First-order Proofs

Specifications section, **Logic** topic, **Lecture 4**

Pavel Panchekha

CS 6110, U of Utah

16 January 2020

Integer Logic Syntax

$$\begin{aligned} p, q &:= \neg p \mid p \wedge q \mid p \vee q \\ &\mid x = y \mid x < y \end{aligned}$$

Boolean Expressions

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

Integer Expressions

Equality, comparison?

Quantifier Semantics

$$p, q := \dots \mid \forall v, p \mid \exists v, p$$

For all integers v, p is true

For some integer v, p is true

$[\![v]\!]_\Gamma =$ **value of** v **in** Γ

$[\![x + y]\!]_\Gamma =$ **sum of** $[\![x]\!]_\Gamma$ **and** $[\![y]\!]_\Gamma$

$[\![\forall v, p]\!]_\Gamma = [\![p]\!]_{\Gamma'}$ **for all** Γ'**, where**

$\Gamma'[x] = \Gamma[x]$ **for all** x **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

Constants

n : Int

Functions

$-Int : Int$

$Int + Int : Int$

$Int \times Int : Int$

$Array[\, Int \,] : Int$

$\mathbf{len}(Array) : Int$

$Array[\, Int := Int \,] : Int$

Relations

$Int = Int$

$Int < Int$

$Int \in Array$

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: sorted(**output**)

sorted(l) := **l[i] ≤ l[i+1]**

```
def quicksort(l):
    pivot = l[len(l)//2]
    left, right = partition(l, pivot)
    left2 = quicksort(left)    ← sorted(left2)
    right2 = quicksort(right)  ← sorted(right2)
    return left2 + right2
```

Spec: left[i] < right[j]

sorted?

Using Logic

Know

$$\textbf{sorted}(\textbf{left2})$$

$$\textbf{sorted}(\textbf{right2})$$

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

Want

$$\textbf{sorted}(\textbf{left2} + \textbf{right2})$$

Using Logic

Know

$$\forall i, \textbf{left2}[i] < \textbf{left2}[i+1]$$ *

$$\textbf{sorted}(\textbf{right2})$$

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

Want

$$\textbf{sorted}(\textbf{left2} + \textbf{right2})$$

Using Logic

Know

$\forall i, \textbf{left2}[i] < \textbf{left2}[i+1]$ *

$\forall i, \textbf{right2}[i] < \textbf{right2}[i+1]$ *

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

Want

$\textbf{sorted}(\textbf{left2} + \textbf{right2})$

Using Logic

Know

$$\forall i, \textbf{left2}[i] < \textbf{left2}[i+1] \ ^{*}$$

$$\forall i, \textbf{right2}[i] < \textbf{right2}[i+1] \ ^{*}$$

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

Want

$$\forall i, (\textbf{left2} + \textbf{right2})[i] < (\textbf{left2} + \textbf{right2})[i+1] \ ^{*}$$

How do we do this?

Evidence of Truth

Proofs of first-order logic statements

Logical Evidence

$\forall x, \exists y, x = y \times y$ **No** → Consider $x = 3$

$\exists x, \forall y, x = y \times y$ **No** → Consider $y = x + 1$

$\forall y, \exists x, x = y \times y$ **Yes** → Consider $x = y \times y$

$\exists y, \forall x, x = y \times y$ **No** → Consider $x = y \times y + 1$

Logical Evidence

$\neg\, \forall x, \exists y, x = y \times y$ — **Yes** → Consider $x = 3$

$\exists x, \forall y, x = y \times y$ — **No** → Consider $y = x + 1$

$\forall y, \exists x, x = y \times y$ — **Yes** → Consider $x = y \times y$

$\exists y, \forall x, x = y \times y$ — **No** → Consider $x = y \times y + 1$

Logical Evidence

$\exists x, \forall y, x \neq y \times y$	**Yes** → Consider $x = 3$
$\exists x, \forall y, x = y \times y$	**No** → Consider $y = x + 1$
$\forall y, \exists x, x = y \times y$	**Yes** → Consider $x = y \times y$
$\exists y, \forall x, x = y \times y$	**No** → Consider $x = y \times y + 1$

