SOLVING TRANSFORMATION

Alessandro Coglio

Kestrel Institute

Problem Specification

$$S(f) \triangleq [\forall x.\, R(x, f(x))]$$

$S \subseteq \mathcal{U} \to \mathcal{U}$ — specification for f — S is 2nd order

$R \subseteq \mathcal{U} \times \mathcal{U}$ — input/output relation

example: $R(x,y) \triangleq [\varphi(x) \Rightarrow \psi(x,y)]$ — φ pre-condition, ψ post-condition

this form of S captures requirements on single runs of f;
richer forms can capture requirements on multiple runs (hyperproperties, e.g. noninterference)

generalizes to n inputs and m outputs:

$S(f) \triangleq [\forall \bar{x}.\, R(\bar{x}, f(\bar{x}))]$ $\qquad S \subseteq \mathcal{U}^n \to \mathcal{U}^m \qquad R \subseteq \mathcal{U}^n \times \mathcal{U}^m$

this is more general than solving; it could be moved to separate notes

Solution by Rewriting to True

$$R(x, f(x)) \xrightarrow{\text{rewriting}} \top$$

$$\Downarrow$$

$\boxed{RW}\ \vdash \forall f, x.\ R(x, f(x))$ — proved by rewriter

$f_0(x) \triangleq \dots$ — anything

$S'(f) \triangleq [f = f_0]$

$\boxed{SS'}\ \vdash S'(f) \Rightarrow S(f)$ — proof does not use δ_{f_0}

$$\begin{tikzcd}
S'(f) \arrow[r, "\delta_{S'}"] & f = f_0 \arrow[dr] & & \\
 & & \forall x.\ R(x, f(x)) \arrow[r, "\delta_S"] & S(f) \\
RW \arrow[r, "f := f_0"'] & \forall x.\ R(x, f_0(x)) \arrow[ur] & &
\end{tikzcd}$$

QED

Solution by Rewriting to Equality

$R(x, f(x)) \xrightarrow{\text{rewriting}} f(x) = t(x)$ — $t(x)$ represents a term over x

$$\Downarrow$$

$\boxed{RW} \vdash \forall f, x.\ f(x) = t(x) \Rightarrow R(x, f(x))$ — proved by rewriter

$f_0(x) \triangleq t(x)$

$S'(f) \triangleq [f = f_0]$

$\boxed{SS'} \vdash S'(f) \Rightarrow S(f)$

$$\begin{tikzcd}
S'(f) \arrow[r, "\delta_{S'}"] & f = f_0 \arrow[rr, bend left] & & \forall x.\ R(x, f(x)) \arrow[r, "\delta_S"] & S(f) \\
RW \arrow[r, "f := f_0"'] & \forall x.\ f_0(x) = t(x) \Rightarrow R(x, f_0(x)) \arrow[r, "\delta_{f_0}"] & \forall x.\ R(x, f_0(x)) \arrow[ur] & &
\end{tikzcd}$$

QED

Solution by User

$t(x)$ — term over x supplied by user

$\boxed{\mathrm{SOL}} \vdash \forall f, x.\ f(x) = t(x) \Rightarrow R(x, f(x))$ — proved by user

$$\Downarrow$$

$f_0(x) \triangleq t(x)$

$S'(f) \triangleq [f = f_0]$

$\boxed{SS'} \vdash S'(f) \Rightarrow S(f)$

$$\begin{tikzcd}
S'(f) \arrow[r, "\delta_{S'}"] & f = f_0 \arrow[rr] & & \forall x.\ R(x, f(x)) \arrow[r, "\delta_S"] & S(f) \\
\mathrm{SOL} \arrow[r, "f := f_0"'] & \forall x.\ f_0(x) = t(x) \Rightarrow R(x, f_0(x)) \arrow[r, "\delta_{f_0}"] & \forall x.\ R(x, f_0(x)) \arrow[ur] & &
\end{tikzcd}$$

QED