CSU44004/CSU55004: FORMAL VERIFICATION

Lecture 8: First Order Logic

Vasileios Koutavas

School of Computer Science and Statistics
Trinity College Dublin
→ gives a syntax for stating atomic facts and combining facts using the operators ∧, ∨, →, ¬
→ gives rules to symbolically reason about facts
   → does $A_1, \ldots, A_n \vdash B$ hold?
   → is $A_1 \rightarrow \ldots \rightarrow A_n \rightarrow B$ valid?
→ guarantees that reasoning is sound and complete
   → $A_1, \ldots, A_n \vdash B$ holds if and only if $A_1, \ldots, A_n \models B$ holds
→ gives a syntax for stating atomic facts and combining facts using the operators $\land$, $\lor$, $\rightarrow$, $\neg$
→ gives rules to symbolically reason about facts
  → does $A_1, \ldots, A_n \vdash B$ hold?
  → is $A_1 \rightarrow \ldots \rightarrow A_n \rightarrow B$ valid?
→ guarantees that reasoning is sound and complete
  → $A_1, \ldots, A_n \vdash B$ holds if and only if $A_1, \ldots, A_n \models B$ holds

How would you represent the following statement in propositional logic?

“Every student is younger than some instructor”

“For every natural number $i$ within the domain of array $A$, the value of $A$ at $i$ is larger than or equal to the value of $A$ at every $j$ less than $i$”
→ gives a syntax for stating atomic facts and combining facts using the operators $\land$, $\lor$, $\rightarrow$, $\neg$
→ gives rules to symbolically reason about facts
  → does $A_1, \ldots, A_n \vdash B$ hold?
  → is $A_1 \rightarrow \ldots \rightarrow A_n \rightarrow B$ valid?
→ guarantees that reasoning is sound and complete
  → $A_1, \ldots, A_n \vdash B$ holds if and only if $A_1, \ldots, A_n \models B$ holds

How would you represent the following statement in propositional logic?

“Every student is younger than some instructor”
“For every natural number $i$ within the domain of array $A$, the value of $A$ at $i$ is larger than or equal to the value of $A$ at every $j$ less than $i$”

Only way to write this is as an atomic fact:

$p$: “Every student is younger than some instructor”
$q$: “Every item of array $A$ is larger than all the items to its left”

We need a richer logic to reason about “every”, “some”, “younger”,
“Every student is younger than some instructor”

First Order Logic (FOL), AKA Predicate Logic is logic which has the operators $\land$, $\lor$, $\neg$, $\rightarrow$ and:

- **Terms**: ‘andy’, ‘paul’ can represent two students
  
- **this is only syntax**
“Every student is younger than some instructor”

First Order Logic (FOL), AKA Predicate Logic is logic which has the operators $\land$, $\lor$, $\lnot$, $\rightarrow$ and:

→ **Terms**: ‘andy’, ‘paul’ can represent two students
  → this is only syntax
→ **Predicates**: 
“Every student is younger than some instructor”

First Order Logic (FOL), AKA Predicate Logic is logic which has the operators $\land$, $\lor$, $\neg$, $\rightarrow$ and:

- **Terms**: ‘andy’, ‘paul’ can represent two students
  - this is only syntax

- **Predicates**:
  - unary predicates can express a property of a term:
    - $S(andy)$ can represent “andy is a student”
    - $I(paul)$ can represent “paul is an instructor”
    - $LengthA(five)$ can represent “five is the length of array A”
“Every student is younger than some instructor”

First Order Logic (FOL), AKA Predicate Logic is logic which has the operators $\land$, $\lor$, $\neg$, $\rightarrow$ and:

→ **Terms**: ‘andy’, ‘paul’ can represent two students
   → this is only *syntax*

→ **Predicates**:
   → **unary predicates** can express a **property of a term**:
     → $S(andy)$ can represent “andy is a student”
     → $I(paul)$ can represent “paul is an instructor”
     → $LengthA(five)$ can represent “five is the length of array A”
   → **multi-arity predicates** can express a **relation between terms**:
     → $Y(andy, paul)$ can represent that “andy is younger than paul”
     → $LT(five, six)$ can represent that “five is less than six”
“Every student is younger than some instructor”

How can we talk about all students?
“Every student is younger than some instructor”

How can we talk about all students?

→ enumerate: $S(andy), S(bob), S(carol), \ldots$
“Every student is younger than some instructor”

How can we talk about all students?

→ enumerate: $S(andy), S(bob), S(carol), \ldots$
→ what if they are infinite?
“Every student is younger than some instructor”

How can we talk about all students?

