Demonstrații II

Traian Florin Șerbănuță

Departamentul de Informatică, FMI, UNIBUC
traian.serbanuta@fmi.unibuc.ro

17 noiembrie 2014

Inducție deductivă pentru mulțimi definite recursiv

Principiul inducției deductive

Pentru a demonstra că P este adevărată pentru orice element al unei mulțimi A definită recursiv de regulile din $\mathcal{R}$:

- Considerăm mulțimea elementelor din A pentru care P e adevărată
- Arătăm că este închisă la regulile din $\mathcal{R}$

Concret, pentru fiecare regulă (H, c), cu $H \subseteq A$

Ipoteza de inducție Presupunem că $P(h)$ e adevărată pentru orice $h \in H$,

Concluzie Demonstrăm că $P(c)$ e adevărată.

Arbori de sintaxă

Sintaxă

$$e ::= n \mid b \mid e\ op\ e \mid \texttt{if}\ e\ \texttt{then}\ e\ \texttt{else}\ e$$
$$\mid\ !\,l \mid l \texttt{:=} e$$
$$\mid \texttt{skip} \mid e\ \texttt{;}\ e \mid \texttt{while}\ e\ \texttt{do}\ e\ \texttt{done}$$

Univers

Totalitatea arborilor cu etichete din mulțimea:

$$\mathbb{E} = \{n \mid n \in \mathbb{Z}\} \cup \{true, false\} \cup \{\_ + \_, \_ \leq \_\} \cup \{\texttt{if}\ \_\ \texttt{then}\ \_\ \texttt{else}\ \_\}$$
$$\cup \{!l \mid l \in \mathbb{L}\} \cup \{l := \_ \mid l \in \mathbb{L}\}$$
$$\cup \{\texttt{skip}, \_;\_, \texttt{while}\ \_\ \texttt{do}\ \_\ \texttt{done}\}$$

Arbori abstracți de sintaxă

Definiți recursiv ca submulțime a arborilor de mai sus

Reguli de formare a arborilor abstracți de sintaxă

(sN) $\quad n \quad$ *dacă* $n \in \mathbb{Z}$

(sB) $\quad b \quad$ *dacă* $b \in \{true, false\}$

(sSkip) $\quad$ `skip`

(sLoc) $\quad !l \quad$ *dacă* $l \in \mathbb{L}$

(sAtrib) $\quad \dfrac{e}{l := \_} \quad$ *dacă* $l \in \mathbb{L}$

$$e$$

(sOp) $\quad \dfrac{e_1 \quad e_2}{\_ \; o \; \_} \quad$ *dacă* $o \in \{+, \leq\}$

$$e_1 \qquad\qquad e_2$$

(sSecv) $\quad \dfrac{e_1 \quad e_2}{\_ ; \_}$

$$e_1 \qquad\qquad e_2$$

(sWhile) $\quad \dfrac{e_1 \quad e_2}{\texttt{while} \; \_ \; \texttt{do} \; \_ \; \texttt{done}}$

$$e_1 \qquad\qquad e_2$$

(sIf) $\quad \dfrac{e_1 \quad e_2 \quad e_3}{\texttt{if} \; \_ \; \texttt{then} \; \_ \; \texttt{else} \; \_}$

$$e_1 \qquad e_2 \qquad e_3$$

Principiul inducției structurale

Inducție pe termeni definiți recursiv

Scop:

Demonstrăm că P este adevărată pentru orice termen (AST) definit (recursiv) de o gramatică independentă de context.

Metoda:

Instanțiem principiul inducției deductive pentru sistemul de reguli indus de producțiile gramaticii.

Concret

Pentru fiecare regulă de formare a expresiilor indusă de gramatică,

Ipoteza de inducție Presupunem că P ține pentru subexpresiile componente

Concluzie Demonstrăm că P ține și pentru expresia definită de regulă.

Ce este o demonstrație?