Logical Evidence

$\exists x, \forall y, x \neq y \times y$ **Yes** → Consider $x = 3$

$\forall x, \exists y, x \neq y \times y$ **Yes** → Consider $y = x + 1$

$\forall y, \exists x, x = y \times y$ **Yes** → Consider $x = y \times y$

$\forall y, \exists x, x \neq y \times y$ **Yes** → 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** → Consider $x = 3$

$\forall x, \exists y, x \neq y \times y$ **Yes** → Consider $y = x + 1$

$\forall y, \exists x, x = y \times y$ **Yes** → Consider $x = y \times y$

$\forall y, \exists x, x \neq y \times y$ **Yes** → 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**

$[v]\ p$	Prove p using variable v
$p[v := e]$	Prove p with v replaced by e

Formally state **rules of evidence**

$$x \notin \Gamma \ \frac{[\Gamma, x]\ p}{[\Gamma]\ \forall x, p} \qquad e \textbf{ from } \Gamma \ \frac{[\Gamma]\ p[x := e]}{[\Gamma]\ \exists x, p}$$

Logical Evidence

$$x \notin \Gamma \; \frac{[\Gamma, x]\; p}{[\Gamma]\; \forall x, p} \qquad\qquad [\Gamma]\; e \; \frac{[\Gamma]\; p[x := e]}{[\Gamma]\; \exists x, p}$$

What about evidence for **other connectives**?

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

$\downarrow$

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

$\downarrow$

Statement $Qx_1, \ldots, Qx_n, (a_1 \vee a_2 \vee \ldots) \wedge (b_1 \vee \ldots) \wedge \ldots$

Logical Evidence

$$x \notin \Gamma \; \frac{[\Gamma, x]\; p}{[\Gamma]\; \forall x, p} \qquad\qquad [\Gamma]\; e \; \frac{[\Gamma]\; p[x := e]}{[\Gamma]\; \exists x, p}$$

Statement $\underbrace{Qx_1, \ldots, Qx_n,}_{x_k = e_k} \underbrace{(a_1 \vee a_2 \vee \ldots) \wedge (b_1 \vee \ldots) \wedge \ldots}_{\textbf{Proof by resolution}}$

Proof **transforms** p into $a_1' \wedge \neg a_2' \wedge \ldots$

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

Example

$$\forall x, (\exists y, x = y \times y \land y \neq 0) \rightarrow 0 < x$$

$\downarrow$ **Definition of ($\rightarrow$)**

$$\forall x, \neg(\exists y, x = y \times y \land y \neq 0) \lor 0 < x$$

$\downarrow$ **Prefix form**

$$\forall x, \forall y, \neg\left(x = y \times y \land y \neq 0\right) \lor 0 < x$$

$\downarrow$ **Conjunctive form**

$$\forall x, \forall y, x \neq y \times y \lor y = 0 \lor 0 < x$$

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**

$$\forall x, x < 0 \vee x = 0 \vee 0 < x$$

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!

$$x \times 0 = 0$$

$$x < 0 \vee x = 0 \vee 0 < x$$

$$x < 0 \wedge a < b \rightarrow x \times b < x \times a \qquad [a := x, b := 0]$$

$$0 < x \wedge a < b \rightarrow x \times a < x \times b$$

$$a = b \wedge c = d \rightarrow a \times c = b \times d$$

$$x \times x = 0 \vee 0 < x \times x$$

Domain Facts

Basic facts **imply** other facts!

$$x \times 0 = 0$$

$$x < 0 \vee x = 0 \vee 0 < x$$

$$x < 0 \wedge x < 0 \rightarrow x \times 0 < x \times x \qquad [a := x, b := 0]$$

$$0 < x \wedge a < b \rightarrow x \times a < x \times b \qquad [a := 0,\ b := x]$$

$$a = b \wedge c = d \rightarrow a \times c = b \times d$$

$$x \times x = 0 \vee 0 < x \times x$$

Domain Facts

Basic facts **imply** other facts!

