Relational parametricity

Previously

Abstraction

$+$

Parametricity

Relational parametricity

We can give precise descriptions of parametricity and abstraction using relations between types.

Definable relations

We define relations between types

$$\rho ::= (x : A, y : B).\phi[x, y]$$

where A and B are System F types, and $\phi[x, y]$ is a logical formula involving x and y.

Definable relations

Logical connectives:

$$\phi ::= \quad \phi \wedge \psi \quad | \quad \phi \vee \psi \quad | \quad \phi \Rightarrow \psi$$

Universal quantifications:

$$\phi ::= \quad \forall x : A.\phi \quad | \quad \forall \alpha.\phi \quad | \quad \forall R \subset A \times B.\phi$$

Existential quantifications:

$$\phi ::= \quad \exists x : A.\phi \quad | \quad \exists \alpha.\phi \quad | \quad \exists R \subset A \times B.\phi$$

Relations:

$$\phi ::= \quad R(t, u)$$

Term equality:

$$\phi ::= \quad (t =_A u)$$

Type substitution

Given:

- type T with free variables $\vec{\alpha} = \alpha_1, \ldots, \alpha_n$
- types $\vec{A} = A_1, \ldots, A_n$

We define the type

$$T[\vec{A}]$$

to be type T with its free variables subtituted by $\vec{A}$.

Relational substitution

Given:

- type T with free variables $\vec{\alpha} = \alpha_1, \ldots, \alpha_n$
- relations $\vec{\rho} = \rho_1 \subset A_1 \times B_1, \ldots, \rho_n \subset A_n \times B_n$

We will define the relation:

$$T[\vec{\rho}] \subset T[\vec{A}] \times T[\vec{B}]$$

Relational substitution: free variables

If T is α_i then

$$T[\vec{\rho}] \quad = \quad \rho_i$$

Relational substitution: products

If T is $T' \times T''$ then

$$\begin{aligned} T[\vec{\rho}] \quad = \quad & (x : T[\overrightarrow{A}],\ y : T[\overrightarrow{B}]). \\ & \quad T'[\vec{\rho}](fst(x),\ fst(y)) \\ & \quad \wedge\ T''[\vec{\rho}](snd(x),\ snd(y)) \end{aligned}$$

Relational substitution: sums

If T is $T' + T''$ then

$$
\begin{array}{rcl}
T[\vec{\rho}] & = & (x : T[\overrightarrow{A}],\ y : T[\overrightarrow{B}]). \\
& & \qquad \exists u' : T'[\overrightarrow{A}].\ \exists v' : T'[\overrightarrow{B}]. \\
& & \qquad\qquad x = inl(u') \ \wedge\ y = inl(v') \\
& & \qquad\qquad \wedge\ T'[\vec{\rho}](u',\, v') \\
& & \vee \\
& & \qquad \exists u'' : T''[\overrightarrow{A}].\ \exists v'' : T''[\overrightarrow{B}]. \\
& & \qquad\qquad x = inr(u'') \ \wedge\ y = inr(v'') \\
& & \qquad\qquad \wedge\ T''[\vec{\rho}](u'',\, v'')
\end{array}
$$

Relational substitution: functions

If T is $T' \to T''$ then

$$
\begin{aligned}
T[\vec{\rho}] \quad = \quad & (f : T[\vec{A}],\ g : T[\vec{B}]). \\
& \quad \forall u : T'[\vec{A}].\, \forall v : T'[\vec{B}]. \\
& \qquad T'[\vec{\rho}](u,\ v) \Rightarrow T''[\vec{\rho}](f\,u,\ g\,v)
\end{aligned}
$$

Relational substitution: univerals

If T is $\forall\beta.T'$ then

$$\begin{array}{rcl} T[\vec{\rho}] & = & (x : T[\overrightarrow{A}],\ y : T[\overrightarrow{B}]). \\ & & \quad \forall\gamma.\ \forall\delta.\ \forall\rho' \subset \gamma \times \delta. \\ & & \qquad T'[\vec{\rho}, \rho'](x[\gamma],\ y[\delta]) \end{array}$$

