

Computer Supported Modeling and Reasoning (WS01/02)

David Basin

Institut für Informatik
Albert-Ludwigs-Universität Freiburg

24.10.01

Overview

- Short review: ND Systems and proofs
- Syntax
- Semantics
- Deduction, some derived rules, and examples

ND: Review

- ND proofs build derivations under (possibly temporary) assumptions

$$\frac{A \quad B}{A \wedge B} \wedge-I \quad \frac{A \wedge B}{A} \wedge-EL \quad \frac{A \wedge B}{B} \wedge-ER$$

$$\frac{\begin{array}{c} [A] \\ \vdots \\ B \end{array}}{A \rightarrow B} \rightarrow-I \quad \frac{A \rightarrow B \quad A}{B} \rightarrow-E$$

- Proof:

$$\frac{\frac{[A \wedge B]}{B} \wedge-EL \quad \frac{[A \wedge B]}{A} \wedge-ER}{B \wedge A} \wedge-I$$

$$\frac{B \wedge A}{A \wedge B \rightarrow B \wedge A} \rightarrow-I$$

Alternative formalization using sequents

- Rules (for \rightarrow / \wedge fragment). Here, H is a set of formulae.

$H \vdash A$ *assumption* (where $A \in H$)

$$\frac{H \vdash A \quad H \vdash B}{H \vdash A \wedge B} \wedge-I \quad \frac{H \vdash A \wedge B}{H \vdash A} \wedge-EL \quad \frac{H \vdash A \wedge B}{H \vdash B} \wedge-ER$$

$$\frac{A, H \vdash B}{H \vdash A \rightarrow B} \rightarrow-I \quad \frac{H \vdash A \rightarrow B \quad H \vdash A}{H \vdash B} \rightarrow-E$$

- Proof:

$$\frac{\frac{A \wedge B \vdash A \wedge B}{A \wedge B \vdash B} \wedge-ER \quad \frac{A \wedge B \vdash A \wedge B}{A \wedge B \vdash A} \wedge-EL}{A \wedge B \vdash B \wedge A} \wedge-I$$

$$\frac{A \wedge B \vdash B \wedge A}{\vdash A \wedge B \rightarrow B \wedge A} \rightarrow-I$$

- Two representations equivalent. Sequent notation seems simpler in practice.

Example: refinement style with metavariables

$$\frac{
 \frac{
 \frac{
 A \wedge (B \wedge C) \vdash A \wedge ?X
 }{
 A \wedge (B \wedge C) \vdash A
 }
 }{
 \frac{
 \frac{
 A \wedge (B \wedge C) \vdash ?Z \wedge (?Y \wedge C)
 }{
 A \wedge (B \wedge C) \vdash (?Y \wedge C)
 }
 }{
 A \wedge (B \wedge C) \vdash C
 }
 }{
 A \wedge (B \wedge C) \vdash A \wedge C
 }
 }{
 \vdash A \wedge (B \wedge C) \rightarrow A \wedge C
 }$$

- Solution for $?Z = A$, $?Y = B$ and $?X = (B \wedge C)$
- This crazy way of carrying out proofs is the (standard) Isabelle-way!
 - Refinement style means we work from goals to axioms
 - Metavariables used to delay commitments

Isabelle allows other refinements/alternatives too (see labs).

Towards stronger logics

- Propositional logic
 - Formulae are Boolean combinations of propositions
 - Relations/Functions are modeled in limited ways, e.g., over finite domains
- Example: modeling time dependency
 - Model 10 time units with Boolean variables x_1, \dots, x_{10} .
 - E.g., $x_1 \wedge \neg x_2 \wedge x_3 \wedge \neg x_4 \wedge x_5 \dots$ expresses “alternating state”
- Non-examples:
 - State alternates over all time: $\forall t. x(t) \leftrightarrow \neg x(t + 1)$
 - y always occurs after x : $\forall t. x(t) \rightarrow \exists t'. t' > t \wedge y(t')$
- Let us now extend propositional logic to first-order logic.