$$x \times 0 = 0$$

$$x < 0 \lor x = 0 \lor 0 < x$$

$$x < 0 \land x < 0 \rightarrow x \times 0 < x \times x \qquad [a := x, b := 0]$$

$$0 < x \land 0 < x \rightarrow x \times 0 < x \times x \qquad [a := 0,\ b := x]$$

$$a = b \land c = d \rightarrow a \times c = b \times d \qquad \begin{array}{l}[a := x, b := 0] \\ [c := x,\ d := 0]\end{array}$$

$$x \times x = 0 \lor 0 < x \times x$$

Domain Facts

Basic facts **imply** other facts!

Abstract block to boolean

$$x \times 0 = 0 \qquad \boxed{x = x}$$

$$\boxed{x < 0} \vee \boxed{x = 0} \vee \boxed{0 < x}$$

$$\boxed{x < 0} \wedge \boxed{x < 0} \rightarrow \boxed{x \times 0 < x \times x} \qquad [a := x, b := 0]$$

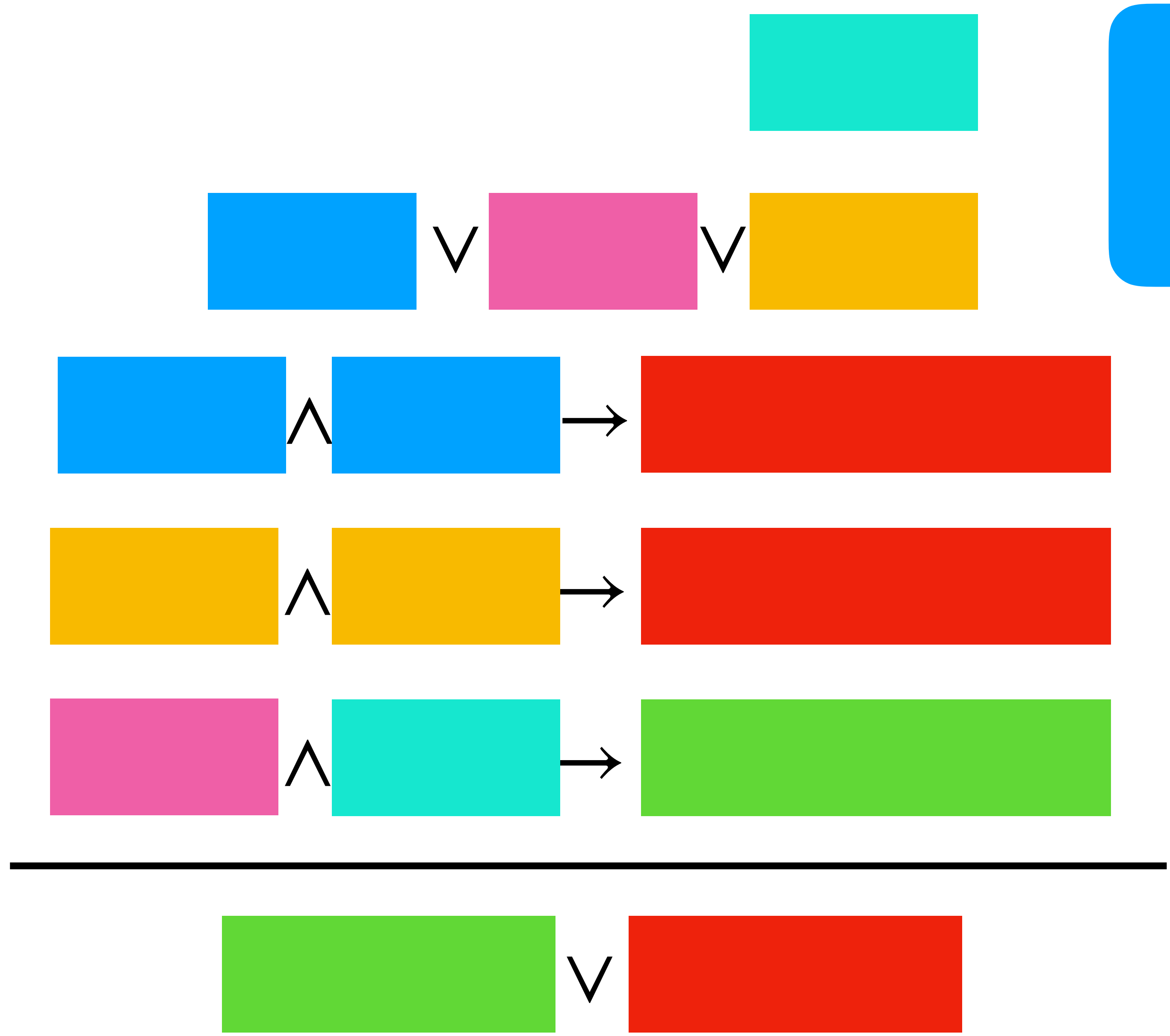
$$\boxed{0 < x} \wedge \boxed{0 < x} \rightarrow \boxed{x \times 0 < x \times x} \qquad [a := 0,\ b := x]$$

