Recap from Last Time

- We constructed a datatype in HOL

$$\begin{array}{rcl} \mathsf{trm} & = & \mathsf{Var} : \mathsf{name} \\ & \mid & \mathsf{App} : \mathsf{trm} \times \mathsf{trm} \\ & \mid & \mathsf{Lam} : \langle\!\langle \mathsf{name} \rangle\!\rangle \mathsf{trm} \end{array}$$

  that represents α-equivalence classes.

- We have:

$$\begin{array}{l} \mathsf{Lam}\,[a].x \;=\; \mathsf{Lam}\,[b].y \qquad \text{iff} \\ \quad (a = b \wedge x = y) \vee \\ \quad (a \neq b \wedge x = (a\,b)\bullet y \wedge a \,\#\, y) \end{array}$$

  and

$$\mathsf{supp}(\mathsf{Lam}\,[a].x) = \mathsf{supp}(x) - \{a\}$$

Structural Ind. Principles

$$\frac{\begin{array}{l}\forall a.\ P\,(\mathsf{Var}(a))\,x \\ \forall t_1,t_2.\ (\forall z.\,P\,t_1\,z) \wedge (\forall z.\,P\,t_2\,z) \Rightarrow P\,(\mathsf{App}(t_1,t_2))\,x \\ \forall a.\ a \# x \Rightarrow (\forall t.\ (\forall z.\,P\,t\,z) \Rightarrow P\,(\mathsf{Lam}\,[a].t)\,x)\end{array}}{P\,t\,x}$$

In the nominal datatype-package

- called: $datatype$.induct_unsafe
- applied with:

(nominal_induct $variable(s)$ rule: $ind.\ rule$)

Example (Reflexivity)

- Types

$$\begin{array}{rcl} \mathsf{ty} & = & \mathsf{TVar}(X) \\ & | & \mathsf{Top} \\ & | & T \to S \\ & | & \forall[X : T].S \end{array}$$

- The domain of type-contexts:

$$\begin{array}{rcl} \mathsf{domain}([]) & = & \varnothing \\ \mathsf{domain}(X :: \Gamma) & = & \{\mathsf{fst}(X)\} \cup \mathsf{domain}(\Gamma) \end{array}$$

Example (Reflexivity)

- Closed_in

$$S \text{ closed\_in } \Gamma \stackrel{\text{def}}{=} \text{supp}(S) \subseteq \text{domain}(\Gamma)$$

- Valid typing-contexts

$$\frac{}{\vdash [\,] \text{ ok}}$$

$$\frac{\vdash \Gamma \text{ ok} \qquad X \# \Gamma \qquad T \text{ closed\_in } \Gamma}{\vdash (X, T) :: \Gamma \text{ ok}}$$

Example (Reflexivity)

$$\frac{\vdash \Gamma\ \mathsf{ok} \quad S\ \mathsf{closed\_in}\ \Gamma}{\Gamma \vdash S <: \mathsf{Top}}\ \mathsf{S\_Top}$$

$$\frac{\vdash \Gamma\ \mathsf{ok} \quad X \in \mathsf{domain}(\Gamma)}{\Gamma \vdash \mathsf{TVar}(X) <: \mathsf{TVar}(X)}\ \mathsf{S\_Refl}$$

$$\frac{\Gamma\ \mathsf{ok} \quad (X, S) \in \Gamma \quad \Gamma \vdash S <: T}{\Gamma \vdash \mathsf{TVar}(X) <: T}\ \mathsf{S\_Var}$$

$$\frac{\Gamma \vdash T_1 <: S_1 \quad \Gamma \vdash S_2 <: T_2}{\Gamma \vdash S_1 \to S_2 <: T_1 \to T_2}\ \mathsf{S\_Arrow}$$

$$\frac{\Gamma \vdash T_1 <: S_1 \quad X \# \Gamma \quad (X, T_1) :: \Gamma \vdash S_2 <: T_2}{\Gamma \vdash \forall[X : S_1].S_2 <: \forall[X : T_1].T_2}\ \mathsf{S\_Tall}$$

Example (Reflexivity)

Lemma: $\vdash \Gamma$ ok $\Rightarrow T$ closed_in $\Gamma \Rightarrow \Gamma \vdash T <: T$

Structural Induction on T.

