Integer Logic Syntax

\[ p, q := \neg p \mid p \land q \mid p \lor q \mid x = y \mid x < y \]

Boolean Expressions

\[ x, y := v \mid n \mid -x \mid x + y \mid x \times y \]

Integer Expressions

Equality, comparison?
Quantifier Semantics

\[ p, q := \ldots \mid \forall v, p \mid \exists v, p \]

For all integers \( v \), \( p \) is true

For some integer \( v \), \( p \) is true

\[ \llbracket v \rrbracket_\Gamma = \text{value of } v \text{ in } \Gamma \]

\[ \llbracket x + y \rrbracket_\Gamma = \text{sum of } \llbracket x \rrbracket_\Gamma \text{ and } \llbracket y \rrbracket_\Gamma \]

\[ \llbracket \forall v, p \rrbracket_\Gamma = \llbracket p \rrbracket_{\Gamma'} \text{ for all } \Gamma', \text{ where} \]

\[ \Gamma'[x] = \Gamma[x] \text{ for all } x \text{ except } v \]

Semantics of \( \forall \)
Theory of Arrays

Theory: a set of sorts, constants, functions, and relations
Theories are like programs, the logic like an OS

Sorts
- Int
- Array

Functions
- $\neg \text{Int} : \text{Int}$
- $\text{Int} + \text{Int} : \text{Int}$
- $\text{Int} \times \text{Int} : \text{Int}$
- $\text{Array}[\text{Int}] : \text{Int}$
- $\text{len} (\text{Array}) : \text{Int}$
- $\text{Array}[\text{Int} := \text{Int}] : \text{Int}$

Constants
- $n : \text{Int}$

Relations
- $\text{Int} = \text{Int}$
- $\text{Int} < \text{Int}$
- $\text{Int} \in \text{Array}$

Separate the logic from the data and operations
Class Progress

Logical reasoning

Program logics

Static analysis

First-order Logic

Decision Procedures

Boolean logic

Syntax

Proof

Theory
First-order Proof

What kind of evidence supports truth?
  Universal elements and witnesses

Axioms to internalize semantic facts
  Proving an axiom; using an axiom in a proof

Does proof work? Completeness and incompleteness
  On the gap between map and territory
The Big Picture

How is logic related to verification?
Quicksort

Post: \text{sorted(output)}

def quicksort(l):
    \textbf{pivot} = l[len(l)//2]
    \text{left}, \text{right} = \text{partition}(l, \text{pivot})
    \text{left2} = \text{quicksort(left)} \leftarrow \text{sorted(left2)}
    \text{right2} = \text{quicksort(right)} \leftarrow \text{sorted(right2)}
    \text{return left2 + right2}

\text{sorted}() := l[i] \leq l[i+1]
Using Logic

Know

\[ \text{sorted}(\text{left2}) \]

\[ \text{sorted}(\text{right2}) \]

\[ \forall i, \forall j, \text{left2}[i] < \text{right2}[j] \]

Want

\[ \text{sorted}(\text{left2} + \text{right2}) \]
Using Logic

Know

\[ \forall i, \text{left2}[i] < \text{left2}[i + 1] \]

\text{sorted(right2)}

\[ \forall i, \forall j, \text{left2}[i] < \text{right2}[j] \]

Want

\text{sorted(left2 + right2)}
Using Logic

Know

\[ \forall i, \text{left2}[i] < \text{left2}[i + 1] \]

\[ \forall i, \text{right2}[i] < \text{right2}[i + 1] \]

\[ \forall i, \forall j, \text{left2}[i] < \text{right2}[j] \]

Want

\text{sorted(left2 + right2)}
Using Logic

Know

∀ i, left2[i] < left2[i + 1] *

∀ i, right2[i] < right2[i + 1] *

∀ i, ∀ j, left2[i] < right2[j]

Want

∀ i, (left2 + right2)[i]

< (left2 + right2)[i + 1] *

How do we do this?
Evidence of Truth

Proofs of first-order logic statements
Logical Evidence

$\forall x, \exists y, x = y \times y$  
$\text{No} \rightarrow \text{Consider } x = 3$