Relational substitution: existentials

If T is $\exists\beta.T'$ then

$$\begin{array}{rcl} T[\vec{\rho}] & = & (x : T[\overrightarrow{A}],\ y : T[\overrightarrow{B}]). \\ & & \quad \exists\gamma.\ \exists\delta.\ \exists\rho' \subset \gamma \times \delta. \\ & & \qquad \exists u : T'[\overrightarrow{A}, \gamma].\ \exists v : T'[\overrightarrow{B}, \delta]. \\ & & \qquad\quad x = \textsf{pack}\ \gamma,\ u\ \textsf{as}\ T[\overrightarrow{A}] \\ & & \qquad\quad \wedge\ y = \textsf{pack}\ \delta,\ v\ \textsf{as}\ T[\overrightarrow{B}] \\ & & \qquad\quad \wedge\ T'[\vec{\rho}, \rho'](u,\ v) \end{array}$$

Relational substitution: example

System F encoding of lists:

$$\mathsf{List}\ \alpha = \forall\beta.\, \beta \to (\alpha \to \beta \to \beta) \to \beta$$

$$\mathsf{nil}_\alpha = \Lambda\beta.\, \lambda \mathsf{n}:\beta.\, \lambda \mathsf{c}:\alpha \to \beta \to \beta.\ \mathsf{n}$$

$$\begin{aligned}\mathsf{cons}_\alpha = {} & \lambda \mathsf{x}:\alpha.\, \lambda \mathsf{xs}:\mathsf{List}\ \alpha.\\ & \Lambda\beta.\, \lambda \mathsf{n}:\beta.\, \lambda \mathsf{c}:\alpha \to \beta \to \beta.\\ & \quad \mathsf{c}\ \mathsf{x}\ (\mathsf{xs}\ [\beta]\ \mathsf{n}\ \mathsf{c})\end{aligned}$$

Relational substitution: example

Given a relation $\rho \subset A \times B$:

$$
\begin{aligned}
&(\mathsf{List}\,\alpha)[\rho] = \\
&\qquad (x : ListA,\ y : ListB). \\
&\qquad\qquad \forall\gamma.\ \forall\delta.\ \forall\rho' \subset \gamma \times \delta. \\
&\qquad\qquad\qquad (\beta \to (\alpha \to \beta \to \beta) \to \beta)[\rho, \rho'](x[\gamma],\ y[\delta])
\end{aligned}
$$

Relational substitution: example

Given a relation $\rho \subset A \times B$:

$$
\begin{aligned}
&(\mathsf{List}\,\alpha)[\rho] = \\
&\quad (x : ListA,\ y : ListB). \\
&\qquad \forall\gamma.\ \forall\delta.\ \forall\rho' \subset \gamma \times \delta. \\
&\qquad\quad \forall n : \gamma.\ \forall m : \delta. \\
&\qquad\quad\ \forall c : A \to \gamma \to \gamma.\ \forall d : B \to \delta \to \delta. \\
&\qquad\qquad \rho'(n,\ m) \Rightarrow \\
&\qquad\qquad\quad (\forall a : A.\ \forall b : B.\ \forall u : \gamma.\ \forall v : \delta. \\
&\qquad\qquad\qquad \rho(a, b) \Rightarrow \rho'(u, v) \Rightarrow \rho'(c\,a\,u,\ d\,b\,v)) \Rightarrow \\
&\qquad\qquad\qquad\quad \rho'(x[\gamma]\,n\,c,\ y[\delta]\,m\,d)
\end{aligned}
$$

Relational substitution: example

If $x = nil_A$ and $y = nil_B$:

$$\begin{array}{l}
\forall\gamma.\ \forall\delta.\ \forall\rho' \subset \gamma \times \delta. \\
\quad \forall n : \gamma.\ \forall m : \delta. \\
\quad \forall c : A \to \gamma \to \gamma.\ \forall d : B \to \delta \to \delta. \\
\quad \forall a : A.\forall u : \gamma.\ \forall b : B.\forall v : \gamma. \\
\qquad \rho'(n,\ m) \Rightarrow \\
\qquad\quad (\forall a : A.\ \forall b : B.\ \forall u : \gamma.\ \forall v : \delta. \\
\qquad\qquad \rho(a, b) \Rightarrow \rho'(u, v) \Rightarrow \rho'(c\,a\,u,\ d\,b\,v)) \Rightarrow \\
\qquad\qquad\quad \rho'(nil_A[\gamma]\,n\,c,\ nil_B[\delta]\,m\,d)
\end{array}$$

