Computer Supported Modeling and Reasoning

David Basin, Achim D. Brucker, Jan-Georg Smaus, and Burkhart Wolff

April 2005

http://www.infsec.ethz.ch/education/permanent/csmr/

First-Order Logic

David Basin, Burkhart Wolff, and Jan-Georg Smaus

First-Order Logic: Overview

In propositional logic, formulae are Boolean combinations of propositions. A proposition is just a letter (variable).

First-Order Logic: Overview

In propositional logic, formulae are Boolean combinations of propositions. A proposition is just a letter (variable).

Can be used to model certain finite scenarios. E.g., we can model 10 time units with variables $x_1, \ldots, x_{10}$. Then $x_1 \wedge \neg x_2 \wedge x_3 \wedge \neg x_4 \wedge x_5 \ldots$ expresses "alternating state".

First-Order Logic: Overview

In propositional logic, formulae are Boolean combinations of propositions. A proposition is just a letter (variable).

Can be used to model certain finite scenarios. E.g., we can model 10 time units with variables $x_1, \ldots, x_{10}$. Then $x_1 \wedge \neg x_2 \wedge x_3 \wedge \neg x_4 \wedge x_5 \ldots$ expresses "alternating state".

Cannot talk about relations and functions.

Cannot say things like "the state alternates over time".

First-Order Logic: Overview

In propositional logic, formulae are Boolean combinations of propositions. A proposition is just a letter (variable).

Can be used to model certain finite scenarios. E.g., we can model 10 time units with variables $x_1, \ldots, x_{10}$. Then $x_1 \wedge \neg x_2 \wedge x_3 \wedge \neg x_4 \wedge x_5 \ldots$ expresses "alternating state".

Cannot talk about relations and functions.

Cannot say things like "the state alternates over time".

Let us now extend propositional logic to first-order logic.

Variables: Intuition

In first-order logic, we talk about "elements of a universe of discourse" and their "properties".

A variable in first-order logic stands for a element of the universe.

Variables: Intuition

In first-order logic, we talk about “elements of a universe of discourse” and their “properties”.

A variable in first-order logic stands for a element of the universe.

This is in contrast to propositional logic.

It is common to use letters x, y, z for variables.

Predicates: Intuition

A predicate denotes a property/relation.

$p(x) \equiv x$ is a prime number $\quad d(x, y) \equiv x$ is divisible by y

Predicates: Intuition

A predicate denotes a property/relation.

$p(x) \equiv x$ is a prime number $\quad d(x, y) \equiv x$ is divisible by y

Propositional connectives are used to build statements

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

Predicates: Intuition

A predicate denotes a property/relation.

$p(x) \equiv x$ is a prime number $\quad d(x, y) \equiv x$ is divisible by y

Propositional connectives are used to build statements

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

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

Predicates: Intuition

A predicate denotes a property/relation.

$p(x) \equiv x$ is a prime number $\quad d(x, y) \equiv x$ is divisible by y

Propositional connectives are used to build statements

- x is a prime and 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

Predicates: Intuition

A predicate denotes a property/relation.

$p(x) \equiv x$ is a prime number $\quad d(x, y) \equiv x$ is divisible by y

Propositional connectives are used to build statements

- x is a prime and 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

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

Predicates: Intuition (2)

We can represent only "abstractions" of these in propositional logic, e.g., $p \wedge (d_1 \vee d_2)$ could be an abstraction of $p(x) \wedge (d(y, x) \vee d(z, x))$.

Here p stands for "x is a prime" and d_1 stands for "y is divisible by x".

Functions: Intuition

- A constant stands for a “fixed thing” in a universe.

Functions: Intuition

- A constant stands for a "fixed thing" in a universe.
- More generally, a function of arity n expresses an n-ary operation over some universe, e.g.

Function	arity	expresses . . .
0		
s		
$+$		

Functions: Intuition

- A constant stands for a "fixed thing" in a universe.
- More generally, a function of arity n expresses an n-ary operation over some universe, e.g.

Function	arity	expresses . . .
0	nullary	
s	unary	
$+$	binary	

Functions: Intuition

- A constant stands for a "fixed thing" in a universe.
- More generally, a function of arity n expresses an n-ary operation over some universe, e.g.

Function	arity	expresses ...
0	nullary	number "0"
s	unary	successor in $\mathcal{N}$
$+$	binary	function plus in $\mathcal{N}$

Quantifiers: Intuition

- A variable stands for "some element" in the universe of discourse. Quantifiers $\forall, \exists$ are used to speak about all or some members of this universe.