Predicates: intuition

- Predicates express properties over some domain

$$p(x) \equiv x \text{ is a prime number} \qquad d(x, y) \equiv x \text{ is divisible by } y$$

- Propositional connectives give rise to a simple modeling language.

- x is a prime and either y or z is divisible by x

$$p(x) \wedge (d(y, x) \vee d(z, x))$$

- x is a man and y is a woman and x likes y but not vice versa

$$m(x) \wedge w(y) \wedge l(x, y) \wedge \neg l(y, x)$$

- We can represent only “abstractions” of these in propositional logic, e.g.,

$$p \wedge (d_1 \vee d_2)$$

Here predicates are abstracted to propositions. (Is this a “valid” abstraction?)

Functions: intuition

- A function, of arity n , expresses an n -ary operation over some domain

$$\forall x, y. 0 + x = x \wedge s(x) + y = s(x + y)$$

Above involves function symbols: 0 (nullary), s (unary) and $+$ (infix binary).

- Functions are generally formalized (axiomatized) and reasoned about equationally
 - Calls for first-order logic with equality (next lecture)
 - Semantically such axioms define a class of algebraic structures
- Satisfying structures for above example
 - Natural numbers under standard interpretation (s is successor)
 - Strings over the alphabet $\{0, 1\}$. 0 is the empty string, $s(x)$ concatenates 0 to x , and $+$ is append.

Quantifiers: intuition

- Used to speak about all (or some) members of some domain.
- Examples: Are they satisfiable? valid?

$\forall x. \exists y. y * 2 = x$ true for rationals

$x < y \rightarrow \exists z. x < z \wedge z < y$ true for any dense order

$\exists x. x \neq 0$ true for domains with more than one element

$(\forall x. p(x, x)) \rightarrow p(a, a)$ valid

Syntax

- Two syntactic categories: **terms** and **formulae**
- Let a finite collection of function symbols \mathcal{F} and predicates \mathcal{P} be given as well as a set \mathcal{V} of variables.

Write f^i [or p^i] to indicate function symbol f [predicate p] has arity $i \in \mathcal{N}$.

- *Term*, the set of **terms in first-order logic**, is the smallest set where
 1. $x \in \text{Term}$ if $x \in \mathcal{V}$, and
 2. $f^n(t_1, \dots, t_n) \in \text{Term}$ if $f^n \in \mathcal{F}$ and $t_j \in \text{Term}$, for all $1 \leq j \leq n$.
- *Form*, the set of **formulae in first-order logic**, is the smallest set where
 1. $\perp \in \text{Form}$,
 2. $p^n(t_1, \dots, t_n) \in \text{Form}$ if $p^n \in \mathcal{P}$ and $t_j \in \text{Term}$, for all $1 \leq j \leq n$,
 3. $\neg \phi \in \text{Form}$ if $\phi \in \text{Form}$,
 4. $\phi \circ \psi \in \text{Form}$ if $\phi \in \text{Form}$, $\psi \in \text{Form}$ and $\circ \in \{\wedge, \vee, \rightarrow\}$,
 5. $\forall x. \phi \in \text{Form}$ and $\exists x. \phi \in \text{Form}$ if $\phi \in \text{Form}$ and $x \in \mathcal{V}$.

Syntax (cont.)

- All occurrences of a variable in a formula are **bound** or **free**

A variable x in a formula ϕ is **bound** if x occurs within a subformula of ϕ of the form $\exists x.\psi$ or $\forall x.\psi$.