$$\dfrac{\begin{array}{l} \forall x\, X.\ P\,(\mathsf{TVar}(X))\,x \\ \forall x.\ P(\mathsf{Top})\,x \\ \forall x\, T_1\, T_2.\ (\forall z.\, P\, T_1 z) \Rightarrow (\forall z.\, P\, T_2\, z) \\ \qquad\qquad\qquad \Rightarrow P\,(T_1 \rightarrow T_2)\,x \\ \forall x\, X\, T_1\, T_2.\ X \;\#\; x \Rightarrow (\forall z.\, P\, T_1\, z) \Rightarrow (\forall z.\, P\, T_2\, z) \\ \qquad\qquad\qquad\quad \Rightarrow P(\forall[X : T_1].T_2)\,x \end{array}}{P\,T\,x}$$

Example (Reflexivity)

Lemma: $\vdash \Gamma$ ok $\Rightarrow T$ closed_in $\Gamma \Rightarrow \Gamma \vdash T <: T$

Structural Induction on T.

$$\frac{\begin{array}{l} \forall \Gamma\, X.\ P\,(\mathsf{TVar}(X))\,\Gamma \\[1ex] \forall \Gamma.\ P(\mathsf{Top})\,\Gamma \\[1ex] \forall \Gamma\, T_1\, T_2.\ (\forall \Gamma'.\ P\, T_1\, \Gamma') \Rightarrow (\forall \Gamma'.\ P\, T_2\, \Gamma') \\ \qquad\qquad \Rightarrow P\,(T_1 \rightarrow T_2)\,\Gamma \\[1ex] \forall \Gamma\, X\, T_1\, T_2.\ X \# \Gamma \Rightarrow (\forall \Gamma'.\ P\, T_1\, \Gamma') \Rightarrow (\forall \Gamma'.\ P\, T_2\, \Gamma') \\ \qquad\qquad \Rightarrow P(\forall [X : T_1].T_2)\,\Gamma \end{array}}{P\, T\, \Gamma}$$

Example (Reflexivity)

- Interesting case $\forall[X : T_2].T_1$:

We have by induction:

$$\forall\Gamma'.\ \vdash \Gamma' \text{ ok} \Rightarrow T_2 \text{ closed\_in } \Gamma' \Rightarrow \Gamma' \vdash T_2 <: T_2$$
$$\forall\Gamma'.\ \vdash \Gamma' \text{ ok} \Rightarrow T_1 \text{ closed\_in } \Gamma' \Rightarrow \Gamma' \vdash T_1 <: T_1$$
$$X \# \Gamma$$

We have to show:

$$\frac{\vdash \Gamma \text{ ok} \quad (\forall[X : T_2].T_1) \text{ closed\_in } \Gamma}{\Gamma \vdash \forall[X : T_2].T_1 <: \forall[X : T_2].T_1}$$

Example (Reflexivity)

- Interesting case $\forall[X : T_2].T_1$:

We have by induction:

$$\forall\Gamma'.\ \vdash \Gamma' \text{ ok} \Rightarrow T_2 \text{ closed\_in } \Gamma' \Rightarrow \Gamma' \vdash T_2 <: T_2$$
$$\forall\Gamma'.\ \vdash \Gamma' \text{ ok} \Rightarrow T_1 \text{ closed\_in } \Gamma' \Rightarrow \Gamma' \vdash T_1 <: T_1$$
$$X \# \Gamma$$

We have to show:

$$\frac{\vdash \Gamma \text{ ok} \quad (\forall[X : T_2].T_1) \text{ closed\_in } \Gamma}{\Gamma \vdash T_2 <: T_2 \quad X \# \Gamma \quad (X, T_2) :: \Gamma \vdash T_1 <: T_1}$$

Example (Reflexivity)

- Interesting case $\forall[X : T_2].T_1$:

We have by induction:

$$\forall\Gamma'.\ \vdash \Gamma' \text{ ok} \Rightarrow T_2 \text{ closed\_in } \Gamma' \Rightarrow \Gamma' \vdash T_2 <: T_2$$
$$\forall\Gamma'.\ \vdash \Gamma' \text{ ok} \Rightarrow T_1 \text{ closed\_in } \Gamma' \Rightarrow \Gamma' \vdash T_1 <: T_1$$
$$X \# \Gamma$$

We have to show:

$$\frac{\vdash \Gamma \text{ ok} \quad (\forall[X : T_2].T_1) \text{ closed\_in } \Gamma}{\Gamma \vdash T_2 <: T_2 \quad (X, T_2) :: \Gamma \vdash T_1 <: T_1}$$

Example (Reflexivity)