$\exists x, \forall y, x = y \times y$  
$\text{No} \rightarrow \text{Consider } y = x + 1$

$\forall y, \exists x, x = y \times y$  
$\text{Yes} \rightarrow \text{Consider } x = y \times y$

$\exists y, \forall x, x = y \times y$  
$\text{No} \rightarrow \text{Consider } x = y \times y + 1$
Logical Evidence

\[ \neg \forall x, \exists y, x = y \times y \quad \text{Yes} \rightarrow \text{Consider } x = 3 \]

\[ \exists x, \forall y, x = y \times y \quad \text{No} \rightarrow \text{Consider } y = x + 1 \]

\[ \forall y, \exists x, x = y \times y \quad \text{Yes} \rightarrow \text{Consider } x = y \times y \]

\[ \exists y, \forall x, x = y \times y \quad \text{No} \rightarrow \text{Consider } x = y \times y + 1 \]
Logical Evidence

\[ \exists x, \forall y, x \neq y \times y \quad \text{Yes} \rightarrow \text{Consider } x = 3 \]

\[ \exists x, \forall y, x = y \times y \quad \text{No} \rightarrow \text{Consider } y = x + 1 \]

\[ \forall y, \exists x, x = y \times y \quad \text{Yes} \rightarrow \text{Consider } x = y \times y \]

\[ \exists y, \forall x, x = y \times y \quad \text{No} \rightarrow \text{Consider } x = y \times y + 1 \]
Logical Evidence

\[ \exists x, \forall y, x \neq y \times y \quad \text{Yes} \rightarrow \text{Consider } x = 3 \]

\[ \forall x, \exists y, x \neq y \times y \quad \text{Yes} \rightarrow \text{Consider } y = x + 1 \]

\[ \forall y, \exists x, x = y \times y \quad \text{Yes} \rightarrow \text{Consider } x = y \times y \]

\[ \forall y, \exists x, x \neq y \times y \quad \text{Yes} \rightarrow \text{Consider } x = y \times y + 1 \]

**Common:** If \( \exists a \) quantifier, value for \( a \)
Logical Evidence

\[ \exists x, \forall y, x \neq y \times y \]

Yes \rightarrow Consider \( x = 3 \)

\[ \forall x, \exists y, x \neq y \times y \]

Yes \rightarrow Consider \( y = x + 1 \)

\[ \forall y, \exists x, x = y \times y \]

Yes \rightarrow Consider \( x = y \times y \)

\[ \forall y, \exists x, x \neq y \times y \]

Yes \rightarrow Consider \( x = y \times y + 1 \)

Common: \( a \) depends on \( b \) only if \( \forall b \) outside \( \exists a \)
Logical Evidence

Two notions: values and dependency

\[[\nu] \, p\] Prove \(p\) using variable \(\nu\)

\(p[\nu := e]\) Prove \(p\) with \(\nu\) replaced by \(e\)

Formally state rules of evidence

\[x \notin \Gamma \quad \frac{[\Gamma, x] \, p}{[\Gamma] \, \forall x, \, p}\]

\[e \text{ from } \Gamma \quad \frac{[\Gamma] \, p[x := e]}{[\Gamma] \, \exists x, \, p}\]
Logical Evidence

$$x \notin \Gamma \quad \frac{[\Gamma, x] ~ p}{[\Gamma] \forall x, p}$$

$$[\Gamma] e \quad \frac{[\Gamma] ~ p[x := e]}{[\Gamma] \exists x, p}$$

What about evidence for other connectives?

**Statement** $p$  
Convert $p$ into **prefix form**; $p'$ has no quantifiers

**Statement** $Qx_1, \ldots, Qx_n, p'$  
Convert $p'$ into **conjunctive form**

**Statement** $Qx_1, \ldots, Qx_n, (a_1 \lor a_2 \lor \ldots) \land (b_1 \lor \ldots) \land \ldots$
Logical Evidence

Statement $Qx_1, \ldots, Qx_n, (a_1 \lor a_2 \lor \ldots) \land (b_1 \lor \ldots) \land \ldots$

