Coinduction beats induction on streams

David von Oheimb, TU München

http://www4.in.tum.de/~oheimb/

A formalization of the first pages of

Manfred Broy:
Specification and Refinement of a Buffer of Length One
Working Material of Marktoberdorf Summer School 1994

Isabelle Sources available from:

http://isabelle.in.tum.de/library/HOLCF/FOCUS/

Overview

- Introduction
- Specifications
  - Equational
  - Assumption/Commitment
  - (State-based)
- Proofs
  - by coinduction
  - by induction on streams
    requiring admissibility
  - simplifications by using coinduction
- Conclusions

Stream Domains

General streams: possibly infinite lists of elements α: $\alpha^\omega = \alpha^* \cup \alpha^\infty$

domain $(\alpha{::}pcpo)\ stream = (\mathsf{ft}{::}\alpha)\ \&\&\ (lazy\ \mathsf{rt}{::}\alpha\ stream)$ $\quad i.e., S \cong \alpha \times S$
constdefs $\# :: (\alpha{::}pcpo)\ stream \Rightarrow inat$
$\#s \equiv \mathsf{if\ stream\_finite}\ s\ \mathsf{then\ fin}\ (\mu n.\ \mathsf{stream\_take}\ n{\cdot}s = s)\ \mathsf{else}\ \infty$

$$stream\_take\_lemma\ \frac{\forall n.\ \mathsf{stream\_take}\ n{\cdot}s = \mathsf{stream\_take}\ n{\cdot}s'}{s = s'}$$

FOCUS streams: streams with flat elements

types $\alpha\ fstream = (\alpha\ lift)\ stream$
$\_\frown\_ :: \alpha \Rightarrow \alpha\ fstream \to \alpha\ fstream$
$a \frown s \equiv \uparrow a\ \&\&\ s$
$\langle\rangle \equiv \bot$

$$fstream\_ind\ \frac{\mathsf{adm}\ P \qquad P\ \langle\rangle \qquad \forall a\ s.\ P\ s \Longrightarrow P\ (a \frown s)}{P\ x}$$

Equational Specification

types D
datatype $M = \mathsf{Md}\ D \mid \bullet$

Input: $\mathsf{Md}\ d_1 \frown \bullet \frown \mathsf{Md}\ d_2 \frown \bullet \frown \ldots$

Output: $d_1 \frown \quad d_2 \frown \ldots$

Loose Specification:

$\mathsf{BufEq} :: (M\ fstream \to D\ fstream)\ set$
$\mathsf{BufEq} \equiv \mathsf{gfp}\ (\lambda B.\ \{f.\ \forall d.\ f \cdot (\mathsf{Md}\ d \frown \langle\rangle) = \langle\rangle\ \wedge$
$(\forall x.\ \exists f' \in B.\ f \cdot (\mathsf{Md}\ d \frown \bullet \frown x) = d \frown f' \cdot x)\})$

Application lemmas (exploiting monotonicity):

Buf_f_empty	$f \in \mathsf{BufEq} \Longrightarrow f \cdot \langle\rangle = \langle\rangle$
Buf_f_d	$f \in \mathsf{BufEq} \Longrightarrow f \cdot (\mathsf{Md}\ d \frown \langle\rangle) = \langle\rangle$
$Buf\_f\_d\_req$	$f \in \mathsf{BufEq} \Longrightarrow \forall x.\ \exists f' \in \mathsf{BufEq}.\ f \cdot (\mathsf{Md}\ d \frown \bullet \frown x) = d \frown f' \cdot x$

Assumption/Commitment Specification

$\mathsf{BufAC\_Asm} :: (M\ \mathit{fstream})\ \mathit{set}$

$\mathsf{BufAC\_Asm} \equiv \mathsf{gfp}\ (\lambda A.\ \{s.\ s = \langle\rangle \lor$
$(\exists d\ x.\ s = \mathsf{Md}\ d \frown x \land (x = \langle\rangle \lor (\mathsf{ft}\cdot x = \uparrow\bullet \land (\mathsf{rt}\cdot x) \in A)))\})$

$\mathsf{BufAC\_Cmt} :: (M\ \mathit{fstream} * D\ \mathit{fstream})\ \mathit{set}$

$\mathsf{BufAC\_Cmt} \equiv \mathsf{gfp}\ (\lambda C.\ \{(s,t).\ \forall d\ x.$
$(s = \langle\rangle \Longrightarrow t = \langle\rangle) \land$
$(s = \mathsf{Md}\ d \frown \langle\rangle \Longrightarrow t = \langle\rangle) \land$
$(s = \mathsf{Md}\ d \frown \bullet \frown x \Longrightarrow \mathsf{ft}\cdot t = \uparrow d \land (x, \mathsf{rt}\cdot t) \in C)\})$

$\mathsf{BufAC} \equiv \{f.\ \forall s.\ s \in \mathsf{BufAC\_Asm} \Longrightarrow (s, f\cdot s) \in \mathsf{BufAC\_Cmt}\}$

Application lemmas:

$BufAC\_Asm\_empty$ $\langle\rangle \in \mathsf{BufAC\_Asm}$

$BufAC\_Asm\_d$ $\mathsf{Md}\ d \frown \langle\rangle \in \mathsf{BufAC\_Asm}$

$BufAC\_Asm\_d\_req$ $\mathsf{Md}\ d \frown \bullet \frown x \in \mathsf{BufAC\_Asm} \Longleftrightarrow x \in \mathsf{BufAC\_Asm}$

⋮

$BufAC\_f\_d\_req$ $f \in \mathsf{BufAC} \Longrightarrow \exists f' \in \mathsf{BufAC}.\ \forall x.\ f\cdot(\mathsf{Md}\ d \frown \bullet \frown x) = d \frown f'\cdot x$