- Interesting case $\forall[X : T_2].T_1$:

We have by induction:

$$\forall\Gamma'.\ \vdash \Gamma' \text{ ok} \Rightarrow T_2 \text{ closed\_in } \Gamma' \Rightarrow \Gamma' \vdash T_2 <: T_2$$
$$\forall\Gamma'.\ \vdash \Gamma' \text{ ok} \Rightarrow T_1 \text{ closed\_in } \Gamma' \Rightarrow \Gamma' \vdash T_1 <: T_1$$
$$X \# \Gamma$$

We have to show:

$$\frac{\vdash \Gamma \text{ ok} \quad \text{supp}(\forall[X : T_2].T_1) \subseteq \text{domain}(\Gamma)}{\Gamma \vdash T_2 <: T_2 \quad (X, T_2) :: \Gamma \vdash T_1 <: T_1}$$

Example (Reflexivity)

- Interesting case $\forall[X : T_2].T_1$:

We have by induction:

$$\forall\Gamma'.\ \vdash \Gamma' \text{ ok} \Rightarrow T_2 \text{ closed\_in } \Gamma' \Rightarrow \Gamma' \vdash T_2 <: T_2$$
$$\forall\Gamma'.\ \vdash \Gamma' \text{ ok} \Rightarrow T_1 \text{ closed\_in } \Gamma' \Rightarrow \Gamma' \vdash T_1 <: T_1$$
$$X \# \Gamma$$

We have to show:

$$\frac{\vdash \Gamma \text{ ok} \quad \text{supp}([X].T_1) \cup \text{supp}(T_2) \subseteq \text{domain}(\Gamma)}{\Gamma \vdash T_2 <: T_2 \quad (X, T_2) :: \Gamma \vdash T_1 <: T_1}$$

Example (Reflexivity)

- Interesting case $\forall[X : T_2].T_1$:

We have by induction:

$$\forall\Gamma'.\ \vdash \Gamma' \text{ ok} \Rightarrow T_2 \text{ closed\_in } \Gamma' \Rightarrow \Gamma' \vdash T_2 <: T_2$$
$$\forall\Gamma'.\ \vdash \Gamma' \text{ ok} \Rightarrow T_1 \text{ closed\_in } \Gamma' \Rightarrow \Gamma' \vdash T_1 <: T_1$$
$$X \# \Gamma$$

We have to show:

$$\frac{\vdash \Gamma \text{ ok} \quad \text{supp}([X].T_1) \subseteq \text{dom}(\Gamma) \quad \text{supp}(T_2) \subseteq \text{dom}(\Gamma)}{\Gamma \vdash T_2 <: T_2 \quad (X, T_2) :: \Gamma \vdash T_1 <: T_1}$$

Example (Reflexivity)

- Interesting case $\forall[X : T_2].T_1$:

We have by induction:

$$\forall\Gamma'.\ \vdash \Gamma' \text{ ok} \Rightarrow T_2 \text{ closed\_in } \Gamma' \Rightarrow \Gamma' \vdash T_2 <: T_2$$
$$\forall\Gamma'.\ \vdash \Gamma' \text{ ok} \Rightarrow T_1 \text{ closed\_in } \Gamma' \Rightarrow \Gamma' \vdash T_1 <: T_1$$
$$X \# \Gamma$$

We have to show:

$$\frac{\vdash \Gamma \text{ ok} \quad \text{supp}([X].T_1) \subseteq \text{dom}(\Gamma) \quad T_2 \text{ closed\_in } \Gamma}{\Gamma \vdash T_2 <: T_2 \quad (X, T_2) :: \Gamma \vdash T_1 <: T_1}$$

Example (Reflexivity)

- Interesting case $\forall[X : T_2].T_1$:

We have by induction:

$$\forall\Gamma'.\ \vdash \Gamma' \text{ ok} \Rightarrow T_2 \text{ closed\_in } \Gamma' \Rightarrow \Gamma' \vdash T_2 <: T_2$$
$$\forall\Gamma'.\ \vdash \Gamma' \text{ ok} \Rightarrow T_1 \text{ closed\_in } \Gamma' \Rightarrow \Gamma' \vdash T_1 <: T_1$$
$$X \# \Gamma$$

We have to show:

$$\frac{\vdash \Gamma \text{ ok} \quad \text{supp}([X].T_1) \subseteq \text{domain}(\Gamma)}{(X, T_2) :: \Gamma \vdash T_1 <: T_1}$$

