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 2^{nd}-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 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)

$\boxed{WF}$	$\emptyset \subset U \subseteq \mathcal{U} \Rightarrow \exists m \in U.\ \forall u \in U \setminus \{m\}.\ u \not\prec m$	— $\prec$ 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

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

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

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

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

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

QED

List Fold Schema and Its Application

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

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

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

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

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

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

induct x

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

$\mathrm{atom}(x) \xrightarrow{\mathrm{BASE}} \rho(x, g(x))$

$\rho(x, \mathrm{fold}(f,g)(x))$

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

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

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

QED

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

$S'(f,g,h) \triangleq [f = \mathrm{fold}(g,h) \wedge S_g(g) \wedge S_h(h)]$

$S_g(g) \triangleq [\forall x.\, \mathrm{atom}(x) \Rightarrow R(x, g(x))]$

$S_h(h) \triangleq [\forall x,y.\, \mathrm{consp}(x) \wedge R(\mathrm{cdr}(x), y) \Rightarrow R(x, h(\mathrm{car}(x), y))]$

$\Big\}$ — new specifications

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

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

$S'(f,g,h) \rightarrow S_g(g)$

$S'(f,g,h) \rightarrow S_h(h)$

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

$[\forall x.\, R(x, f(x))] \overset{\delta_S}{=} S(f)$

QED