# 15-317 Lecture 6: Quantification

- HW2 due today
- HW3 out later today

- Recap on goal of verifications

- Quantifiers/first-order logic
  - Universal $\forall$
  - Existential $\exists$
- Verifications for quantifiers
- Proof terms for quantifiers

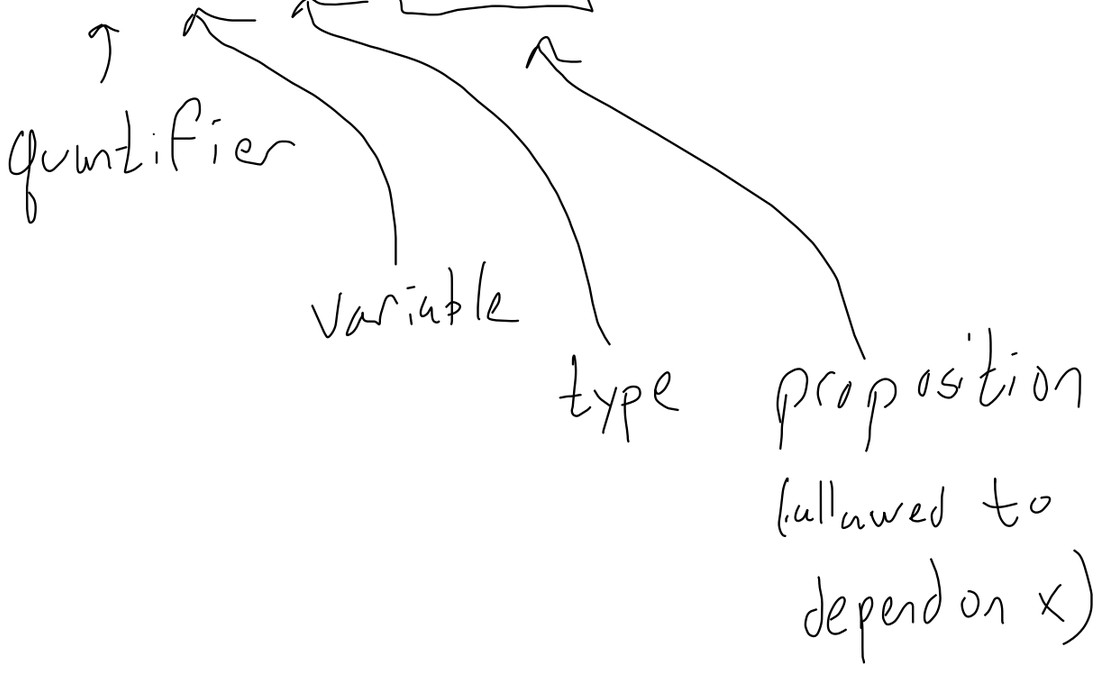
## Recap of Verifications

- Major goal is to simplify proof search
- Restrict available proof rules at any given step
- Fewer choices / less branching
- Very useful for automating proofs

- Easier to show some $A$ true <u>not</u> provable

# Quantifiers

- $\forall x : \Sigma . A(x)$




- $\forall x : \Sigma . A(x) \cong \forall y : \Sigma . A(y)$
  - x is bound by the quantifier

$$\frac{\begin{array}{c}[a : \Sigma] \\ \vdots \\ A(a)\ \text{true}\end{array}}{\forall x : \Sigma .\ A(x)\ \text{true}}\ \forall I^{a}$$

$$\frac{\forall x : \Sigma . A(x)\ \text{true} \qquad t : \Sigma}{A(t)\ \text{true}}\ \forall E$$

# Harmony for $\forall$

- Local reduction

$$\dfrac{\dfrac{\dfrac{}{a : \mathbb{I}}}{\vdots\,\mathcal{D}}}{\dfrac{A(a)\ \mathrm{true}}{\forall x : \mathbb{I}.\, A(x)\ \mathrm{true}}\forall I^{a} \quad \mathcal{E}}\quad \dfrac{}{t : \mathbb{I}}}{A(t)\ \mathrm{true}}\forall E \quad \Longrightarrow_{R} \quad \dfrac{\mathcal{E}}{\dfrac{t : \mathbb{I}}{\vdots\,\mathcal{D}[t/a]}}{A(t)\ \mathrm{true}}$$

# Local expansion for $\forall$

$$\dfrac{\mathcal{D}}{\forall x : \mathbb{Z} . A(x)} \Longrightarrow_E$$

$$\dfrac{\dfrac{\mathcal{D}}{\forall x : \mathbb{Z}\ A(x)\ \text{true}} \qquad \dfrac{}{a : \mathbb{Z}}\,a}{\dfrac{A(a)\ \text{true}}{\forall x : \mathbb{Z} . A(x)\ \text{true}}\,\forall I^a}\,\forall E$$

# Example

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\forall x{:}\Sigma\ B(x,x)\ \text{true}}\,u \qquad \dfrac{}{a:\Sigma}\,a}{B(a,a)\ \text{true}}\,\forall E}{\forall y{:}\Sigma\ B(a,y)\ \text{true?}}\,\forall I^{a}}{\forall x{:}\Sigma.\forall y{:}\Sigma.\ B(x,y)\ \text{true?}}\,\forall I^{a}}{(\forall x{:}\Sigma\ B(x,x)) > (\forall x{:}\Sigma.\forall y{:}\Sigma.\ B(x,y))\ \text{true?}}\,{>}I^{u}$$