- Example: $(q(x) \vee \exists x. \forall y. p(f(x), z) \wedge q(a)) \vee \forall x. r(x, z, g(x))$

Semantics

- A **structure** is a pair $\mathcal{A} = \langle U_{\mathcal{A}}, I_{\mathcal{A}} \rangle$ where $U_{\mathcal{A}}$ is a nonempty set, the **universe**, and $I_{\mathcal{A}}$ is a mapping where
 1. $I_{\mathcal{A}}(p^n)$ is an n -ary relation on $U_{\mathcal{A}}$, for $p^n \in \mathcal{P}$,
 2. $I_{\mathcal{A}}(f^n)$ is an n -ary (total) function on $U_{\mathcal{A}}$, for $f^n \in \mathcal{F}$, and
 3. $I_{\mathcal{A}}(x)$ is an element of $U_{\mathcal{A}}$, for each $x \in \mathcal{V}$.

As shorthand, write $p^{\mathcal{A}}$ for $I_{\mathcal{A}}(p)$, etc.

- For \mathcal{A} a structure, define the **value of a term t under \mathcal{A}** , written $\mathcal{A}(t)$ by
 1. $\mathcal{A}(x) = x^{\mathcal{A}}$, for $x \in \mathcal{V}$, and
 2. $\mathcal{A}(f(t_1, \dots, t_n)) = f^{\mathcal{A}}(\mathcal{A}(t_1), \dots, \mathcal{A}(t_n))$.

Semantics (cont.)

- We define the (truth-)value of the formula F , written $\mathcal{A}(F)$ under \mathcal{A} as:

$$\begin{aligned}
 \mathcal{A}(\perp) &= 0 \\
 \mathcal{A}(p(t_1, \dots, t_n)) &= \begin{cases} 1 & \text{if } (\mathcal{A}(t_1), \dots, \mathcal{A}(t_n)) \in p^{\mathcal{A}} \\ 0 & \text{otherwise} \end{cases} \\
 \mathcal{A}(\neg \phi) &= \begin{cases} 1 & \text{if } \mathcal{A}(\phi) = 0 \\ 0 & \text{otherwise} \end{cases} \\
 &\vdots \\
 \mathcal{A}(\forall x. \phi) &= \begin{cases} 1 & \text{if for all } u \in U_{\mathcal{A}}, \mathcal{A}_{[x/u]}(\phi) = 1 \\ 0 & \text{otherwise} \end{cases} \\
 \mathcal{A}(\exists x. \phi) &= \begin{cases} 1 & \text{if for some } u \in U_{\mathcal{A}}, \mathcal{A}_{[x/u]}(\phi) = 1 \\ 0 & \text{otherwise} \end{cases}
 \end{aligned}$$

Here $\mathcal{A}_{[x/u]}$ is the structure \mathcal{A}' identical to \mathcal{A} , except that $x^{\mathcal{A}'} = u$.

- When $\mathcal{A}(\phi) = 1$, we write $\mathcal{A} \models \phi$ and say ϕ is true in \mathcal{A} or \mathcal{A} is a model of ϕ . When every suitable structure is a model, we write $\models \phi$ and say ϕ is valid. If there is at least one model for ϕ , ϕ is satisfiable (and contradictory otherwise).

An example

$$\forall x.p(x, s(x))$$

- A model:

$$U_{\mathcal{A}} = \mathcal{N}$$

$$p^{\mathcal{A}} = \{(m, n) \mid m, n \in U_{\mathcal{A}} \text{ and } m < n\}$$

$$s^{\mathcal{A}} = \text{the successor function on } U_{\mathcal{A}}$$

$$= \text{i.e., } s^{\mathcal{A}}(x) = x + 1$$

- A nonmodel:

$$U_{\mathcal{A}} = \{a, b, c\}$$

$$p^{\mathcal{A}} = \{(a, b), (a, c)\}$$

$$s^{\mathcal{A}} = \text{the identify function}$$

Informal reasoning about quantifiers

- Consider an “ordinary” mathematical proof of

$$\text{if } x > 2 \text{ then } x^2 > 4$$

N.B.: quantifiers (here $\forall x$) often implicit in natural language statements.

- Proof: Consider an arbitrary x (\forall -I) where $x > 2$ (\rightarrow -I).

