What's relationship between them?

Soundness

Example

Consider Pierce Law

$$((A \to B) \to A) \to A.$$

- Give its tableau proof.
- Give its truth table.

Sign & Noncontradictory Path

Example

Given proposition $((A \to B) \to (A \to C)) \to (B \to C)$, there is a truth valuation which make it false.

Consider the tableau with the root as

$$F\ ((A \to B) \to (A \to C)) \to (B \to C)$$

Soundness

Lemma

If V is a valuation that agrees with the root entry of a given tableau τ given as $\cup \tau_n$, then τ has a path P every entry of which agrees with V.

Soundness(Cont.)

Theorem (Soundness)

If α is tableau provable, then α is valid, i.e. $\vdash \alpha \Rightarrow \models \alpha$.

Completeness

Example

Given proposition $((A \to B) \to (A \to C)) \to (B \to C)$, there is a truth valuation which make it false. Observe the non-contradictory path of the tableau with the root as $F\ ((A \to B) \to (A \to C)) \to (B \to C)$

Completeness

Lemma

Let P be a noncontradictory path of a finished tableau τ. Define a truth assignment $\mathcal{A}$ on all propositional letters A as follows:

1. $\mathcal{A}(A) = T$ *if* TA *is an entry on* P.
2. $\mathcal{A}(A) = F$ *otherwise.*

If $\mathcal{V}$ is the unique valuation extending the truth assignment $\mathcal{A}$, then $\mathcal{V}$ agrees with all entries of P.

Completeness(Cont.)

Theorem (Completeness)

If α *is valid, then* α *is tableau provable, i.e.* $\models \alpha \Rightarrow \vdash \alpha$*.*
In fact, any finished tableau with root entry $F\alpha$ *is a proof of* α *and so, in particular, the complete systematic tableaux with root* $F\alpha$ *is such a proof.*

Hilbert Proof System

Definition

The axioms of Hilbert system are all propositions of the following forms:

1. $(\alpha \to (\beta \to \alpha))$
2. $((\alpha \to (\beta \to \gamma)) \to ((\alpha \to \beta) \to (\alpha \to \gamma)))$
3. $(\neg\beta \to \neg\alpha) \to ((\neg\beta \to \alpha) \to \beta)$

The Rule of Inference

Definition (Modus Ponens)

From α and $\alpha \to \beta$, we can infer β. This rule is written as follows:

$$\begin{array}{r} \alpha \\ \alpha \to \beta \\ \hline \beta \end{array}$$

Hilbert Proof System

Definition

Let Σ be a set of propositions.

1. A *proof from* Σ is a finite sequence $\alpha_1, \alpha_2, \ldots, \alpha_n$ such that for each $i \leq n$ either:
   1. α_i is a member of Σ.
   2. α_i is an axiom;

      or
   3. α_i can be inferred from some of previous α_j by an application of a rule of inference.
2. α is *provable from* Σ, $\Sigma \vdash_H \alpha$, if there is a proof $\alpha_1, \alpha_2, \ldots, \alpha_n$ from Σ where $\alpha_n = \alpha$.
3. A *proof* of α is simply a proof from the empty set 0; α is *provable* if it is provable from 0.

Next Class

- Deduction from premises
- Compactness