Introduces variable $a$ that is already in use

## Existential Quantifier

$$-\exists x{:}\tau.\, A(x)$$

$$\frac{t:\tau \qquad A(t)\ \mathrm{true}}{\exists x{:}\tau.\, A(x)\ \mathrm{true}}\ \exists I$$

$$\frac{\exists x{:}\tau.\, A(x)\ \mathrm{true}}{A(t)\ \mathrm{true}}\ \exists E\ ?$$

$$\frac{\exists x{:}\tau.\, A(x)\ \mathrm{true} \qquad \begin{array}{c}\overline{a:\tau} \quad \overline{A(a)\ \mathrm{true}}^{\,u} \\ \vdots \\ C\ \mathrm{true}\end{array}}{C\ \mathrm{true}}\ \exists E^{a,u}$$

# Harmony for $\exists$

$$\dfrac{\dfrac{\mathcal{D}}{t : \mathbb{I}} \quad \dfrac{\mathcal{E}}{A(t)\ true}}{\exists x{:}\mathbb{I}.\, A(x)\ true}\exists I \qquad \dfrac{\dfrac{}{a : \mathbb{I}}\,a \quad \dfrac{}{A(a)\ true}\,u \quad \vdots\ \mathcal{F}}{C\ true}\exists E^{a,u} \qquad \Longrightarrow_R$$

$$\dfrac{\mathcal{D}}{C\ true}$$

$$\dfrac{\mathcal{D}}{t : \mathbb{I}} \quad \dfrac{\mathcal{E}}{A(t)\ true} \quad \vdots\ \mathcal{F}[t/a, \mathcal{E}/u]$$

$$C\ true$$

$$\dfrac{\mathcal{D}}{\exists x{:}\mathbb{I}.\, A(x)\ true} \qquad \Longrightarrow_E$$

$$\dfrac{\mathcal{D} \qquad \dfrac{}{a : \mathbb{I}}\,a \quad \dfrac{}{A(a)\ true}\,u}{\exists x{:}\mathbb{I}.\, A(x)\ true}\exists I \qquad \dfrac{\exists x{:}\mathbb{I}.\, A(x)\ true \qquad \exists x{:}\mathbb{I}.\, A(x)\ true}{\exists x{:}\mathbb{I}.\, A(x)\ true}\exists E^{a,u}$$

Example

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\forall x{:}\tau.\, A(x) \wedge \exists x{:}\tau.\, \top\ \mathit{true}}\,u}{\exists x{:}\tau.\, \top\ \mathit{true}}\,\wedge E_2 \qquad \dfrac{\dfrac{\dfrac{\dfrac{}{\forall x{:}\tau.\, A(x)\ \mathit{true}}\,\wedge E_1 \qquad \dfrac{}{a : \tau}\,a}{\forall x{:}\tau.\, A(x)\ \mathit{true}}\,\forall E \qquad \dfrac{}{a : \tau}\,a}{A(a)\ \mathit{true}}\,\exists I}{\exists x{:}\tau.\, A(x)\ \mathit{true}}\,\exists E^{a,v}}{\exists x{:}\tau.\, A(x)\ \mathit{true}}\,\supset I^{u}}{(\forall x{:}\tau.\, A(x) \wedge \exists x{:}\tau.\, \top) \supset \exists x{:}\tau.\, A(x)\ \mathit{true}}$$

# Verifications

$$\dfrac{\dfrac{}{a : \Sigma}\quad \vdots \quad A(a)\uparrow}{\forall x{:}\Sigma.\ A(x)\uparrow}\ \forall I^{a}$$

$$\dfrac{t : \Sigma \qquad A(t)\uparrow}{\exists x{:}\Sigma.\ A(x)\uparrow}\ \exists I$$

$$\dfrac{\forall x{:}\Sigma.\ A(x)\downarrow \qquad t : \Sigma}{A(t)\downarrow}\ \forall E$$

$$\dfrac{\exists x{:}\Sigma.\ A(x)\downarrow \qquad \begin{array}{c}\dfrac{}{a : \Sigma}\ a \qquad \dfrac{}{A(a)\downarrow}\ u \\ \vdots \\ C\uparrow\end{array}}{C\uparrow}\ \exists E^{a,u}$$

# Proof terms

$$\dfrac{\dfrac{}{a : \Sigma}\quad \vdots \quad M : A(a)}{(\mathrm{fn}\ a \Rightarrow M) : \forall x{:}\Sigma.\, A(x)}\ \forall I^{a} \qquad \dfrac{M : \forall x{:}\Sigma.\, A(x) \qquad t : \Sigma}{M\ t : A(t)}\ \forall E$$

$$(\mathrm{fn}\ a \Rightarrow M)\ t \Longrightarrow_{R} M[t/a]$$

$$M : \forall x{:}\Sigma.\, A(x) \Longrightarrow_{E} (\mathrm{fn}\ a \Rightarrow M\ a)$$

$$\frac{t : \tau \qquad M : A(t)}{(t, M) : \exists x{:}\tau.\, A(x)}\ \exists I$$

$$\frac{\overline{a : \tau}^{\,a} \qquad \overline{u : A(a)}^{\,u}}{\begin{array}{c}\vdots \\ M : \exists x{:}\tau.\, A(x) \qquad N : C\end{array}}\ \exists E^{a,u}$$
$$\text{let } (a, u) = M \text{ in } N : C$$

$$\text{let } (a, u) = (t, M) \text{ in } N \Longrightarrow_R N[t/a, M/u]$$

$$M \Longrightarrow_E \text{let } (a, u) = M \text{ in } (a, u)$$