Relational substitution: example

If $x = nil_A$ and $y = nil_B$:

$$\begin{array}{l} \forall\gamma.\ \forall\delta.\ \forall\rho' \subset \gamma \times \delta. \\ \quad \forall n : \gamma.\ \forall m : \delta. \\ \quad \forall c : A \to \gamma \to \gamma.\ \forall d : B \to \delta \to \delta. \\ \quad \forall a : A. \forall u : \gamma.\ \forall b : B. \forall v : \gamma. \\ \qquad \rho'(n,\ m) \Rightarrow \\ \qquad\quad (\forall a : A.\ \forall b : B.\ \forall u : \gamma.\ \forall v : \delta. \\ \qquad\qquad \rho(a, b) \Rightarrow \rho'(u, v) \Rightarrow \rho'(c\,a\,u,\ d\,b\,v)) \Rightarrow \\ \qquad\qquad\quad \rho'(n,\ m) \end{array}$$

Relational substitution: example

If $x = cons_A\, i\, l$ and $y = cons_B\, j\, k$:

$$
\begin{array}{l}
\forall \gamma.\ \forall \delta.\ \forall \rho' \subset \gamma \times \delta. \\
\quad \forall n : \gamma.\ \forall m : \delta. \\
\quad\ \forall c : A \to \gamma \to \gamma.\ \forall d : B \to \delta \to \delta. \\
\qquad \rho'(n,\ m) \Rightarrow \\
\qquad\quad (\forall a : A.\ \forall b : B.\ \forall u : \gamma.\ \forall v : \delta. \\
\qquad\qquad \rho(a, b) \Rightarrow \rho'(u, v) \Rightarrow \rho'(c\, a\, u,\ d\, b\, v)) \Rightarrow \\
\qquad\qquad\ \rho'(cons_A[\gamma]\, i\, l\, n\, c,\ cons_B[\delta]\, j\, k\, m\, d)
\end{array}
$$

Relational substitution: example

If $x = cons_A\, i\, l$ and $y = cons_B\, j\, k$:

$$
\begin{array}{l}
\forall\gamma.\ \forall\delta.\ \forall\rho' \subset \gamma\times\delta. \\
\quad \forall n : \gamma.\ \forall m : \delta. \\
\quad \forall c : A \to \gamma \to \gamma.\ \forall d : B \to \delta \to \delta. \\
\quad\quad \rho'(n,\, m) \Rightarrow \\
\quad\quad\quad (\forall a : A.\ \forall b : B.\ \forall u : \gamma.\ \forall v : \delta. \\
\quad\quad\quad\quad \rho(a, b) \Rightarrow \rho'(u, v) \Rightarrow \rho'(c\, a\, u,\, d\, b\, v)) \Rightarrow \\
\quad\quad\quad\quad\quad \rho'(c\, i\, (l[\gamma]\, n\, c),\, d\, j\, (k[\gamma]\, m\, d))
\end{array}
$$

Relational substitution: example

If $x = cons_A\, i\, l$ and $y = cons_B\, j\, k$:

$$\begin{array}{l}
\forall\gamma.\ \forall\delta.\ \forall\rho' \subset \gamma \times \delta. \\
\quad \forall n : \gamma.\ \forall m : \delta. \\
\quad\ \forall c : A \to \gamma \to \gamma.\ \forall d : B \to \delta \to \delta. \\
\qquad \rho'(n,\ m) \Rightarrow \\
\qquad\quad (\forall a : A.\ \forall b : B.\ \forall u : \gamma.\ \forall v : \delta. \\
\qquad\qquad \rho(a, b) \Rightarrow \rho'(u, v) \Rightarrow \rho'(c\, a\, u,\ d\, b\, v)) \Rightarrow \\
\qquad\qquad\ \rho(i, j)\ \wedge\ \rho'(l[\gamma]\, n\, c,\ k[\gamma]\, m\, d)
\end{array}$$

Relational substitution: example

If $x = cons_A \, i \, l$ and $y = cons_B \, j \, k$:

$$\rho(i,j) \;\wedge\; (\mathsf{List}\,\alpha)[\rho](l,k)$$

Relational substitution: example

It can be shown that $(\mathsf{List}\,\alpha)[\rho](x, y)$ holds iff x and y have the same length and corresponding elements are related.