O demonstrație formală

- O derivare a concluziei din premize folosind logică formală
- Exemplu: un arbore de demonstrație
- Greu de scris de mână dar ușor de verificat automat

O demonstrație informală, dar riguroasă

- Noțiunea uzuală de demonstrație matematică
- Un argument cu suficiente detalii pentru a convinge că poate fi transformat într-o demonstrație formală

Apă de ploaie

Orice nu se încadrează în cele două cazuri de mai sus.

De ce demonstrăm lucruri „evidente“?

- O demonstrație ne poate arăta de ce e evidentă o afirmație
- Uneori afirmațiile evidente se dovedesc a fi false
    - O demonstrație ne poate ajuta să descoperim ipoteze lipsă
- Uneori afirmațiile evidente nu sunt deloc evidente
    - E.g., Conjectura lui Kepler, teorema celor 4 culori
- Demonstrațiile constructive pot conduce la metode algoritmice

Determinism puternic

Teoremă (Limbajul IMP este puternic determinist)

Dacă $\langle e, s\rangle \rightarrow \langle e_1, s_1\rangle$ *și* $\langle e, s\rangle \rightarrow \langle e_2, s_2\rangle$*, atunci* $e_1 = e_2$ *și* $s_1 = s_2$*.*

Idee de demonstrație.

Fie P proprietatea definită de

$P(e) \stackrel{def}{=} \forall s, e_1, s_1, e_2, s_2.$

$$\langle e, s\rangle \rightarrow \langle e_1, s_1\rangle \wedge \langle e, s\rangle \rightarrow \langle e_2, s_2\rangle \implies \langle e_1, s_1\rangle = \langle e_2, s_2\rangle$$

Demonstrăm că P e adevărată pentru toate expresiile IMP prind inducție asupra structurii lui e. □

Determinism puternic

Definiție (Valoare)

Spunem că v e valoare, notat $valoare(v)$, dacă v e întreg, boolean, sau `skip`. Fie $\mathbb{V}$ mulțimea valorilor, adică

$$\mathbb{V} = \mathbb{Z} \cup \{true, false\} \cup \{\texttt{skip}\}$$

Lemă (Valorile nu mai pot fi reduse)

Dacă v este valoare, atunci pentru orice stare a memoriei s,

$$\langle v, s \rangle \not\rightarrow$$

Cazuri de inducție structurală pentru IMP

Cazuri de bază. Demonstrăm

- $P(n)$ pentru orice $n \in \mathbb{Z}$,
- $P(true)$ și $P(false)$
- $P(\texttt{skip})$
- $P(\texttt{!}\ l)$ pentru orice $l \in \mathbb{L}$

Recursie simplă. Demonstrăm că dacă $P(e)$ atunci și

- $P(l \texttt{ := } e)$ pentru orice $l \in \mathbb{L}$

Recursie dublă. Demonstrăm că dacă $P(e_1)$ și $P(e_2)$, atunci și

- $P(e_1 \text{ o } e_2)$ pentru orice $o \in \{\leq, +\}$
- $P(e_1 \texttt{ ; } e_2)$
- $P(\texttt{while } e_1 \texttt{ do } e_2 \texttt{ done})$

Recursie triplă. Demonstrăm că dacă $P(e_1)$, $P(e_2)$ și $P(e_3)$, atunci și

- $P(\texttt{if } e_1 \texttt{ then } e_2 \texttt{ else } e_3)$

Proprietatea de a progresa a sistemului de tipuri

Teoremă

Dacă $\Gamma \vdash e : T$ *și* $Dom(\Gamma) \subseteq Dom(s)$ *atunci e este valoare sau există* e', s' *astfel încât* $\langle e, s\rangle \to \langle e', s'\rangle$.

Idee de demonstrație.