$x_k = e_k$

Proof by resolution

Proof transforms $p$ into $a'_1 \land \neg a'_2 \land \ldots$

Each $a'_i = a_i[x_k = e_k]_k$ is a relation from the domain
Example

∀x, (∃y, x = y × y ∧ y ≠ 0) → 0 < x

Definition of (→)

∀x, ¬(∃y, x = y × y ∧ y ≠ 0) ∨ 0 < x

Prefix form

∀x, ∀y, ¬(x = y × y ∧ y ≠ 0) ∨ 0 < x

Conjunctive form

∀x, ∀y, x ≠ y × y ∨ y = 0 ∨ 0 < x
Summary

Quantifiers → Values for $\exists x$ values

Boolean logic → Proof by resolution

Relations → ???

Statement → Evidence
Axioms
Making the world legible
Domain Facts

Talked about evidence of first-order logic statements

Reduced to simple problem: evidence of relations

\[ \forall x, x < 0 \lor x = 0 \lor 0 < x \]

Which terms are true depends on \( x \)

Asked to prove a basic fact about the \(<\) relation

How many basic facts are there?
Domain Facts

Basic facts **imply** other facts!

\[
x \times 0 = 0
\]

\[
x < 0 \lor x = 0 \lor 0 < x
\]

\[
x < 0 \land a < b \rightarrow x \times b < x \times a
\]

\[
[a := x, b := 0]
\]

\[
0 < x \land a < b \rightarrow x \times a < x \times b
\]

\[
a = b \land c = d \rightarrow a \times c = b \times d
\]

\[
x \times x = 0 \lor 0 < x \times x
\]
Domain Facts

Basic facts **imply** other facts!

\[ x \times 0 = 0 \]

\[ x < 0 \lor x = 0 \lor 0 < x \]

\[ x < 0 \land x < 0 \rightarrow x \times 0 < x \times x \]

\[ 0 < x \land a < b \rightarrow x \times a < x \times b \]

\[ a = b \land c = d \rightarrow a \times c = b \times d \]

\[ x \times x = 0 \lor 0 < x \times x \]
Domain Facts

Basic facts **imply** other facts!

\[
x \times 0 = 0
\]

\[
x < 0 \lor x = 0 \lor 0 < x
\]

\[
x < 0 \land x < 0 \rightarrow x \times 0 < x \times x
\]

\[\]

\[\]

\[a := x, b := 0\]

\[a := 0, b := x\]

\[a := x, b := 0\]

\[c := x, d := 0\]

\[
x \times x = 0 \lor 0 < x \times x
\]
Domain Facts

Basic facts **imply** other facts!

**Abstract block to boolean**

\[
\begin{align*}
    x \times 0 &= 0 & x &= x \\
    x < 0 \lor x = 0 \lor 0 < x \\
    x < 0 \land x < 0 &\implies x \times 0 < x \times x \\
    0 < x \land 0 < x &\implies x \times 0 < x \times x \\
    x = 0 \land x = x &\implies x \times x = 0 \times 0 \\
    x \times x &= 0 \lor 0 < x \times x
\end{align*}
\]
Domain Facts

Basic facts **imply** other facts!

Pure boolean expression!
Axioms

Set of basic facts you use to prove other facts

\[
\frac{\Gamma \vdash a_1, a_2, \ldots}{\vdash p} \quad \text{Axioms}
\]

Axioms can be quantified, with rules:

\[
\frac{e}{\Gamma \vdash a[x := e] \vdash p}
\]

\[
\frac{\Gamma \vdash \forall x, a \vdash p}{\Gamma \vdash \forall x, a \vdash p}
\]

\[
\frac{x \not\in \Gamma}{\Gamma, x \vdash a \vdash p}
\]

\[
\frac{\Gamma, x \vdash a \vdash p}{\Gamma \vdash \exists x, a \vdash p}
\]
Example

\[
\begin{align*}
\neg a \lor a & \quad \text{Resolution} \\
[x] \neg P(x) \lor P(x) & \quad \text{Abstract out } P(x) \\
[x] P(x) \rightarrow P(x) & \quad \text{Definition of } \rightarrow \\
[x] P(x) \vdash P(x) & \quad \text{Definition of } \vdash \\
[x] \forall y, P(y) \vdash P(x) & \quad y := x \\
[ ] \forall y, P(y) \vdash \forall x, P(x) & \quad x \not\in [ ]
\end{align*}
\]
Summary

Quantifiers → Values for $\exists x$ values

Boolean logic → Proof by resolution

+ Relations → ???