Quantifiers: Intuition

- A variable stands for "some element" in the universe of discourse. Quantifiers $\forall, \exists$ are used to speak about all or some members of this universe.
- Examples: Are they satisfiable? valid?

$$\forall x.\, \exists y.\, y * 2 = x$$

Quantifiers: Intuition

- A variable stands for "some element" in the universe of discourse. Quantifiers $\forall, \exists$ are used to speak about all or some members of this universe.
- Examples: Are they satisfiable? valid?

$$\forall x.\, \exists y.\, y * 2 = x \quad \text{true for rationals}$$

Quantifiers: Intuition

- A variable stands for "some element" in the universe of discourse. Quantifiers $\forall, \exists$ are used to speak about all or some members of this universe.
- Examples: Are they satisfiable? valid?

$$\forall x.\, \exists y.\, y * 2 = x \quad \text{true for rationals}$$

$$x < y \rightarrow \exists z.\, x < z \wedge z < y$$

Quantifiers: Intuition

- A variable stands for "some element" in the universe of discourse. Quantifiers $\forall, \exists$ are used to speak about all or some members of this universe.
- 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

Quantifiers: Intuition

- A variable stands for "some element" in the universe of discourse. Quantifiers $\forall, \exists$ are used to speak about all or some members of this universe.
- Examples: Are they satisfiable? valid?

$$\forall x.\, \exists y.\, y * 2 = x \quad \text{true for rationals}$$

$$x < y \rightarrow \exists z.\, x < z \wedge z < y \quad \text{true for any dense order}$$

$$\exists x.\, x \neq 0$$

Quantifiers: Intuition

- A variable stands for "some element" in the universe of discourse. Quantifiers $\forall, \exists$ are used to speak about all or some members of this universe.
- 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 universes with more than one element

Quantifiers: Intuition

- A variable stands for "some element" in the universe of discourse. Quantifiers $\forall, \exists$ are used to speak about all or some members of this universe.
- 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 universes with more than one element
$(\forall x.\, p(x, x)) \rightarrow p(a, a)$	

Quantifiers: Intuition

- A variable stands for "some element" in the universe of discourse. Quantifiers $\forall, \exists$ are used to speak about all or some members of this universe.
- 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 universes with more than one element
$(\forall x. p(x, x)) \rightarrow p(a, a)$	valid

First-Order Logic: Syntax

- Two syntactic categories: terms and formulae
- A first-order language is characterized by giving a finite collection of function symbols $\mathcal{F}$ and predicates $\mathcal{P}$ as well as a set Var of variables.

First-Order Logic: Syntax

- Two syntactic categories: terms and formulae
- A first-order language is characterized by giving a finite collection of function symbols $\mathcal{F}$ and predicates $\mathcal{P}$ as well as a set Var of variables.
- Sometimes write f^i (or p^i) to indicate that function symbol f (predicate p) has arity $i \in \mathcal{N}$.

First-Order Logic: Syntax

- Two syntactic categories: terms and formulae
- A first-order language is characterized by giving a finite collection of function symbols $\mathcal{F}$ and predicates $\mathcal{P}$ as well as a set Var of variables.
- Sometimes write f^i (or p^i) to indicate that function symbol f (predicate p) has arity $i \in \mathcal{N}$.
- One often calls the pair $(\mathcal{F}, \mathcal{P})$ a signature.

Terms in First-Order Logic

$Term$, the set of terms, is the smallest set where

1. $x \in Term$ if $x \in Var$, and
2. $f^n(t_1, \ldots, t_n) \in Term$ if $f^n \in \mathcal{F}$ and $t_j \in Term$, for all $1 \leq j \leq n$.

Formulae in First-Order Logic

$Form$, the set of formulae, is the smallest set where

1. $\bot \in Form$,
2. $p^n(t_1, \ldots, t_n) \in Form$ if $p^n \in \mathcal{P}$ and $t_j \in Term$, for all $1 \leq j \leq n$,
3. $\neg\phi \in Form$ if $\phi \in Form$,
4. $(\phi \circ \psi) \in Form$ if $\phi \in Form$, $\psi \in Form$ and $\circ \in \{\wedge, \vee, \rightarrow\}$,
5. $\forall x.\, \phi \in Form$ and $\exists x.\, \phi \in Form$ if $\phi \in Form$ and $x \in Var$.

The formulae 2 above are called atoms.

Variable Occurrences

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

  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:

  $$(q(x) \lor \exists x.\, \forall y.\, p(f(x), z) \land q(a)) \lor \forall x.\, r(x, z, g(x))$$

Which are bound?

Variable Occurrences

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

  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:

  $(q(x) \lor \exists x.\, \forall y.\, p(f(x), z) \land q(a)) \lor \forall x.\, r(x, z, g(x))$

Which are bound?

Which are free?

Variable Occurrences

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

  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:

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

Which are bound?

Which are free?

Which are binding?

Variable Occurrences

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

  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:

  $$(q(x) \lor \exists x.\, \forall y.\, p(f(x), z) \land q(a)) \lor \forall x.\, r(x, z, g(x))$$

Which are bound?

Which are free?

Which are binding?

First-Order Logic: Semantics

A structure is a pair $\mathcal{A} = \langle U_\mathcal{A}, I_\mathcal{A} \rangle$ where $U_\mathcal{A}$ is an nonempty set, the universe, and $I_\mathcal{A}$ is a mapping where

1. $I_\mathcal{A}(f^n)$ is an n-ary (total) function on $U_\mathcal{A}$, for $f^n \in \mathcal{F}$,
2. $I_\mathcal{A}(p^n)$ is an n-ary relation on $U_\mathcal{A}$, for $p^n \in \mathcal{P}$, and
3. $I_\mathcal{A}(x)$ is an element of $U_\mathcal{A}$, for each $x \in Var$.

