A logic for parametric polymorphism

Gordon Plotkin & Martin Abadi

System F

Types $A ::= X \mid A \to A \mid \forall X.A$

Terms $t ::= x \mid \lambda x{:}A.t \mid tt \mid \Lambda X.t \mid tA$

Formulae $\varphi ::= t =_A t \mid R(t,t) \mid \varphi \supset \varphi \mid \forall x{:}A.\varphi \mid \forall X.\varphi \mid \forall R \subset A \times A.\varphi$

R ranges over relation variables. $R \subset A \times B$ means R is a relation between A and B.

In System F types of terms are unique, so often subscript of equality is omitted.

Other usefull constructs for formulae:

$\bot \mid \neg\varphi \mid \varphi \wedge \varphi \mid \varphi \vee \varphi \mid \exists x{:}A.\varphi \mid \exists X.\varphi \mid \exists R \subseteq A \times A.\varphi$

Environments:

$\Delta ::= \cdot \mid \Delta, X$ } becomes $E ::= \cdot \mid E, X \mid E, x{:}A$

$\Gamma ::= \cdot \mid \Gamma, x{:}A$ } normal rules for $E \vdash A$, $E \vdash *{:}A$

$G ::= \cdot \mid G, R \subset A \times A$ $\quad E \vdash G$ means $E \vdash A$ and $E \vdash B$ for all $R \subseteq A \times B \in G$

$E; G \vdash \varphi$ well-formedness.

Definable relations $\rho ::= (x{:}A, y{:}B).\varphi(x,y)$

Examples:
- $eq_A = (x{:}A, y{:}A).\ x =_A y$
- $\langle f \rangle = (x{:}A, y{:}B).\ fx =_B y$ (for $f{:}A \to B$)
- $R = (x{:}A, y{:}B).\ R(x,y)$ (for $R \subset A \times B$)

Notation: If $\rho = (x{:}A, y{:}B).\varphi(x,y)$ and $t \in A$, $u{:}B$ then $t\,\rho\,u$ or $\rho(t,u)$ denotes $\varphi[t/x, u/y]$

We can substitute definable relations for relation variables in formulae as expected. Needed for rules relational quantification.

Substitution in types needed for parametricity schema

- $X[\rho/X] = \rho$, $Y[\rho/X] = Y$
- $(A \to B)[\rho] = A[\rho] \to B[\rho]$
- $(\forall X.A)[\rho] = \forall Y,Z,R \subset Y \times Z.\ A[\rho/X, R/X']$

Where given $\rho_1 \subset A_1 \times B_1$ and $\rho_2 \subset A_2 \times B_2$ the relation $\rho_1 \to \rho_2 \subset (A_1 \to A_2) \times (B_1 \to B_2)$ is defined by

$f(\rho_1 \to \rho_2)g \equiv \forall x{:}A_1, y{:}B_1.\ x\rho_1 y \supset fx\ \rho_2\ gy$

and given $\rho : A \times B$ the relation $\forall Y,Z,R \in Y \times Z.\ \rho \subset \forall Y.A \times \forall Z.B$ is defined by

$y(\forall Y,Z,R \subset Y \times Z.\ \rho)z \equiv \forall Y,Z,R \subset Y \times Z.\ (yY)\rho(zZ)$

Defining rules for $\Gamma \vdash_{E;G} \varphi$, where Γ is a finite set of formulae and all formulae are well-formed w.r.t. $E;G$