Example (Reflexivity)

- Interesting case $\forall[X : T_2].T_1$:

We have by induction:

$$\forall\Gamma'.\ \vdash \Gamma' \text{ ok} \Rightarrow T_2 \text{ closed\_in } \Gamma' \Rightarrow \Gamma' \vdash T_2 <: T_2$$
$$\forall\Gamma'.\ \vdash \Gamma' \text{ ok} \Rightarrow T_1 \text{ closed\_in } \Gamma' \Rightarrow \Gamma' \vdash T_1 <: T_1$$
$$X \# \Gamma$$

We have to show:

$$\frac{\vdash \Gamma \text{ ok} \quad \text{supp}(T_1) - \{X\} \subseteq \text{domain}(\Gamma)}{(X, T_2) :: \Gamma \vdash T_1 <: T_1}$$

Example (Reflexivity)

- Interesting case $\forall[X : T_2].T_1$:

We have by induction:

$$\forall\Gamma'.\ \vdash \Gamma' \text{ ok} \Rightarrow T_2 \text{ closed\_in } \Gamma' \Rightarrow \Gamma' \vdash T_2 <: T_2$$
$$\forall\Gamma'.\ \vdash \Gamma' \text{ ok} \Rightarrow T_1 \text{ closed\_in } \Gamma' \Rightarrow \Gamma' \vdash T_1 <: T_1$$
$$X \# \Gamma$$

We have to show:

$$\frac{\vdash \Gamma \text{ ok} \quad \text{supp}(T_1) \subseteq \text{domain}((X,T_2)::\Gamma)}{(X,T_2)::\Gamma \vdash T_1 <: T_1}$$

Example (Reflexivity)

- Interesting case $\forall[X : T_2].T_1$:

We have by induction:

$$\forall\Gamma'.\ \vdash \Gamma' \text{ ok} \Rightarrow T_2 \text{ closed\_in } \Gamma' \Rightarrow \Gamma' \vdash T_2 <: T_2$$
$$\forall\Gamma'.\ \vdash \Gamma' \text{ ok} \Rightarrow T_1 \text{ closed\_in } \Gamma' \Rightarrow \Gamma' \vdash T_1 <: T_1$$
$$X \# \Gamma$$

We have to show:

$$\frac{\vdash \Gamma \text{ ok} \quad T_1 \text{ closed\_in } ((X, T_2) :: \Gamma)}{(X, T_2) :: \Gamma \vdash T_1 <: T_1}$$

Example (Reflexivity)

- Interesting case $\forall[X : T_2].T_1$:

We have by induction:

$$\forall\Gamma'.\ \vdash \Gamma' \text{ ok} \Rightarrow T_2 \text{ closed\_in } \Gamma' \Rightarrow \Gamma' \vdash T_2 <: T_2$$
$$\forall\Gamma'.\ \vdash \Gamma' \text{ ok} \Rightarrow T_1 \text{ closed\_in } \Gamma' \Rightarrow \Gamma' \vdash T_1 <: T_1$$
$$X \# \Gamma$$

We have to show:

$$\frac{\vdash ((X,T_2)::\Gamma) \text{ ok} \quad T_1 \text{ closed\_in } ((X,T_2)::\Gamma)}{(X,T_2)::\Gamma \vdash T_1 <: T_1}$$

Example (Reflexivity)

- Interesting case $\forall[X : T_2].T_1$:

We have by induction:

$\forall\Gamma'.\ \vdash \Gamma'$ ok $\Rightarrow T_2$ closed_in $\Gamma' \Rightarrow \Gamma' \vdash T_2 <: T_2$
$\forall\Gamma'.\ \vdash \Gamma'$ ok $\Rightarrow T_1$ closed_in $\Gamma' \Rightarrow \Gamma' \vdash T_1 <: T_1$
$X \# \Gamma$

We have to show:

Done. :o(

So What?

- These strengthened structural induction principles are crystal clear; they only need to be automated.
- We can do the same for rule inductions (a.k.a. induction over the definition of an inductively defined relation). They are of the form:

$$\frac{\begin{array}{l}\text{as many implications as}\\ \text{there are cases}\\ \vdots\end{array}}{R\,t_1\ldots t_n \Rightarrow P\,t_1\ldots t_n\,x}$$

So What?