Fie P proprietatea definită de
$P(\Gamma \vdash e : t) \stackrel{def}{=} value(e) \vee (\forall s.$

$$Dom(\Gamma) \subseteq Dom(s) \implies \exists e', s'.\langle e, s\rangle \to \langle e', s'\rangle$$

Demonstrăm că P e adevărată pentru toate expresiile care au un tip prin inducție asupra definiției relației de tip. □

Proprietatea de a progresa a sistemului de tipuri

Lemă

Dacă $\Gamma \vdash e : T$ și e este valoare, atunci

Dacă $T = \mathtt{int}$ atunci există n întreg astfel încât $e = n$

Dacă $T = \mathtt{bool}$ atunci $e = \mathit{true}$ sau $e = \mathit{false}$

Dacă $T = \mathtt{unit}$ atunci $e = \mathtt{skip}$

Reguli pentru tipuri

(τN) $\Gamma \vdash n : \mathtt{int}$ *dacă* $n \in \mathbb{Z}$

(τB) $\Gamma \vdash b : \mathtt{bool}$ *dacă* $b \in \{true, false\}$

(τ+) $\dfrac{\Gamma \vdash e_1 : \mathtt{int} \quad \Gamma \vdash e_2 : \mathtt{int}}{\Gamma \vdash e_1 + e_2 : \mathtt{int}}$ (τ≤) $\dfrac{\Gamma \vdash e_1 : \mathtt{int} \quad \Gamma \vdash e_2 : \mathtt{int}}{\Gamma \vdash e_1 <= e_2 : \mathtt{bool}}$

(τIf) $\dfrac{\Gamma \vdash e_1 : \mathtt{bool} \quad \Gamma \vdash e_2 : T \quad \Gamma \vdash e_3 : T}{\Gamma \vdash \mathtt{if}\ e_1\ \mathtt{then}\ e_2\ \mathtt{else}\ e_3 : T}$

(τAtrib) $\dfrac{\Gamma \vdash e : \mathtt{int}}{\Gamma \vdash l := e : \mathtt{unit}}$ *dacă* $\Gamma(l) = \mathtt{intref}$

(τLoc) $\Gamma \vdash !l : int$ *dacă* $\Gamma(l) = \mathtt{intref}$

(τSkip) $\Gamma \vdash \mathtt{skip} : \mathtt{unit}$

(τSecv) $\dfrac{\Gamma \vdash e_1 : \mathtt{unit} \quad \Gamma \vdash e_2 : T}{\Gamma \vdash e_1 ; e_2 : T}$

(τWhile) $\dfrac{\Gamma \vdash e_1 : \mathtt{bool} \quad \Gamma \vdash e_2 : \mathtt{unit}}{\Gamma \vdash \mathtt{while}\ e_1\ \mathtt{do}\ e_2\ \mathtt{done} : \mathtt{unit}}$

Proprietatea de conservare a tipului

Teoremă

Dacă $\Gamma \vdash e : T$, $Dom(\Gamma) \subseteq Dom(s)$ *și* $\langle e, s\rangle \to \langle e', s'\rangle$, *atunci* $\Gamma \vdash e' : T$ *și* $Dom(\Gamma) \subseteq Dom(s')$.

Idee de demonstrație.

Fie P proprietatea definită de
$P(\langle e, s\rangle \to \langle e', s'\rangle) \stackrel{def}{=} \forall \Gamma, T.$

$$\Gamma \vdash e : T \wedge Dom(\Gamma) \subseteq Dom(s) \implies \Gamma \vdash e' : T \wedge Dom(\Gamma) \subseteq Dom(s')$$

Demonstrăm că P e adevărată pentru întreg sistemul de tranziție asociat semanticii IMP prin inducție asupra definiției sistemului de tranziție. □

Definiția sistemului de tranziție pentru limbajul IMP

(+) $\langle n_1 + n_2, s\rangle \to \langle n, s\rangle$ *dacă* $n = n_1 + n_2$

(≤) $\langle n_1 \mathrel{<=} n_2, s\rangle \to \langle b, s\rangle$ *dacă* $b = (n_1 \leq n_2)$

(OpS) $$\frac{\langle e_1, s\rangle \to \langle e_1', s'\rangle}{\langle e_1\ o\ e_2, s\rangle \to \langle e_1'\ o\ e_2, s'\rangle}$$