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

The Value of Terms

Let $\mathcal{A}$ be a structure. We define the value of a term t under $\mathcal{A}$, written $\mathcal{A}(t)$, as

1. $\mathcal{A}(x) = x^{\mathcal{A}}$, for $x \in Var$, and
2. $\mathcal{A}(f(t_1, \ldots, t_n)) = f^{\mathcal{A}}(\mathcal{A}(t_1), \ldots, \mathcal{A}(t_n))$.

The Value of Formulae

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

$$\begin{aligned}
\mathcal{A}(\bot) &= 0 \\
\mathcal{A}(p(t_1, \ldots, t_n)) &= \begin{cases} 1 & \text{if } (\mathcal{A}(t_1), \ldots \mathcal{A}(t_n)) \in p^{\mathcal{A}} \\ 0 & \text{otherwise} \end{cases} \\
\mathcal{A}(\neg\phi) &= \begin{cases} 1 & \text{if } \mathcal{A}(\phi) = 0 \\ 0 & \text{otherwise} \end{cases}
\end{aligned}$$

$$\vdots$$

The Value of Formulae (2)

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

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

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

Models

- If $\mathcal{A}(\phi) = 1$, we write $\mathcal{A} \models \phi$ and say ϕ is true in $\mathcal{A}$ or $\mathcal{A}$ is a model of ϕ.

Models

- If $\mathcal{A}(\phi) = 1$, we write $\mathcal{A} \models \phi$ and say ϕ is true in $\mathcal{A}$ or $\mathcal{A}$ is a model of ϕ.
- If every suitable structure is a model, we write $\models \phi$ and say ϕ is valid or ϕ is a tautology.

Models

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

Models

- If $\mathcal{A}(\phi) = 1$, we write $\mathcal{A} \models \phi$ and say ϕ is true in $\mathcal{A}$ or $\mathcal{A}$ is a model of ϕ.
- If every suitable structure is a model, we write $\models \phi$ and say ϕ is valid or ϕ is a tautology.
- If there is at least one model for ϕ, then ϕ is satisfiable.
- If there is no model for ϕ, then ϕ is contradictory.

Models

- If $\mathcal{A}(\phi) = 1$, we write $\mathcal{A} \models \phi$ and say ϕ is true in $\mathcal{A}$ or $\mathcal{A}$ is a model of ϕ.
- If every suitable structure is a model, we write $\models \phi$ and say ϕ is valid or ϕ is a tautology.
- If there is at least one model for ϕ, then ϕ is satisfiable.
- If there is no model for ϕ, then ϕ is contradictory.

There are alternative ways to formulate this.

An Example

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

An Example

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

A model:

$$\begin{aligned} U_{\mathcal{A}} &= \mathcal{N} \\ p^{\mathcal{A}} &= \{(m, n) \mid m < n\} \\ s^{\mathcal{A}}(x) &= x + 1 \end{aligned}$$

An Example

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

A model:

$$\begin{aligned} U_{\mathcal{A}} &= \mathcal{N} \\ p^{\mathcal{A}} &= \{(m, n) \mid m < n\} \\ s^{\mathcal{A}}(x) &= x + 1 \end{aligned}$$

Not a model:

$$\begin{aligned} U_{\mathcal{A}} &= \{\mathsf{a}, \mathsf{b}, \mathsf{c}\} \\ p^{\mathcal{A}} &= \{(\mathsf{a}, \mathsf{b}), (\mathsf{a}, \mathsf{c})\} \\ s^{\mathcal{A}} &= \text{“the identity function”} \end{aligned}$$

Towards a Deductive System

Consider an “ordinary” mathematical proof of

if $x > 2$ then $x^2 > 4$.

Towards a Deductive System

Consider an "ordinary" mathematical proof of

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

In natural language, quantifiers are often implicit.

Proof:

Towards a Deductive System

Consider an "ordinary" mathematical proof of

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

In natural language, quantifiers are often implicit.

Proof: Consider an arbitrary x where $x > 2$.

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

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

Towards a Deductive System

Consider an “ordinary” mathematical proof of

if $x > 2$ then $x^2 > 4$.

In natural language, quantifiers are often implicit.

Proof: Consider an arbitrary x ($\forall$-*I*) where $x > 2$ ($\rightarrow$-*I*). Then $x = 2 + y$ for some $y > 0$ and hence

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

Some phrases used in this proof have a flavor of introduction rules.

Towards a Deductive System

Consider an "ordinary" mathematical proof of

if $x > 2$ then $x^2 > 4$.

In natural language, quantifiers are often implicit.

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?

Weaker Statement

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

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

Weaker Statement

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

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

Intuition: existential statements are proven by giving a witness.