Review: First Order Logic

- A language for mathematical assertions
- Includes logical-symbols $\forall, \exists, =, \wedge, \vee, \neg$
  - The meaning of these symbols is fixed
- Includes non-logical symbols (like $\oplus$)
  - The meaning of these symbols is not fixed. (We can even vary the set V of these symbols as needed.)
- A structure M fixes the meaning of the non-logical symbols (and the universe of elements).
  - Also called an interpretation

Review: First Order Logic

- $M \vDash \phi$ is same as
  - M is a model for ϕ
  - i.e., "ϕ holds true in the given structure M"
- Let Ψ be a set of assertions $\{\psi_1, \cdots\}$
- $M \vDash \Psi$ is same as
  - M is a model for Ψ
  - i.e., "every $\psi_i \in \Psi$ holds true in the given structure M
- $\Psi \vDash \phi$ is short for
  - Any structure M that is a model for Ψ is also a model for ϕ

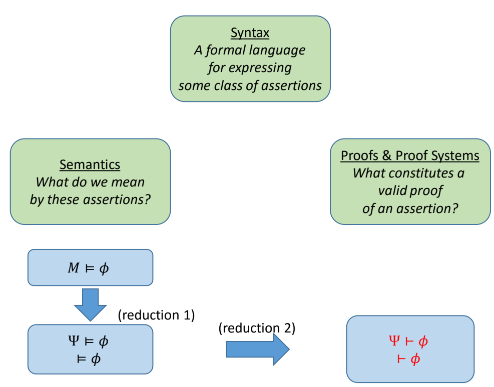
Review: First Order Logic

- Suppose $M \vDash \Psi$
- Problem reduction:

(soundness holds)
$\Leftarrow$

Does $M \vDash \phi$? → Does $\Psi \vDash \phi$?

$\Rightarrow ?$
(completeness may not hold)



Proofs & Proof Systems

- A proof system (or deduction system) is used to define what a valid proof is
- A proof is a tree-like structure
  - Leafs: axioms (or axiom instances)
  - Internal nodes: compose sub-proofs using inference rules
  - Root: the theorem that is proven
  - (convenient to draw upside-down)

Proofs & Proof Systems

- A proof-system S is an inductive definition of judgements of the form $\vdash_S \phi$ or $\Psi \vdash_S \phi$
- We use the judgement $\vdash_S \phi$ to denote that ϕ can be proven to be valid (in system S)
- The judgement $\Psi \vdash \phi$ denotes that ϕ can be proven given proofs of all $\psi \in \Psi$ (in system S).

Example

$$\frac{}{\Psi, \phi \vdash \phi}$$

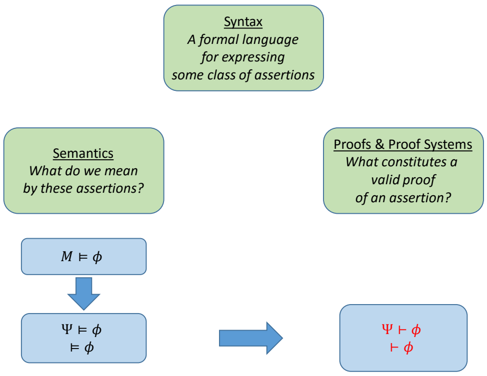
$$\frac{\Psi \vdash \phi_1, \qquad \Psi \vdash \phi_1 \Rightarrow \phi_2}{\Psi \vdash \phi_2} \text{ (modus ponens)}$$

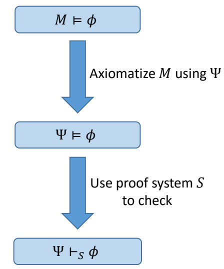
$$\frac{\Psi, \phi_1 \vdash \phi_2}{\Psi \vdash \phi_1 \Rightarrow \phi_2}$$

$$\frac{\Psi \vdash \phi_1, \qquad \Psi \vdash \phi_2}{\Psi \vdash \phi_1 \wedge \phi_2}$$

Soundness & Completeness

- A proof system is said to be sound if all provable formulae are valid: that is,
  - $\Psi \vdash \phi$ implies $\Psi \vDash \phi$
- A proof system is said to be complete if all valid formulae are provable: that is,
  - $\Psi \vDash \phi$ implies $\Psi \vdash \phi$





Godel's Completeness & Incompleteness Theorems

Summary

- By design [of formal proof systems]
  - Correctness of a given proof can be easily machine-checked
    - But can be tedious for us to write
  - The set of proofs (for a chosen set of axioms) is recursively enumerable
    - Can automate search for proofs
    - Challenges
      - Efficiency
      - Choosing a set of axioms

Satisfiability Modulo Theories (SMT Solvers)

- *Extend SAT solvers to check satisfiability modulo one or more theories*

```
method Eg2 (x, y : int)
  returns (z : int)
{
   assume x < y;
   z := (x+y)/2;
   assert x < z;
}
```

Valid iff for all x, y, z:

$$\left((x < y) \land \left(z = \frac{x+y}{2}\right) \Rightarrow (x < z)\right)$$

(x, y, z) is a counterexample iff

$$(x < y) \land (z = \frac{x+y}{2})) \land (x \geq z)$$