Preservation of relations

Given a type T with free variables $\alpha, \beta_1, \ldots, \beta_n$:

$$\begin{aligned} &\forall \beta_1. \ldots \forall \beta_n. \forall x : (\forall \alpha. T). \\ &\quad \forall \gamma.\ \forall \delta.\ \forall \rho \subset \gamma \times \delta. \\ &\quad\quad T[\rho, =_{\beta_1}, \ldots, =_{\beta_n}](x[\gamma],\ x[\delta]) \end{aligned}$$

Preservation of relations

Ignoring free variables:

$$\begin{aligned}&\forall x : (\forall \alpha . T).\\ &\qquad \forall \gamma.\ \forall \delta.\ \forall \rho \subset \gamma \times \delta.\\ &\qquad\qquad T[\rho](x[\gamma],\ x[\delta])\end{aligned}$$

Preservation of relations

Any value with a universal type must preserve all type relations between any two types that it can be instantiated with.

Theorems for free

Theorems for free

Parametricity applied to $\forall\alpha.\alpha \to \alpha$:

$$\begin{aligned}
&\forall f : (\forall\alpha.\alpha \to \alpha).\\
&\qquad \forall\gamma.\ \forall\delta.\ \forall\rho \subset \gamma \times \delta.\\
&\qquad\qquad \forall u : \gamma.\ \forall v : \delta.\\
&\qquad\qquad\qquad \rho(u,\ v) \Rightarrow \rho(f[\gamma]\,u,\ f[\delta]\,v)
\end{aligned}$$

Theorems for free

Define a relation is_u to represent being equal to a value $u : T$:

$$\mathsf{is}_u(x : T, y : T) \quad = \quad (x =_T u) \wedge (y =_T u)$$

Theorems for free

$$\begin{aligned} &\forall f : (\forall \alpha . \alpha \to \alpha). \\ &\qquad \forall \gamma . \forall u : \gamma . \\ &\qquad\qquad \mathsf{is}_u(u, u) \Rightarrow \mathsf{is}_u(f[\gamma]\, u,\ f[\gamma]\, u) \end{aligned}$$

Theorems for free

$$
\begin{aligned}
&\forall f : (\forall \alpha . \alpha \to \alpha). \\
&\quad \forall \gamma . \forall u : \gamma . \\
&\qquad f[\gamma]\, u \; =_{\gamma} u
\end{aligned}
$$

Theorems for free

Parametricity applied to $\forall\alpha.\mathsf{List}\,\alpha \to \mathsf{List}\,\alpha$:

$$\begin{aligned}
&\forall f : (\forall\alpha.\mathsf{List}\,\alpha \to \mathsf{List}\,\alpha).\\
&\quad \forall\gamma.\ \forall\delta.\ \forall\rho \subset \gamma \times \delta.\\
&\qquad \forall u : \mathsf{List}\,\gamma.\ \forall v : \mathsf{List}\,\delta.\\
&\qquad\quad (\mathsf{List}\,\alpha)[\rho](u,\ v) \Rightarrow (\mathsf{List}\,\alpha)[\rho](f[\gamma]\,u,\ f[\delta]\,v)
\end{aligned}$$

Theorems for free

Define a relation $\langle g \rangle$ to represent a function $g : A \to B$

$$\langle g \rangle (x : A, y : B) \quad = \quad (g\, x =_B y)$$

Note that

$$(\mathsf{List}\, \alpha)[\langle g \rangle](xs : List\, A, ys : List\, B) \;=\; (\mathsf{map}\, g\, xs =_{List\ B} ys)$$