$$\boxed{x = 0} \wedge \boxed{x = x} \rightarrow \boxed{x \times x = 0 \times 0} \qquad [a := x, b := 0]\ [c := x,\ d := 0]$$

$$\boxed{x \times x = 0} \vee \boxed{0 < x \times x}$$

Domain Facts

Basic facts **imply** other facts!



Pure boolean expression!

Axioms

Set of basic facts you use **to prove other facts**

$$[\Gamma]\ \underbrace{a_1, a_2, \ldots}_{\textbf{Axioms}} \vdash p$$

Axioms can be **quantified**, with rules:

$$[\Gamma]\ e\ \frac{[\Gamma]\ a[x := e] \vdash p}{[\Gamma]\ \forall x, a \vdash p} \qquad x \notin \Gamma\ \frac{[\Gamma, x]\ a \vdash p}{[\Gamma]\ \exists x, a \vdash p}$$

Example

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\neg a \vee a}\ \textbf{Resolution}}{[x]\ \neg P(x) \vee P(x)}\ \textbf{Abstract out } P(x)}{[x]\ P(x) \rightarrow P(x)}\ \textbf{Definition of } \rightarrow}{[x]\ P(x) \vdash P(x)}\ \textbf{Definition of } \vdash}{[x]\ \forall y, P(y) \vdash P(x)}\ y := x}{[\ ]\ \forall y, P(y) \vdash \forall x, P(x)}\ x \notin [\ ]$$

Summary

	Quantifiers	→ Values for $\exists x$ values
	Boolean logic	→ Proof by resolution
+	**Relations**	→ ???
	Statement	→ **Evidence**

Summary

	Quantifiers	→ Values for $\exists x$ values
	Boolean logic	→ Proof by resolution
	Axioms	→ ???
+	**Relations**	→ Implied by axioms
	Statement	→ **Evidence**

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)

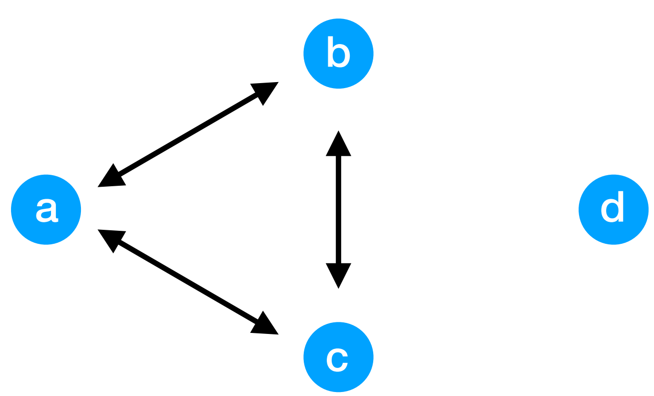
Choosing Axioms

Completeness, incompleteness, and the possible

Example

Reasoning about **nodes** of **this graph**

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



$\textbf{edge}(a, b)$ $\textbf{edge}(b, c)$

$\textbf{edge}(a, c)$ $\neg\textbf{edge}(b, d)$

$\neg\textbf{edge}(a, d)$ $\neg\textbf{edge}(c, d)$

$\forall x, \neg\textbf{edge}(x, x)$ $\forall x, \forall y, \textbf{edge}(x, y) \rightarrow \textbf{edge}(y, x)$

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**?