Proof by Coinduction

Goal: BufAC $\subseteq$ BufEq $(= \mathsf{gfp}\ (\lambda B.\ \ldots))$

Principle: $weak\_coinduction\ \dfrac{X \subseteq F\ X}{X \subseteq \mathsf{gfp}\ F}$

Subgoals:

$$f \in \mathsf{BufAC} \Longrightarrow f \cdot (\mathsf{Md}\ d \frown \bot) = \bot$$
$$f \in \mathsf{BufAC} \Longrightarrow \forall x.\ \exists f' \in \mathsf{BufAC}.\ f \cdot (\mathsf{Md}\ d \frown \bullet \frown x) = d \frown f' \cdot x$$

Proof by Induction on Streams

Goal: BufEq $\subseteq$ BufAC

Subgoal: $f\in\mathsf{BufEq} \Longrightarrow (\forall s.\ s\in\mathsf{BufAC\_Asm} \Longrightarrow (s,\ f\cdot s)\in\mathsf{BufAC\_Cmt})$

Principle:

$$fstream\_ind2\ \frac{\mathsf{adm}\ P \quad P\ \langle\rangle \quad \forall a.\ P\ (a\frown\langle\rangle) \quad \forall a\ b\ s.\ P\ s \Longrightarrow P\ (a\frown b\frown s)}{P\ x}$$

Subgoals:

$$f\in\mathsf{BufEq} \Longrightarrow \mathsf{adm}\ (\lambda s.\ s\in\mathsf{BufAC\_Asm} \Longrightarrow (s,\ f\cdot s)\in\mathsf{BufAC\_Cmt})$$
$$f\in\mathsf{BufEq} \Longrightarrow \perp\in\mathsf{BufAC\_Asm} \Longrightarrow (\perp,\ f\cdot\perp)\in\mathsf{BufAC\_Cmt}$$
$$f\in\mathsf{BufEq} \Longrightarrow d\frown\perp\in\mathsf{BufAC\_Asm} \Longrightarrow (a\frown\perp,\ f\cdot(a\frown\perp))\in\mathsf{BufAC\_Cmt}$$
$$f\in\mathsf{BufEq} \Longrightarrow (s\in\mathsf{BufAC\_Asm} \Longrightarrow (s,\ f\cdot s)\in\mathsf{BufAC\_Cmt}) \Longrightarrow$$
$$a\frown b\frown s\in\mathsf{BufAC\_Asm} \Longrightarrow (a\frown b\frown s,\ f\cdot(a\frown b\frown s))\in\mathsf{BufAC\_Cmt}$$

Proof of Admissibility

Goal: $f \in \mathsf{BufEq} \Longrightarrow \mathsf{adm}\ (\lambda s.\ s \in \mathsf{BufAC\_Asm} \Longrightarrow (s,\ f \cdot s) \in \mathsf{BufAC\_Cmt})$

Admissibility with stream expansion (exploiting flatness):

$$fs\_admI\ \frac{\forall Y.\ \mathsf{chain}\ Y \Longrightarrow \forall i.\ P\ (Y\ i) \Longrightarrow \forall k.\ \exists j.\ \mathsf{fin}\ k < \#(Y\ j) \Longrightarrow P\ (\bigsqcup Y)}{\mathsf{adm}\ P}$$

Iterative approximation of fixpoint: (exploiting continuity)

$x \in \mathsf{gfp}\ F = (\forall n.\ x \in \mathsf{iterate\_from\_UNIV}\ F\ n)$

Lemmas: (require reasoning about stream length *etc.*)

- adm_BufAC_Asm: $\mathsf{adm}\ (\lambda s.\ s \in \mathsf{BufAC\_Asm})$
- $adm\_non\_BufAC\_Asm$: $\mathsf{adm}\ (\lambda s.\ s \notin \mathsf{BufAC\_Asm})$
- $BufAC\_Asm\_cong$: $[\![f \in \mathsf{BufEq};\ f' \in \mathsf{BufEq};\ s \in \mathsf{BufAC\_Asm}]\!] \Longrightarrow f \cdot s = f' \cdot s$
- $BufAC\_Asm\_antiton$: $x \sqsubseteq y \Longrightarrow y \in \mathsf{BufAC\_Asm} \Longrightarrow x \in \mathsf{BufAC\_Asm}$

Simplifications by Use of Coinduction

$BufAC\_Asm\_cong$: $[\![f{\in}\mathsf{BufEq};\ f'{\in}\mathsf{BufEq};\ s{\in}\mathsf{BufAC\_Asm}]\!] \Longrightarrow f{\cdot}s = f'{\cdot}s$
using $stream\_take\_lemma$, avoiding admissibility

Goal: $\mathsf{BufEq} \subseteq \mathsf{BufAC}$

Subgoal: $f{\in}\mathsf{BufEq} \Longrightarrow s{\in}\mathsf{BufAC\_Asm} \Longrightarrow (s,\ f{\cdot}s){\in}\mathsf{gfp}\ (\lambda C.\ \ldots)$

Idea: re-write to make coinduction applicable

Principle:

$$weak\_coinduct\_image\ \frac{a{\in}X \qquad g`X \subseteq F\ (g`X)}{g\ a \in \mathsf{gfp}\ F}$$

Conclusions

Mechanical theorem prover . . .

- enforces clean proofs
- assists with the details
- gives maximal confidence in results

For proofs on infinite structures . . .

- induction is complicated because of admissibility
- equality by take lemma is quite handy
- for recursive predicates, coinduction is the method of choice