Then $x = 2 + y$ for some $y > 0$ and hence

$$x^2 = (2 + y)^2 = 4 + 4y + y^2 \geq 4 + 4 + 1 \geq 9 > 4$$

Note: Proof holds for natural numbers. How would you adapt for reals?

- Even easier to prove the weaker statement $\exists x. x > 2 \rightarrow x^2 > 4$

Let $x = 0$ (indeed any number!). Statement follows as $0 > 2 \rightarrow 0^2 > 4$.

- We now give rules for formal derivations in FOL.

Universal quantification

- Rules

$$\frac{P(x)}{\forall x. P(x)} \forall\text{-I}^* \qquad \frac{\forall x. P(x)}{P(t)} \forall\text{-E}$$

- Are these rules reasonable? Consider the following “proof”

$$\frac{\frac{\frac{[x = 0]^1}{\forall x. x = 0} \forall\text{-I}}{x = 0 \rightarrow \forall x. x = 0} \rightarrow\text{-I}^1}{\forall x. (x = 0 \rightarrow \forall x. x = 0)} \forall\text{-I}}{\frac{0 = 0 \rightarrow \forall x. x = 0}{\forall x. x = 0} \forall\text{-E} \qquad 0 = 0} \rightarrow\text{-E}$$

- Side condition (*): x is really arbitrary!

More formally: x not free in any assumption on which $P(x)$ depends.

Universal quantification (cont.)

- Is the following a proof?

$$\frac{\frac{[\forall x. \neg \forall y. x = y]^1}{\neg \forall y. y = y} \forall\text{-E}}{\forall x. \neg \forall y. x = y \rightarrow \neg \forall y. y = y} \rightarrow\text{-I}^1$$

- Conclusion is not valid. Reason: false when $U_{\mathcal{A}}$ has at least 2 elements.
- Proof is incorrect. Reason: substitution must be capture avoiding.
i.e., y must be free for x in $\neg \forall y. y = y$, which is not the case.
- This detail concerns substitution (and renaming of bound variables), not \forall -E.

Universal quantification (cont.)

- Proof?

$$\begin{array}{c}
 \frac{[\forall x. A(x) \wedge B(x)]^1}{A(x) \wedge B(x)} \forall\text{-}E \quad \frac{[\forall x. A(x) \wedge B(x)]^1}{A(x) \wedge B(x)} \forall\text{-}E \\
 \frac{A(x) \wedge B(x)}{A(x)} \wedge\text{-}EL \quad \frac{A(x) \wedge B(x)}{B(x)} \wedge\text{-}ER \\
 \frac{A(x)}{\forall x. A(x)} \forall\text{-}I \quad \frac{B(x)}{\forall x. B(x)} \forall\text{-}I \\
 \frac{\forall x. A(x) \quad \forall x. B(x)}{\forall x. A(x) \wedge \forall x. B(x)} \wedge\text{-}I \\
 \frac{\forall x. A(x) \wedge \forall x. B(x)}{\forall x. A(x) \wedge B(x) \rightarrow \forall x. A(x) \wedge \forall x. B(x)} \rightarrow\text{-}I^1
 \end{array}$$

- Yes. (check side conditions of $\forall\text{-}I$)

Universal quantification (cont.)

- Define $A \leftrightarrow B$ as $A \rightarrow B \wedge B \rightarrow A$. Following is derivable

$$\frac{\begin{array}{c} [A] \\ \vdots \\ B \end{array} \quad \begin{array}{c} [B] \\ \vdots \\ A \end{array}}{A \leftrightarrow B}$$

- Proof?

$$\frac{\frac{A}{\forall x. A} \forall-I \quad \frac{\forall x. A}{A} \forall-E}{A \leftrightarrow \forall x. A}$$

- Yes, but only if x not free in A .

Similar requirement arises in proving $(\forall x. A \rightarrow B(x)) \rightarrow (A \rightarrow \forall x. B(x))$.