Standard ND rules for connectives and quantifiers:

$$\frac{}{\Gamma \vdash \varphi}\ \varphi \in \Gamma \qquad \frac{\Gamma, \varphi \vdash \psi}{\Gamma \vdash \varphi \supset \psi} \qquad \frac{\Gamma \vdash \varphi \supset \psi \quad \Gamma \vdash \varphi}{\Gamma \vdash \psi}$$

$$\frac{\Gamma \vdash_{E,X;G} \varphi[X]}{\Gamma \vdash_{E;G} \forall X.\varphi[X]}\ X \text{ not in } \Gamma \qquad \frac{\Gamma \vdash_{E;G} \forall R \subset A \times B.\ \varphi(R) \quad E;G \vdash \rho \subset A \times B}{\Gamma \vdash_{E;G} \varphi[\rho]}$$

rules for equational part of System F:

reflexivity: $\Gamma \vdash \forall X \forall x{:}X.\ x =_X x$

substitution: $\Gamma \vdash \forall X,Y,R \subset X \times Y, x{:}X, x'{:}X, y{:}Y, y'{:}Y.\ (R(x,y) \wedge x =_X x' \wedge y =_Y y') \supset R(x',y')$

Congruence schema's: $(t{:}B, u{:}B)$

$$\frac{\Gamma \vdash \forall x{:}A.\ t =_B u}{\Gamma \vdash \lambda x{:}A.t =_{A \to B} \lambda x{:}A.u} \qquad \frac{\Gamma \vdash \forall X.\ t =_B u}{\Gamma \vdash \Lambda X.t =_{\forall X.B} \Lambda X.u}$$

β-equalities: $\Gamma \vdash \forall x{:}A.(\lambda x{:}A.t)x =_\beta t$ $\quad \forall X.(\Lambda X.t)X =_\beta t$

η-equalities: $\Gamma \vdash \forall X,Y,f{:}X\to Y.\ \lambda x{:}X.fx = f$

$\Gamma \vdash \forall X, f{:}(\forall X.A).\ \Lambda X.fX = f$

Parametricity schema:

$\Gamma \vdash \forall Y_1,\dots,Y_n, x{:}(\forall X.A[X,Y_1,\dots,Y_n]).\ x(\forall X.A[X, eq_{Y_1},\dots,eq_{Y_n}])x$

$\Gamma \vdash \forall x{:}(\forall X.A[X]).\ \forall Y,Z,R\subset Y\times Z.\ (xY)A[R](xZ)$

"Instantiating an element of a polymorphic type (x) at two "related" types (Y, Z, related by R), results in two related elements."

Example: $I : \forall X.\ X\to X$

parametricity says for any types A and B and relation $R \subset A\times B$ we have $(IA)(R\to R)(IB)$

$\Rightarrow \forall x{:}A, y{:}B\ (xRy \supset I_{A\times R} I_B xy)$

Identity Extension lemma:

For any type $A(X_1,\dots,X_n)$ it is provable in APL that

$\forall X_1,\dots,X_n, x{:}A(X_1,\dots,X_n), y{:}A(X_1,\dots,X_n).\ xA[eq_{X_1},\dots eq_{X_n}]y \equiv (x = y)$

Logical Relations lemma:

For any $A_1(X),\dots,A_n(X), B(X)$. If $X, a_1{:}A_1(X),\dots,a_n{:}A_n(X) \vdash t{:}B(X)$ then it is provable in APL without parametricity that

$\forall X,Y,R\subset X\times Y,\ x_1{:}A_1(X),\dots,x_n{:}A_n(X), y_1{:}A_1(Y),\dots,y_n{:}A_n(Y).$

$x_1 A_1[R]y_1 \wedge \dots \wedge x_n A_n[R]y_n \supset t(x_1,\dots,x_n)\ B[R]\ t(y_1,\dots,y_n).$

Proof by induction on A:

$A = X$.

$$x =_X y \vdash x =_X y$$
$$\vdash x =_X y \supset x =_X y$$
$$\vdash x =_{XY} y \cong x =_X y \quad \text{def } eq_X$$
$$\vdash x\ eq_X\ y \equiv x =_X y$$
$$\vdash x\ X[eq_X]\ y \equiv x =_X y$$
$$\vdash \forall X, x{:}X, y{:}X.\ x\ X[eq_X]\ y \equiv x =_X y$$