(OpD) $$\frac{\langle e_2, s\rangle \to \langle e_2', s'\rangle}{\langle n_1\ o\ e_2, s\rangle \to \langle n_1\ o\ e_2', s'\rangle}$$

(Loc) $\langle !\ l, s\rangle \to \langle n, s\rangle$ *dacă* $l \in Dom(s), n = s(l)$

(Atrib) $\langle l := n, s\rangle \to \langle \mathtt{skip}, s[l \mapsto n]\rangle$ *dacă* $l \in Dom(s)$

(AtribD) $$\frac{\langle e, s\rangle \to \langle e', s'\rangle}{\langle l := e, s\rangle \to \langle l := e', s'\rangle}$$

(Secv) $\langle \mathtt{skip};\ e_2, s\rangle \to \langle e_2, s\rangle$

(SecvS) $$\frac{\langle e_1, s\rangle \to \langle e_1', s'\rangle}{\langle e_1\ ;\ e_2\rangle, s \to \langle e_1'\ ;\ e_2, s'\rangle}$$

(IfTrue) $\langle \mathtt{if\ true\ then}\ e_1\ \mathtt{else}\ e_2, s\rangle \to \langle e_1, s\rangle$

(IfFalse) $\langle \mathtt{if\ false\ then}\ e_1\ \mathtt{else}\ e_2, s\rangle \to \langle e_2, s\rangle$

(IfS) $$\frac{\langle e, s\rangle \to \langle e', s'\rangle}{\langle \mathtt{if}\ e\ \mathtt{then}\ e_1\ \mathtt{else}\ e_2, s\rangle \to \langle \mathtt{if}\ e'\ \mathtt{then}\ e_1\ \mathtt{else}\ e_2, s'\rangle}$$

(While) $\langle \mathtt{while}\ e_1\ \mathtt{do}\ e_2\ \mathtt{done}\ , s\rangle \to$
$\langle \mathtt{if}\ e_1\ \mathtt{then}\ (e_2\ ;\ \mathtt{while}\ e_1\ \mathtt{do}\ e_2\ \mathtt{done})\ \mathtt{else\ skip}, s\rangle$

Proprietatea de siguranță a sistemului de tipuri

programele bine formate nu se împotmolesc

Teoremă

Dacă $\Gamma \vdash e : T$, $Dom(\Gamma) \subseteq Dom(s)$ *și* $\langle e, s\rangle \longrightarrow^* \langle e', s'\rangle$, *atunci* e' *este valoare sau există* e'', s'' *astfel încât* $\langle e', s'\rangle \to \langle e'', s''\rangle$.

Idee de demonstrație.

Fie P proprietatea definită de

$P(k) \stackrel{def}{=} \forall \Gamma, e, T, s, e', s'.\, valoare(e) \vee$

$$\Gamma \vdash e : T \wedge Dom(\Gamma) \subseteq Dom(s) \wedge \langle e, s\rangle \longrightarrow^k \langle e', s'\rangle$$

$$\implies \exists e'', s''.\langle e', s'\rangle \to \langle e'', s''\rangle$$

Demonstrăm că P e adevărată pentru întreg sistemul de tranziție asociat semanticii IMP prin inducție naturală asupra lui k. □

Tehnici de demonstrație

Rezumat

Determinism Inducție structurală pe definiția expresiilor e

Progres Inducție deductivă pe definiția relației de tip $\Gamma \vdash e : T$

Conservarea tipurilor Inducție deductivă pe definiția sistemului de tranziție $\langle e', s' \rangle \rightarrow \langle e'', s'' \rangle$

Siguranță Inducție matematică pe lungimea secvenței de tranziții $\longrightarrow^k$

Cum alegem pe ce facem inducție?

Cu grijă... în general alegem metoda cea mai la îndemână, încercăm să rescriem proprietatea pentru a vedea ce se cuantifică universal.