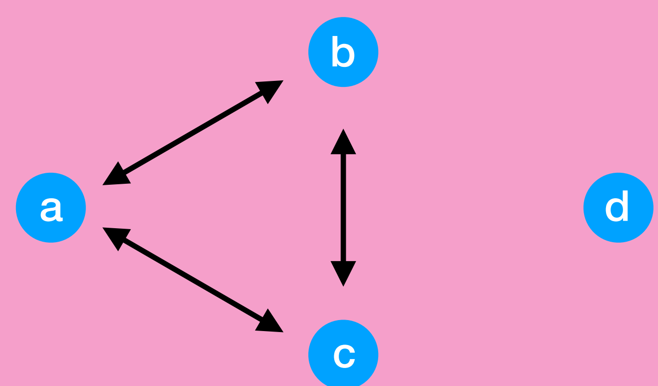
$$\exists x, x \neq x \qquad\qquad \forall y, y = y$$

Now you can **prove false things**!

$$\cfrac{\cfrac{\cfrac{\cfrac{}{a \wedge \neg a \to \bot}\ \textbf{Resolution}}{[x]\ x \neq x, x = x \vdash \bot}\ \textbf{Abstract}\ x = x}{[x]\ x \neq x, (\forall y, y = y) \vdash \bot}\ y := x}{[\,]\ (\exists x, x \neq x), (\forall y, y = y) \vdash \bot}\ x \notin [\,]$$

Missing Axioms

What happens if you have a **missing axiom**?



$\textbf{edge}(a, b)$ $\textbf{edge}(b, c)$

$\textbf{edge}(a, c)$ $\neg\textbf{edge}(b, d)$

$\neg\textbf{edge}(a, d)$ $\neg\textbf{edge}(c, d)$

$\forall x, \neg\textbf{edge}(x, x)$ $\forall x, \forall y, \textbf{edge}(x, y) \rightarrow \textbf{edge}(y, x)$

Now you **can't prove** $\exists x, \exists y, \neg\textbf{edge}(x, y)$

Impossibility

Some things **cannot** be axiomatized well

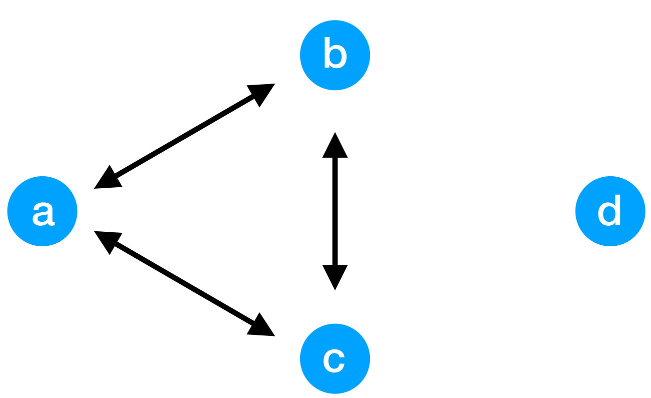
Could you axiomatize **reachability** from graphs?

Relation: $\textbf{path}(x, y)$

path defined via **path**

Axiom: $\forall x, \forall y, \textbf{path}(x, y) \leftrightarrow$

$$x = y \lor \exists z, \textbf{edge}(x, z) \land \textbf{path}(z, y)$$



"infinite path" from a to d

Prove: $\neg\textbf{path}(a, d)$

Whence Axioms

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

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

Equality

Strings

Reals

Integers

Sets

Arrays

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

EQUALITY

IDENTITY

FUNCTION

INTEGERS

INFINITE AXIOMS

ARRAYS

MIXED THEORIES

Next class:

First-order Theories

To do:

- ☐ Course feedback
- ☐ Read / do LogiText
- ☐ Assignment 1 due