

Welcome to 15-317 (Constructive Logic)

- Logistics
  - Course outline
  - Course goals
- 

- Why constructive?

---

- Judgements
- Propositions (briefly)
- Proof Rules
- Conjunction, truth, implication

# Course Outline

I: Proofs as Evidence of Truth

II: Proofs as Programs

III: Proof Search as Computation

IV: Other Logics

---

## Goals

- Understanding Constructive Logic
- Apply Constructive Logic to CS

# Constructivity

- Proofs give effective algorithms

Example/ There exist  $a, b$  irrational s.t.  $a^b$  is rational.

Consider  $\sqrt{2}^{\sqrt{2}}$ . Is this rational?

Case 1: Yes — take  $a = b = \sqrt{2}$ .

Case 2: No — take  $a = \sqrt{2}^{\sqrt{2}}$ ,  $b = \sqrt{2}$ .

Then  $a^b = (\sqrt{2}^{\sqrt{2}})^{\sqrt{2}} = \sqrt{2}^2 = 2$ , which is rational

If  $\sqrt{2}^{\sqrt{2}}$  is rational or  $\sqrt{2}^{\sqrt{2}}$  is irrational, then ...

- $\exists x. A(x)$  must have a witness —  
some specific  $x$  and a proof of  $A(x)$
- A proof of  $A \vee B$  is either a proof of  $A$  or of  $B$
- $A \vee \neg A$  is not necessarily provable.
- A proof of  $A \supset B$  is a function from proofs of  $A$  to proofs of  $B$ .

Example /  $\exists x \left[ \overline{A(x)} \supset \forall y. A(y) \right] \quad ( \text{if } \exists x. \overline{T} )$

Proof (Classical) /

[If  $\forall y. A(y)$ , then choose any  $y$  to be the desired  $x$ .

- [Otherwise  $\exists x. \neg A(x)$ , and this is desired  $x$ .

$\neg \forall y. A(y)$   $\nearrow$

# Judgements

- "Something we can know"
- "Something we can prove"
- Similar, but not the same as propositions.

---

- Separate object language  
(formal objects we study,  
Propositions) from metalanguage

(how we talk about objects)

Main Judgement

A true or "A is true".

Other examples:

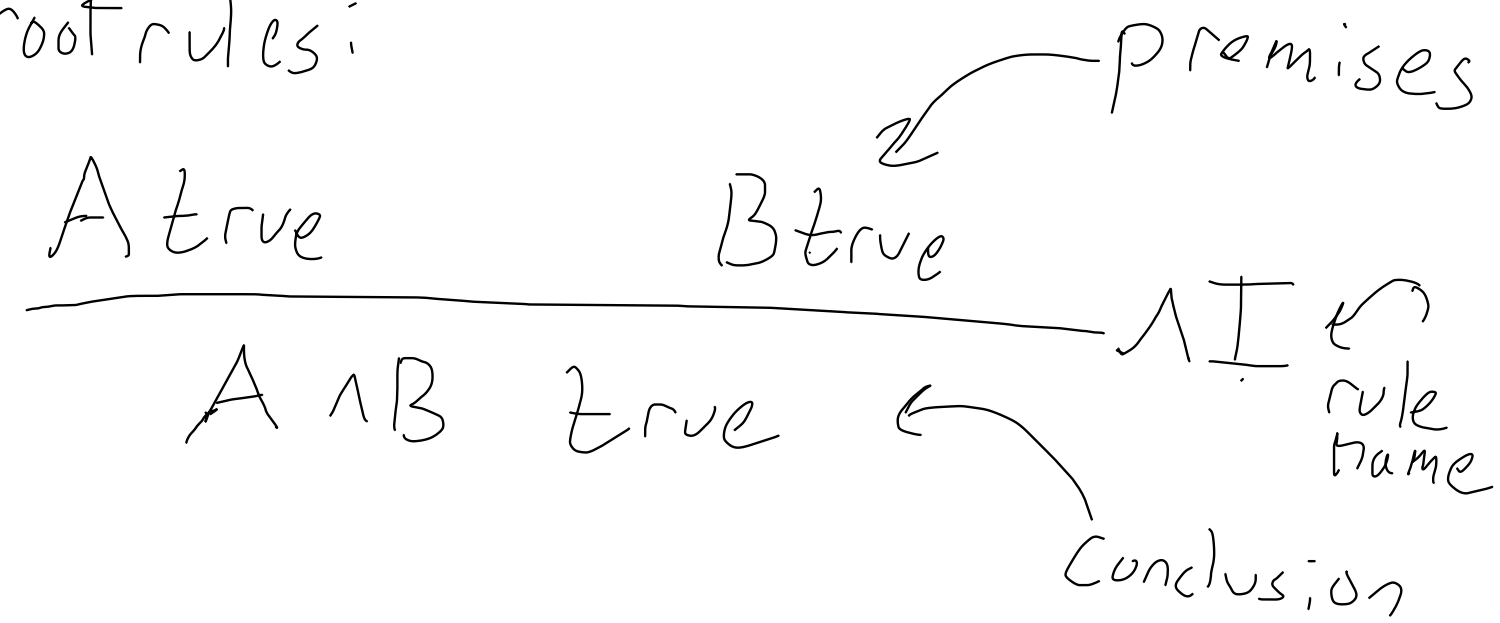
- A false
- A valid
- A true at time  $t$
- $M : \perp$
- A prop

