DIVIDE & CONQUER 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:

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

this is more general than divide & conquer; it could be moved to separate notes

Representative Schema

$$DC(a,b,c,d)(x) \triangleq \underline{\text{if}}\ a(x)\ \underline{\text{then}}\ b(x)\ \underline{\text{else}}\ \underline{\text{let}}\ (x_1,x_2) = d(x)\ \underline{\text{in}}\ c(DC(a,b,c,d)(x_1),\ DC(a,b,c,d)(x_2))$$

$a \subseteq \mathcal{U}$	— atomic (i.e. non-decomposable) problems
$b : \mathcal{U} \to \mathcal{U}$	— base case, i.e. direct solution for atomic problems
$c : \mathcal{U} \times \mathcal{U} \to \mathcal{U}$	— compose solutions to sub-problems
$d : \mathcal{U} \to \mathcal{U} \times \mathcal{U}$	— decompose problems into sub-problems
$DC(a,b,c,d) : \mathcal{U} \to \mathcal{U}$	— solve all problems via divide & conquer
$\mu : \mathcal{U} \to \mathcal{U}$	— measure of DC (variable, schematic)
$\prec \subseteq \mathcal{U} \times \mathcal{U}$	— well-founded relation of DC (variable, schematic)
$\rho \subseteq \mathcal{U} \times \mathcal{U}$	— input/output relation (i.e. definition of solutions to problems)

$\boxed{WF}$	$\emptyset \subset U \subseteq \mathcal{U} \Rightarrow \exists m \in U.\ \forall u \in U \setminus \{m\}.\ u \nprec m$	— $\prec$ well-founded
$\boxed{\tau}$	$\neg a(x) \wedge d(x) = (x_1, x_2) \Rightarrow \mu(x_1) \prec \mu(x) \wedge \mu(x_2) \prec \mu(x)$	— DC terminates
$\boxed{BASE}$	$a(x) \Rightarrow \rho(x, b(x))$	— b solves atomic case
$\boxed{STEP}$	$\neg a(x) \wedge d(x) = (x_1, x_2) \wedge \rho(x_1, y_1) \wedge \rho(x_2, y_2) \Rightarrow \rho(x, c(y_1, y_2))$	— c composes sub-solutions into solutions
$\boxed{ALL}$	$\rho(x, DC(a,b,c,d)(x))$	

$\boxed{COR} \vdash \boxed{BASE} \wedge \boxed{STEP} \Rightarrow \boxed{ALL}$ — correctness theorem

induct DC

$a(x) \xrightarrow{\delta_{DC}} DC(a,b,c,d)(x) = b(x) \longrightarrow \rho(x, DC(a,b,c,d)(x))$

$a(x) \xrightarrow{BASE} \rho(x, b(x)) \longrightarrow \rho(x, DC(a,b,c,d)(x))$

$\neg a(x) \xrightarrow{\delta_{DC}} DC(a,b,c,d)(x) = c(DC(a,b,c,d)(x_1), DC(a,b,c,d)(x_2)) \longrightarrow \rho(x, DC(a,b,c,d)(x))$

$(x_1, x_2) \triangleq d(x)$

$\xrightarrow{IH} \begin{cases} \rho(x_1, DC(a,b,c,d)(x_1)) \\ \rho(x_2, DC(a,b,c,d)(x_2)) \end{cases} \xrightarrow{STEP} \rho(x, c(DC(a,b,c,d)(x_1), DC(a,b,c,d)(x_2))) \longrightarrow \rho(x, DC(a,b,c,d)(x))$

QED

List Fold Schema and Its Application

$$\mathrm{fold}(g,h)(x) \triangleq \underline{\mathrm{if}}\ \mathrm{atom}(x)\ \underline{\mathrm{then}}\ g(x)\ \underline{\mathrm{else}}\ h(\mathrm{car}(x), \mathrm{fold}(g,h)(\mathrm{cdr}(x)))$$

$$\mu_{fold}(x) \triangleq \mathrm{len}(x) \qquad \boxed{\tau_{fold}} \vdash \neg\,\mathrm{atom}(x) \Rightarrow \mathrm{len}(\mathrm{cdr}(x)) < \mathrm{len}(x)$$

$\boxed{\text{BASE}}$ $\mathrm{atom}(x) \Rightarrow \rho(x, g(x))$

$\boxed{\text{STEP}}$ $\mathrm{consp}(x) \wedge \rho(\mathrm{cdr}(x), y) \Rightarrow \rho(x, h(\mathrm{car}(x), y))$

$\boxed{\text{ALL}}$ $\rho(x, \mathrm{fold}(g,h)(x))$

$\boxed{\text{COR}} \vdash \boxed{\text{BASE}} \wedge \boxed{\text{STEP}} \Rightarrow \boxed{\text{ALL}}$

induct x

$$\mathrm{atom}(x) \xrightarrow{\delta_{fold}} \mathrm{fold}(g,h)(x) = g(x) \longrightarrow \rho(x, \mathrm{fold}(g,h)(x))$$

$$\mathrm{atom}(x) \xrightarrow{\text{BASE}} \rho(x, g(x)) \longrightarrow \rho(x, \mathrm{fold}(g,h)(x))$$

$$\mathrm{consp}(x) \xrightarrow{\delta_{fold}} \mathrm{fold}(f,g)(x) = h(\mathrm{car}(x), \mathrm{fold}(g,h)(\mathrm{cdr}(x))) \longrightarrow \rho(x, \mathrm{fold}(g,h)(x))$$

$$\mathrm{consp}(x) \xrightarrow{\text{IH}} \rho(\mathrm{cdr}(x), \mathrm{fold}(g,h)(\mathrm{cdr}(x))) \xrightarrow{\text{STEP}} \rho(x, h(\mathrm{car}(x), \mathrm{fold}(g,h)(\mathrm{cdr}(x)))) \longrightarrow \rho(x, \mathrm{fold}(g,h)(x))$$