Statement → Evidence
<table>
<thead>
<tr>
<th>Summary</th>
<th>Values for $\exists x$ values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Quantifiers</td>
<td></td>
</tr>
<tr>
<td>Boolean logic</td>
<td>Proof by resolution</td>
</tr>
<tr>
<td>Axioms</td>
<td>???</td>
</tr>
<tr>
<td>Relations</td>
<td>Implied by axioms</td>
</tr>
<tr>
<td>Statement</td>
<td>Evidence</td>
</tr>
</tbody>
</table>
Course Updates
Details on Assignment 1
Survey Comments

I am a little lost about the connection between lecture and software verification.

Pace was a little slow.  It's a little difficult to keep up.

The examples were helpful.

Great if there could be some short exercises.  
Would be helpful to have a few practice problems.
Exercises

Experiment with exercises for some lectures

http://logitext.mit.edu

Introduces sequent calculus for first-order logic

Similar to what was introduced in class

Interactive proof tool right in the browser

Textbook, exercises don’t exactly match lecture

Such variations improve learning (make you think)
Choosing Axioms
Completeness, incompleteness, and the possible
Example

Reasoning about nodes of this graph

Constants: $a, b, c, d$  Relations: $\text{edge}(x, y)$

- $\text{edge}(a, b)$, $\text{edge}(b, c)$
- $\text{edge}(a, c)$, $\neg\text{edge}(b, d)$
- $\neg\text{edge}(a, d)$, $\neg\text{edge}(c, d)$
- $\forall x, \neg\text{edge}(x, x)$
- $\forall x, \forall y, \text{edge}(x, y) \rightarrow \text{edge}(y, x)$

Are they correct?  Are they useful?
Whose Axioms?

Axioms come with the **theory**, not the problem
Responsibility of **logic designer**, not the prover

**Prover questions**
- What’re the axioms?
- Which to use?

**Logician questions**
- Are they correct?
- Are they useful?

No easy answers!
Wrong Axioms

What happens if you have a false axiom?

\[ \exists x, x \neq x \quad \forall y, y = y \]

Now you can prove false things!

\[
\begin{array}{c}
\hline
a \land \neg a \rightarrow \bot \\
\hline
\end{array}
\]

\[ [x] x \neq x, x = x \vdash \bot \]

\[ [x] x \neq x, (\forall y, y = y) \vdash \bot \]

\[ [\ ] (\exists x, x \neq x), (\forall y, y = y) \vdash \bot \]

Resolution

Abstract \( x = x \)
\[ y := x \]
\[ x \notin [\ ] \]
What happens if you have a missing axiom?

Now you can’t prove $\exists x, \exists y, \neg \text{edge}(x, y)$
Impossibility

Some things **cannot** be axiomatized well

Could you axiomatize **reachability** from graphs?

**Relation:** \( \text{path}(x, y) \)

**Axiom:** \( \forall x, \forall y, \text{path}(x, y) \leftrightarrow x = y \lor \exists z, \text{edge}(x, z) \land \text{path}(z, y) \)

Prove: \( \neg \text{path}(a, d) \)
Whence Axioms

Axiomatizing things seems **hard** and **risky**

Hence, **standard theories** known to work well

- Equality
- Strings
- Reals
- Integers
- Arrays
- Sets
- RegEx

Next time: describe theories & **what can be proven**
Next class:
First-order Theories

To do:
☐ Course feedback
☐ Read / do LogiText
☐ Assignment 1 due
First-order Proof

What kind of *evidence* supports truth?

Universal elements and witnesses

**Axioms** to internalize semantic facts

Proving an axiom; using an axiom in a proof

How do you *pick* axioms?

On the gap between map and territory
INTEGERS

INFINITE AXIOMS
Arrays

Mixed Theories
Next class:
First-order Theories

To do:
- Course feedback
- Read / do LogiText
- Assignment 1 due