- These ... ion princi... need to be ...
- We co... ns (a.k.a. ... an inductively defined relation). They are of the form:

Which conditions need to be satisfied for the strengthening:

- x needs to have finite support
- R needs to be **equivariant**

$$\frac{\begin{array}{l}\text{as many implications as}\\ \text{there are cases}\\ \vdots\end{array}}{R\,t_1\ldots t_n \Rightarrow P\,t_1\ldots t_n\,x}$$

Equivariance

- A relation R is equivariant provided

$$R\, t_1 \ldots t_n \Rightarrow R\,(\pi \bullet t_1) \ldots (\pi \bullet t_n)$$

(If we regard the relation as set, then this means the set is closed under permutations.)

- A function f is equivariant provided

$$\pi \bullet (f\ x) = f(\pi \bullet x)$$

(Strictly speaking one does not need to distinguish functions and relations.)

If we have

- $\pi \bullet \mathsf{True} \stackrel{\mathsf{def}}{=} \mathsf{True}$
- $\pi \bullet \mathsf{False} \stackrel{\mathsf{def}}{=} \mathsf{False}$

then

$$\pi \bullet (R\, t_1 \ldots t_n) = R\, t_1 \ldots t_n$$

and for equivariant relations

$$R\, t_1 \ldots t_n = R\, (\pi \bullet t_1) \ldots (\pi \bullet t_n)$$

- A rela

$$R\, t \qquad\qquad)$$

(If we ... n

this m

permu

- A function f is equivariant provided

$$\pi \bullet (f\ x) = f(\pi \bullet x)$$

(Strictly speaking one does not need to distinguish functions and relations.)

When Do We Have Eqvt?

The following relations and functions can all be shown to be equivariant

- $\Gamma \vdash t : \tau \Rightarrow (\pi \bullet \Gamma) \vdash (\pi \bullet t) : (\pi \bullet \tau)$
- $\pi \bullet \mathsf{domain}(\Gamma) = \mathsf{domain}(\pi \bullet \Gamma)$
- T closed_in $\Gamma \Rightarrow (\pi \bullet T)$ closed_in $(\pi \bullet \Gamma)$
- $\vdash \Gamma$ ok $\Rightarrow \vdash (\pi \bullet \Gamma)$ ok
- $\Gamma \vdash T <: S \Rightarrow (\pi \bullet \Gamma) \vdash (\pi \bullet T) <: (\pi \bullet S)$

A: When the definition has empty support, because. . .

Empty Support

Remember that

$$\text{if } a \# x \text{ and } b \# x \text{ implies } (a\,b)\bullet x = x$$

and

$$\pi\bullet(f\ x) = (\pi\bullet f)(\pi\bullet x)$$

We have

$$(\forall a\,b.\ (a\,b)\bullet x = x) \Leftrightarrow (\forall \pi.\ \pi\bullet x = x)$$

Therefore for f having empty support:

$$\forall \pi.\ \pi\bullet(f\ x) = f(\pi\bullet x)$$

Actually we have that with “if-and-only-if”.

Empty Support

Remember that

if

and

We

(

The

Other direction:

$$
\begin{aligned}
& \mathsf{supp}(f) \\
\stackrel{\text{def}}{=}\ & \{a \mid \mathsf{inf}\{b \mid (a\,b)\bullet f \neq f\}\} \\
=\ & \{a \mid \mathsf{inf}\{b \mid \exists x. ((a\,b)\bullet f)\, x \neq f x\}\} \\
=\ & \{a \mid \mathsf{inf}\{b \mid \exists x. (a\,b)\bullet (f((a\,b)\bullet x)) \neq f x)\}\} \\
=\ & \{a \mid \mathsf{inf}\{b \mid \exists x. f((a\,b)\bullet (a\,b)\bullet x) \neq f x)\}\} \\
=\ & \{a \mid \mathsf{inf}\{b \mid \exists x. f x \neq f x)\}\} \\
=\ & \varnothing
\end{aligned}
$$

$$\forall \pi.\ \pi\bullet(f\ x) = f(\pi\bullet x)$$

Actually we have that with “if-and-only-if”.

When Do We Have Eqvt?

A: When the definition has empty support.

Q: When does a definition have empty support?

A: Provided all the components that built up the definition have empty support.

Unfortunately there is not yet any machine-support for determining when a formula/definition has empty support. We would need to analyse the structure of the formula/definition—probably a decision procedure that works in practise seems possible.

What is Coming Next

- How one can define functions over α-equivalence classes (this is a sore point in the current version of the nominal datatype package).
- More Isar-stuff (if wanted).