# Proofs

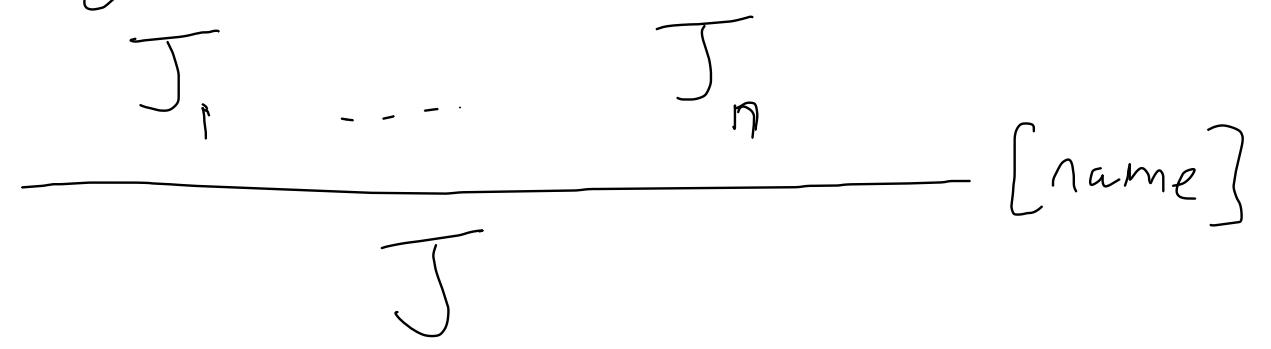
- How do we define what a proposition means?
- Classically - when is the prop. true? (Truth tables)
- Constructively - the meaning of a proposition is defined by its set of proofs\*

- what does  $A \wedge B$  mean?

Proof rules:



In general:



$$\frac{A \wedge B \text{ true}}{A \text{ true}} \wedge E_1, \quad \frac{A \wedge B \text{ true}}{B \text{ true}} \wedge E_2$$

Truth, written T

$$\frac{}{T \text{ true}} \text{TI} \quad \text{No TE rule}$$



$\frac{A \wedge B \text{ true}}{A \text{ true}} \wedge E_1$

Hypothetical Judgement

$J_1, \dots, J_n$

$\vdots$

$J$

"If  $J_1, \dots, J_n$  all hold,  
then so does  $J$ " or

"We can prove  $J$  from  
hypothesis  $J_1, \dots, J_n$ ."

Also written

$J_1, \dots, J_n \vdash J$

# Implication

$\frac{A \text{ true}}{B \text{ true}} \supset I^u$   
 $\frac{}{(A \supset B) \text{ true}} \supset I^u$

~~$\frac{A \text{ true}}{B \text{ true}} \supset I^u$   
 $\frac{}{A \supset B \text{ true}}$~~  Not valid

$\frac{A \text{ true} \quad (A \supset B) \text{ true}}{B \text{ true}} \supset E$

$$\frac{\frac{\overline{A \text{ true}}^u}{A \text{ true}} \quad \frac{\overline{A \text{ true}}^u}{A \text{ true}}}{A \wedge A \text{ true}} \wedge I$$

$$\frac{A \wedge A \text{ true}}{(A \supset (A \wedge A)) \text{ true}} \supset I^u$$

A	B	$A \wedge B$	$B \supset (A \wedge B)$
True	True	True	True
True	False	False	True
False	True	False	True
False	False	False	True

$$\frac{\frac{\frac{A \text{ true} \quad B \text{ true}}{A \wedge B \text{ true}} \wedge I}{B \supset (A \wedge B) \text{ true}} \supset I}{A \supset (B \supset (A \wedge B)) \text{ true}} \supset I^u$$