

# Intro to Interactive Theorem Proving

Joomy Korkut

Wesleyan University

October 5th, 2017

`http://github.com/joom/presentations`

# Why?

- Proofs are too long to write formally!

# Why?

- Proofs are too long to write formally!
- Proofs are too long to check carefully!

# Why?

- Proofs are too long to write formally!
- Proofs are too long to check carefully!
- Seeing what we proved so far helps during the proof process.

# Examples

- Four color theorem (required checking 1,936 cases)  
Appel & Haken 1976 with computer assistance  
Werner & Gonthier 2005 with Coq

- Four color theorem (required checking 1,936 cases)  
Appel & Haken 1976 with computer assistance  
Werner & Gonthier 2005 with Coq
- Kepler conjecture (hexagonal close packing of spheres)  
Hales 1998 with computer assistance (C++ etc.)  
Hales 2014 with HOL Light and Isabelle (Flyspeck)

# How?

- Curry-Howard isomorphism

# How?

- Curry-Howard isomorphism
- Martin-Löf type theory



# Curry-Howard Isomorphism

for simply typed  $\lambda$ -calculus and intuitionistic prop logic,

- Types are propositions!

# Curry-Howard Isomorphism

for simply typed  $\lambda$ -calculus and intuitionistic prop logic,

- Types are propositions!
- Terms are proofs!

# Curry-Howard Isomorphism

for simply typed  $\lambda$ -calculus and intuitionistic prop logic,

- Types are propositions!
- Terms are proofs!

$$\frac{\Gamma, A \vdash B}{\Gamma \vdash A \rightarrow B}$$

# Curry-Howard Isomorphism

for simply typed  $\lambda$ -calculus and intuitionistic prop logic,

- Types are propositions!
- Terms are proofs!

$$\frac{\Gamma, A \vdash B}{\Gamma \vdash A \rightarrow B}$$

$$\frac{\Gamma, x : A \vdash t : B}{\Gamma \vdash \lambda x. t : A \rightarrow B}$$

1

---

<sup>1</sup> $\lambda x. t$  is a different notation for a function  $x \mapsto t$

# Curry-Howard Isomorphism

for simply typed  $\lambda$ -calculus and intuitionistic prop logic,

- Types are propositions!
- Terms are proofs!

$$\frac{\Gamma, A \vdash B}{\Gamma \vdash A \rightarrow B}$$

$$\frac{\Gamma, x : A \vdash t : B}{\Gamma \vdash \lambda x. t : A \rightarrow B}$$

$$\frac{\Gamma \vdash A \quad \Gamma \vdash B}{\Gamma \vdash A \wedge B}$$

---

<sup>1</sup> $\lambda x. t$  is a different notation for a function  $x \mapsto t$

# Curry-Howard Isomorphism

for simply typed  $\lambda$ -calculus and intuitionistic prop logic,

- Types are propositions!
- Terms are proofs!

$$\frac{\Gamma, A \vdash B}{\Gamma \vdash A \rightarrow B}$$

$$\frac{\Gamma \vdash A \quad \Gamma \vdash B}{\Gamma \vdash A \wedge B}$$

$$\frac{\Gamma, x : A \vdash t : B}{\Gamma \vdash \lambda x. t : A \rightarrow B}$$

$$\frac{\Gamma \vdash a : A \quad \Gamma \vdash b : B}{\Gamma \vdash (a, b) : A \times B}$$

1

---

<sup>1</sup> $\lambda x. t$  is a different notation for a function  $x \mapsto t$

# Martin-Löf type theory

- Extension of Curry-Howard to a full intuitionistic logic
- So it allows  $\forall$  and  $\exists$  in your types

- Extension of Curry-Howard to a full intuitionistic logic
- So it allows  $\forall$  and  $\exists$  in your types

## Note

MLTT is constructive, but you can add the law of excluded middle as an axiom and prove classical theorems.



# Some Proof Assistants

- Isabelle (1986) (tactics!)
- Coq (1989) (tactics!)
- Agda (2007)
- Idris (2007) (actually mainly a general purpose language)