QED

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

$$\left.\begin{aligned} S'(f,g,h) &\triangleq [f = \mathrm{fold}(g,h) \wedge S_g(g) \wedge S_h(h)] \\ S_g(g) &\triangleq [\forall x.\, \mathrm{atom}(x) \Rightarrow R(x, g(x))] \\ S_h(h) &\triangleq [\forall x,y.\, \mathrm{consp}(x) \wedge R(\mathrm{cdr}(x), y) \Rightarrow R(x, h(\mathrm{car}(x), y))] \end{aligned}\right\}$$ — new specifications

$\boxed{\text{SS}'} \vdash S'(f,g,h) \Rightarrow S(f)$

$$S'(f,g,h) \xrightarrow{\delta_{S'}} f = \mathrm{fold}(g,h) \longrightarrow [\forall x.\, R(x, f(x))] \overset{\delta_S}{=} S(f)$$

$$S'(f,g,h) \longrightarrow S_g(g),\ S_h(h) \xrightarrow[\rho := R]{\text{COR}} \forall x.\, R(x, \mathrm{fold}(g,h)(x)) \longrightarrow [\forall x.\, R(x, f(x))]$$

QED

More General List Fold Schema and Its Application

$S(f) \triangleq [\forall x, \bar{x}.\ R(x, \bar{x}, f(x, \bar{\alpha}(\bar{x})))]$ — more general form of problem specification — $\alpha : \mathcal{U}^n \to \mathcal{U}^m$

$fold(g,h)(x, \bar{z}) \triangleq \underline{if}\ atom(x)\ \underline{then}\ g(x, \bar{z})\ \underline{else}\ h(car(x), \bar{z}, fold(g,h)(cdr(x), \bar{z}))$ — same as before, plus $\bar{z}$

$\mu_{fold}(x) \triangleq len(x)$ $\quad \boxed{\tau_{fold}} \vdash \neg atom(x) \Longrightarrow len(cdr(x)) < len(x)$

$\boxed{BASE}\ atom(x) \Longrightarrow \rho(x, \bar{x}, g(x, \bar{\alpha}(\bar{x})))$

$\boxed{STEP}\ consp(x) \wedge \rho(cdr(x), \bar{x}, y) \Longrightarrow \rho(x, \bar{x}, h(car(x), \bar{\alpha}(\bar{x}), y))$

$\boxed{ALL}\ \rho(x, \bar{x}, fold(g,h)(x, \bar{\alpha}(\bar{x})))$

$\boxed{COR} \vdash \boxed{BASE} \wedge \boxed{STEP} \Longrightarrow \boxed{ALL}$

induct x

$atom(x) \xrightarrow[\bar{z} := \bar{\alpha}(\bar{x})]{\delta_{fold}} fold(g,h)(x, \bar{\alpha}(\bar{x})) = g(\bar{x}, \bar{\alpha}(\bar{x})) \longrightarrow \rho(x, \bar{x}, fold(g,h)(x, \bar{\alpha}(\bar{x})))$

$atom(x) \xrightarrow{BASE} \rho(x, \bar{x}, g(x, \bar{\alpha}(\bar{x}))) \longrightarrow \rho(x, \bar{x}, fold(g,h)(x, \bar{\alpha}(\bar{x})))$

$consp(x) \xrightarrow[\bar{z} := \bar{\alpha}(\bar{x})]{\delta_{fold}} fold(g,h)(\bar{x}, \alpha(\bar{x})) = h(car(x), \bar{\alpha}(\bar{x}), fold(g,h)(cdr(x), \bar{\alpha}(\bar{x})))$

$consp(x) \xrightarrow{IH} \rho(cdr(x), \bar{x}, fold(g,h)(cdr(x), \bar{\alpha}(\bar{x}))) \xrightarrow{STEP} \rho(x, \bar{x}, h(car(x), \bar{\alpha}(\bar{x}), fold(g,h)(cdr(x), \bar{\alpha}(\bar{x}))))$

$\longrightarrow \rho(x, \bar{x}, fold(g,h)(\bar{x}, \alpha(\bar{x})))$

QED

$$\left.\begin{array}{l} S'(f,g,h) \triangleq [f = fold(g,h) \wedge S_g(g) \wedge S_h(h)] \\ S_g(g) \triangleq [\forall x, \bar{x}.\ atom(x) \Rightarrow R(x, \bar{x}, g(x, \bar{\alpha}(\bar{x})))] \\ S_h(h) \triangleq [\forall x, \bar{x}, y.\ consp(x) \wedge R(cdr(x), \bar{x}, y) \Rightarrow R(x, \bar{x}, h(car(x), \bar{\alpha}(\bar{x}), y))] \end{array}\right\}$$ — new specifications

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

$S'(f,g,h) \xrightarrow{\delta_{S'}} f = fold(g,h)$, $S_g(g)$, $S_h(h)$

$S_g(g), S_h(h) \xrightarrow[\rho := R]{COR} \forall x.\ R(x, \bar{x}, fold(g,h)(x, \bar{\alpha}(\bar{x}))) \longrightarrow [\forall x.\ R(x, \bar{x}, f(x, \bar{\alpha}(\bar{x})))] \overset{\delta_S}{=} S(f)$

QED