→ enumerate: $S(andy), S(bob), S(carol), \ldots$
→ what if they are infinite?
→ FOL uses variables and universal quantification $\forall$
  → $\forall x.\ S(x)$ represents “all terms are students”
  → $\forall x.\ (S(x) \rightarrow \ldots)$ represents “for all terms who are students, ...”
“Every student is younger than some instructor”

How can we talk about the existence of at least one instructor?

How can we represent “Every item of array A is larger than all the items to its left”?
“Every student is younger than some instructor”

How can we talk about the existence of at least one instructor?
→ enumerate: \( l(paul), l(john), l(mary), \ldots \)

How can we represent “Every item of array A is larger than all the items to its left”?
“Every student is younger than some instructor”

How can we talk about the existence of at least one instructor?

→ enumerate: $I(paul), I(john), I(mary), \ldots$

→ what if the instructor depends on the student we pick?

How can we represent “Every item of array A is larger than all the items to its left”?
“Every student is younger than some instructor”

How can we talk about the existence of at least one instructor?

→ enumerate: \( l(paul), l(john), l(mary), \ldots \)

→ what if the instructor depends on the student we pick?

→ FOL uses variables and existential quantification \( \exists \)
   - \( \exists x. \; l(x) \) represents “there exists (at least one) term which is an instructor”
   - \( \exists x. \; (l(x) \land Y(andy, x)) \) represents “there exists a term which is an instructor and andy is younger than this instructor”

How can we represent “Every item of array A is larger than all the items to its left”?
“Every student is younger than some instructor”

How can we talk about the existence of at least one instructor?

→ enumerate: \( I(paul), I(john), I(mary), \ldots \)

→ what if the instructor depends on the student we pick?

→ FOL uses variables and existential quantification \( \exists \)
  
  → \( \exists x. I(x) \) represents “there exists (at least one) term which is an instructor”
  
  → \( \exists x. (I(x) \land Y(andy, x)) \) represents “there exists a term which is an instructor and \( andy \) is younger than this instructor”
  
  → \( \forall x. (S(x) \rightarrow \exists y. (I(y) \land Y(x,y))) \) represents...?
  
  → “for every term \( x \), if \( x \) is a student then there exists term \( y \) such that \( y \) is an instructor and \( x \) is younger than \( y \)”

How can we represent “Every item of array \( A \) is larger than all the items to its left”? 
“Not all birds can fly”
“Not all birds can fly”

→ $B(x)$ represents “$x$ is a bird”
ANOTHER EXAMPLE

“Not all birds can fly”

→ $B(x)$ represents “$x$ is a bird”
→ $F(y)$ represents “$y$ can fly”
ANOTHER EXAMPLE

“Not all birds can fly”

→ $B(x)$ represents “$x$ is a bird”
→ $F(y)$ represents “$y$ can fly”
→ $\forall x. (B(x) \rightarrow \ldots)$ represents “all birds”
ANOTHER EXAMPLE

“Not all birds can fly”

→ $B(x)$ represents “$x$ is a bird”
→ $F(y)$ represents “$y$ can fly”
→ $\forall x. (B(x) \rightarrow \ldots)$ represents “all birds”
→ $\forall x. (B(x) \rightarrow F(x))$ represents “all birds can fly”
Another example

“Not all birds can fly”

→ \( B(x) \) represents “\( x \) is a bird”
→ \( F(y) \) represents “\( y \) can fly”
→ \( \forall x. (B(x) \rightarrow \ldots) \) represents “all birds”
→ \( \forall x. (B(x) \rightarrow F(x)) \) represents “all birds can fly”
→ \( \neg \forall x. (B(x) \rightarrow F(x)) \) represents “not all birds can fly”
ANOTHER EXAMPLE

“Not all birds can fly”

→ $B(x)$ represents “$x$ is a bird”
→ $F(y)$ represents “$y$ can fly”
→ $\forall x. (B(x) \rightarrow \ldots)$ represents “all birds”
→ $\forall x. (B(x) \rightarrow F(x))$ represents “all birds can fly”
→ $\neg \forall x. (B(x) \rightarrow F(x))$ represents “not all birds can fly”
→ Is there an equivalent English sentence to say the same without using “all”?
“Not all birds can fly”

→ $B(x)$ represents “$x$ is a bird”
→ $F(y)$ represents “$y$ can fly”
→ $\forall x.(B(x) \rightarrow \ldots)$ represents “all birds”
→ $\forall x.(B(x) \rightarrow F(x))$ represents “all birds can fly”
→ $\neg \forall x.(B(x) \rightarrow F(x))$ represents “not all birds can fly”
→ Is there an equivalent English sentence to say the same without using “all”?
→ $\exists x.(B(x) \land \neg F(x))$
FOL reasons about the properties of terms