Theorems for free

$$
\begin{aligned}
&\forall f : (\forall \alpha. \mathsf{List}\, \alpha \to \mathsf{List}\, \alpha). \\
&\quad \forall \gamma.\ \forall \delta.\ \forall g : \gamma \to \delta \\
&\quad\quad \forall u : \mathsf{List}\, \gamma.\ \forall v : \mathsf{List}\, \delta. \\
&\quad\quad\quad (\mathsf{List}\, \alpha)[\langle g \rangle](u,\ v) \Rightarrow (\mathsf{List}\, \alpha)[\langle g \rangle](f[\gamma]\, u,\ f[\delta]\, v)
\end{aligned}
$$

Theorems for free

$$\begin{aligned}
&\forall f : (\forall \alpha . \mathsf{List}\, \alpha \to \mathsf{List}\, \alpha). \\
&\quad \forall \gamma.\ \forall \delta.\ \forall g : \gamma \to \delta \\
&\qquad \forall u : \mathsf{List}\, \gamma.\ \forall v : \mathsf{List}\, \delta. \\
&\qquad\quad (\mathsf{map}\, g\, u = v) \Rightarrow (\mathsf{map}\, g\, (f[\gamma]\, u) = f[\delta]\, v)
\end{aligned}$$

Theorems for free

$$\begin{aligned}
&\forall f : (\forall \alpha. \mathsf{List}\,\alpha \to \mathsf{List}\,\alpha). \\
&\quad \forall \gamma.\ \forall \delta.\ \forall g : \gamma \to \delta \\
&\qquad \forall u : \mathsf{List}\,\gamma.\ \forall v : \mathsf{List}\,\delta. \\
&\qquad\quad \mathsf{map}\,g\,(f[\gamma]\,u) = f[\delta]\,(\mathsf{map}\,g\,u)
\end{aligned}$$

Terms and conditions apply

Terms and conditions apply

```
let f (x : 'a) : 'a =
  Printf.printf "Lanch missiles\n";
  x

let f (x : 'a) : 'a = raise Exit

let rec f (x : 'a) : 'a = f x
```

Terms and conditions apply

Parametricity applied to $\forall\alpha.\alpha \to \alpha \to \mathsf{Bool}$:

$$
\begin{aligned}
&\forall f : (\forall\alpha.\alpha \to \alpha \to \mathsf{Bool}).\\
&\quad \forall\gamma.\ \forall\delta.\ \forall\rho \subset \gamma \times \delta.\\
&\qquad \forall u : \gamma.\ \forall v : \delta.\ \forall u' : \gamma.\ \forall v' : \delta.\\
&\qquad\quad \rho(u,\ v) \Rightarrow \rho(u',\ v') \Rightarrow\\
&\qquad\qquad Bool[\rho](f[\gamma]\,u\,u',\ f[\delta]\,v\,v')
\end{aligned}
$$

Terms and conditions apply

Parametricity applied to $\forall\alpha.\alpha \to \alpha \to \text{Bool}$:

$$
\begin{aligned}
&\forall f : (\forall\alpha.\alpha \to \alpha \to \text{Bool}).\\
&\quad \forall\gamma.\ \forall\delta.\ \forall\rho \subset \gamma \times \delta.\\
&\quad\quad \forall u : \gamma.\ \forall v : \delta.\ \forall u' : \gamma.\ \forall v' : \delta.\\
&\quad\quad\quad \rho(u,\ v) \Rightarrow \rho(u',\ v') \Rightarrow\\
&\quad\quad\quad\quad (f[\gamma]\, u\, u' =_{Bool} f[\delta]\, v\, v')
\end{aligned}
$$

Terms and conditions apply

$$\begin{aligned}
&\forall f : (\forall \alpha. \alpha \to \alpha \to \mathsf{Bool}).\\
&\quad \forall \gamma.\ \forall \delta.\\
&\qquad \forall u : \gamma.\ \forall v : \delta.\ \forall u' : \gamma.\ \forall v' : \delta.\\
&\qquad\quad (f[\gamma]\, u\, u' =_{Bool} f[\delta]\, v\, v')
\end{aligned}$$

Terms and conditions apply

```
val (=) : 'a -> 'a -> bool
```