Existential quantification

- Define $\exists x. A$ as $\neg \forall x. \neg A$.
- Equivalence follows semantically from Tarskian definition

$$\mathcal{A}(\neg A) = \begin{cases} 1 & \text{if } \mathcal{A}(A) = 0 \\ 0 & \text{otherwise} \end{cases}$$

$$\mathcal{A}(\forall x. A) = \begin{cases} 1 & \text{if for all } u \in U_{\mathcal{A}}, \mathcal{A}_{[x/u]}(A) = 1 \\ 0 & \text{otherwise} \end{cases}$$

$$\mathcal{A}(\exists x. A) = \begin{cases} 1 & \text{if for some } u \in U_{\mathcal{A}}, \mathcal{A}_{[x/u]}(A) = 1 \\ 0 & \text{otherwise} \end{cases}$$

Conclude: $\mathcal{A}(\exists x. A) = \mathcal{A}(\neg \forall x. \neg A)$

- We can use definition to **derive** ND proof rules

Alternative: give rules as part of the deduction system and prove equivalence as a lemma, instead of by definition.

Existential quantification (cont.)

- \exists -I as a derived rule

$$\frac{\frac{\frac{[\forall x. \neg A(x)]}{\neg A(t)} \forall\text{-}E \quad A(t)}{\perp} \rightarrow\text{-}E}{\neg \forall x. \neg A(x)} \rightarrow\text{-}I \quad \text{demonstrates} \quad \frac{A(t)}{\exists x. A(x)} \exists\text{-}I$$

- As with \forall -E: t must be free for x in A .

Existential quantification (cont.)

- \exists -E as a derived rule

$$\begin{array}{c}
 \frac{\frac{\frac{[\neg B]^2 \quad B}{\perp} \rightarrow -I^1 \quad \frac{[A(x)]^1 \quad \vdots \quad B}{\neg A(x)} \forall -I}{\neg \forall x. \neg A(x)} \rightarrow -E}{\perp} \text{RAA}^2 \\
 \frac{\perp}{B}
 \end{array}
 \quad \text{demonstrates} \quad
 \frac{\frac{\frac{[A(x)] \quad \vdots \quad B}{\exists x. A(x)} \exists -E}{B} \exists -E$$

- Note use of hypothetical derivation: B from assumptions $A(x)$ and (implicit) H .

$$\text{i.e. if } H, A(x) \vdash B \text{ then } H, \exists x. A(x) \vdash B$$

- Side condition for \exists -E: side conditions from \forall -I in derivation!

x not free in B or in hypotheses of the subderivation of B other than $A(x)$.

Sample Derivation

Assumption: x does not occur free in B

$$\begin{array}{c}
 \frac{[\forall x. A(x) \rightarrow B]^3}{A(x) \rightarrow B} \forall\text{-}E \quad \frac{[A(x)]^1}{B} \rightarrow\text{-}E \\
 \frac{[\exists x. A(x)]^2}{B} \exists\text{-}E^1 \\
 \frac{B}{\exists x. A(x) \rightarrow B} \rightarrow\text{-}I^2 \\
 \frac{\exists x. A(x) \rightarrow B}{(\forall x. A(x) \rightarrow B) \rightarrow (\exists x. A(x) \rightarrow B)} \rightarrow\text{-}I^3
 \end{array}$$

Summary

- Propositional logic is good for reasoning about simple patterns

Language of Boolean connectives for patterns like “if . . . then . . . else”

- Mathematical statements often involve generality or scope

All men are mortal, Socrates is a man, therefore Socrates is mortal

- There are still controversies about what the best logic is for such reasoning, e.g., arguments for intuitionistic, relevant, and other “deviant” logics.

From “a dollar buys a candy bar” and “a dollar buys an ice cream” we cannot normally conclude “a dollar buys a candy bar and ice cream”.

- However for ordinary mathematical reasoning first-order logic is often enough

Knowledge about or restrictions on the world are expressed in first-order theories, which we will see next.