$A = B \to C$:

refl, refl

subst. $\Gamma \vdash (fx) =_C (fx)$ $\quad \Gamma \vdash f =_A f$ $\quad \Gamma \vdash f =_A g$ $\quad$ refl $\quad$ refl $\quad \Gamma \vdash x\ B[eq_X]\ y$ IH

subst $\quad \Gamma \vdash (fx) =_C (gx)$ $\quad \Gamma \vdash x =_B x$ $\quad \Gamma \vdash x =_B y$

$\Gamma \vdash (fx) =_C (gy)$ IH

$f =_A g,\ x\ B[eq_X]\ y \vdash (fx)\ C[eq_X]\ (gy)$

$f =_A g \vdash x\ B[eq_X]\ y \supset (fx)\ C[eq_X]\ (gy)$

$\Gamma = f{=}g,\ x\ B[eq]\ y$

$\varphi = \forall x{:}B\, y{:}C.\ x\ B[eq]\ y \supset fx\ C[eq]\ gy$

IH = induction hypothesis

$\varphi \vdash \varphi$ $\quad$ refl $\quad \varphi \vdash x =_B x$ IH

$\varphi \vdash x\ B[eq_X]\ x \supset (fx)\ C[eq_X]\ (gx)$ $\quad \varphi \vdash x\ B[eq_X]\ x$

$\varphi \vdash (fx)\ C[eq_X]\ (gx)$ IH

$\varphi \vdash \forall x{:}B.\ (fx)\ C[eq_X]\ (gx)$

$\varphi \vdash fx =_C gx$ $\quad$ η-eq $\quad$ η-eq

subst $\quad \varphi \vdash \lambda x.fx =_A \lambda x.gx$ $\quad \varphi \vdash \lambda x.fx =_B f$ $\quad \varphi \vdash \lambda x.gx =_B g$

$\varphi \vdash f =_A g$

$$\vdash \forall x{:}B, y{:}C.\ x\ B[eq_X]\ y \supset (fx)\ C[eq_X]\ (gy) \equiv f =_A g$$
$$\vdash f\ (B[eq_X] \to C[eq_X])\ g \equiv f =_A g$$
$$\vdash f\ A[eq_X]\ g \equiv f =_A g$$
$$\vdash \forall X.\ f, g{:}A(X).\ f\ A[eq_X]\ g \equiv f =_A g$$

$A = \forall X.B$

$\varphi \vdash \varphi$

$\varphi \vdash \forall R \subset Z \times Z.\ (xz)\ B[eq_X, R]\ (yz)$ $\quad \varphi = \forall Z, Z', R \subset Z \times Z'.\ xz\ B[eq_X R]\ yZ'$

$\varphi \vdash (xz)\ B[eq_X, eq_Y]\ (yz)$ IH $\quad$ param. $\quad$ refl.

$\varphi \vdash xz =_B yz$ $\quad$ subst. $x=y \vdash (xz)\ B[eq_X, R]\ (yz')_{x=y \vdash x=x}$ $\quad x=y \vdash x=y$

$\varphi \vdash \forall z.\ xz =_B yz$ $\quad$ η-eq $\quad$ η-eq

subst $\quad \varphi \vdash \Lambda z.xz =_A \Lambda z.yz$ $\quad \varphi \vdash \Lambda z.xz =_B x$ $\quad \varphi \vdash \Lambda z.yz =_A y$ $\quad x =_A y \vdash (xz)\ B[eq_X R]\ (yz')$

$\varphi \vdash x =_A y$ $\quad x =_A y \vdash \varphi$

$$\vdash (\forall z, z', R \subset z \times z'.\ (xz)\ B[eq_X, R]\ (yz')) \equiv x =_A y$$
$$\vdash x\ A[eq_X]\ y \equiv x =_A y$$
$$\forall X, x{:}A(X), y{:}A(X).\ x\ A[eq_X]\ y \equiv x =_A y$$