Terms in FOL are strings from the syntax:

\[ t ::= x \mid c \mid f(t, \ldots, t) \]

A term can be:

→ a **variable**

→ e.g.: \( x, y, z, \ldots \)
FOL reasons about the properties of terms

Terms in FOL are strings from the syntax:

\[ t ::= x \mid c \mid f(t, \ldots, t) \]

A term can be:

→ a variable
  → e.g.: \( x, y, z, \ldots \)

→ a constant \( c \), AKA a nullary function (a function with zero arguments)
  → e.g.: andy, mary, ...
  → we pick constants from a set \( \mathcal{F} \) of functions
**TERMS**

**FOL reasons about the properties of terms**

Terms in FOL are strings from the syntax:

\[ t ::= x \mid c \mid f(t, \ldots, t) \]

A term can be:

- a **variable**
  - e.g.: \( x, y, z, \ldots \)

- a **constant** \( c \), AKA a nullary function (a function with zero arguments)
  - e.g.: \( andy, mary, \ldots \)
  - we pick constants from a set \( F \) of functions

- an application of an \( n \)-ary \( (n > 0) \) function \( f \) to \( n \) terms \( t_1, \ldots, t_n \)
  - e.g. natural numbers:
    - \( zero, succ(zero), succ(succ(zero)), succ(x), \ldots \)
  - we pick functions from the same set \( F \)
FOL reasons about the properties of terms

Formulas in FOL are strings from the syntax:

\[ A ::= P(t_1, \ldots, t_n) \mid (\neg A) \mid (A \land A) \mid (A \lor A) \mid (A \to A) \mid \forall x. A \mid \exists x. A \]

A formula can be:

\[ \to \text{ an application of a predicate } P \text{ with arity } n > 0 \text{ to terms } t_1, \ldots, t_n \]
\[ \to \text{ e.g.: } l(\text{mary}), Y(\text{andy}, x) \]
\[ \to \text{ we pick constants from a set } \mathcal{P} \]
FORMULAS

FOL reasons about the properties of terms

Formulas in FOL are strings from the syntax:

\[ A ::= P(t_1, \ldots, t_n) \mid (\neg A) \mid (A \land A) \mid (A \lor A) \mid (A \rightarrow A) \mid \forall x.A \mid \exists x.A \]

A formula can be:

\[ \rightarrow \text{ an application of a predicate } P \text{ with arity } n > 0 \text{ to terms } t_1, \ldots, t_n \]
\[ \rightarrow \text{ e.g.: } I(\text{mary}), Y(\text{andy}, x) \]
\[ \rightarrow \text{ we pick constants from a set } \mathcal{P} \]
\[ \rightarrow \text{ if } A, B \text{ are formulas then so are } (\neg A), (A \land B), (A \lor B), (A \rightarrow B) \]
FOL reasons about the properties of terms

Formulas in FOL are strings from the syntax:

\[ A ::= P(t_1, \ldots, t_n) \mid (\neg A) \mid (A \land A) \mid (A \lor A) \mid (A \rightarrow A) \mid \forall x.A \mid \exists x.A \]

A formula can be:

- an application of a predicate \( P \) with arity \( n > 0 \) to terms \( t_1, \ldots, t_n \)
  - e.g.: \( l(mary) \), \( Y(andy, x) \)
  - we pick constants from a set \( \mathcal{P} \)
- if \( A, B \) are formulas then so are \( (\neg A) \), \( (A \land B) \), \( (A \lor B) \), \( (A \rightarrow B) \)
- if \( A \) is a formula and \( x \) is a variable then \( \forall x.A \) and \( \exists x.A \) are formulas.
FOL SYNTAX

\[ t ::= x \mid c \mid f(t, \ldots, t) \]
\[ A ::= P(t_1, \ldots, t_n) \mid (\neg A) \mid (A \land A) \mid (A \lor A) \mid (A \rightarrow A) \mid \forall x.A \mid \exists x.A \]

binding priorities:

\neg \forall x, \exists x \text{ bind more tightly than} \quad \land \text{ and } \lor \text{ which bind more tightly than} \quad \rightarrow \text{ which is right-associative}

FOL formulas are syntax trees where

\rightarrow all the \textbf{leaves} are \textbf{terms}
\rightarrow all \textbf{nodes above leaves} are \textbf{predicates}
\rightarrow and all \textbf{other internal nodes} are \textbf{operators}
Express in FOL and write as a syntax tree the following:
“every son of my father is my brother”