Formální Metody a Specifikace (LS 2011)
Přednáška 10: Terminace, totální správnost programů

Stefan Ratschan

Katedra číslicového návrhu
Fakulta informačních technologií
Ceské vysoké učení technické v Praze

29. duben 2011

Parciální vs. totální správnost

$x \leftarrow 564$
while T do
@ $x = 564$
return x

Aserce vždy platí, tj. splňuje *parciální* správnost.

Ale: Neskončí, tj. nesplňuje *totální* správnost.

Collatzův problém, rozhodnutelnost

while $x \neq 1$ **do**
    if $x \bmod 2 = 0$ **then**
        $x \leftarrow x/2$
    else
        $x \leftarrow 3x + 1$

Skončí pro každý vstup x?

Věta [Turing, 1937]:
Problém ověřování terminace (problém zastavení, halting problem) je nerozhodnutelný.

Terminace a výpočetní strom

Výpočetní strom:

- Kořeny: stavy s tak, že $s \models I$
- Pokud s je uzlem výpočetního stromu, a $s \to s'$,
  pak s' je další uzel s hranou z uzlu s do uzlu s'

Parciální správnost:

Pro každý uzel s tohoto stromu, $s \models O$.

Chybí pro totální správnost:

Každá cesta má konečnou délku.

Pozor: Totální správnost neimplikuje že existuje horní mez na délku cest!

Jinak řečeno, neimplikuje že existuje k tak, že

$$\bigcup_{i \in \{0,\ldots,k\}} \to^i \; = \; \to^*$$

Fundované relace

Binární predikát $\prec$ přes množinu S je *fundovanou relací* přesně když neexistuje žádná nekonečná posloupnost $s_1, s_2, \ldots$ tak, že $s_1 \succ s_2 \succ \ldots$

Příklad: $<$ je fundovanou relací přes přirozená čísla

Lexikografické uspořádání:

Pro $S = S_1 \times \cdots \times S_n$, příslušné uspořádání $\prec_1, \ldots, \prec_n$

$$(s_1, \ldots s_n) \prec (t_1, \ldots, t_n) \;:\Leftrightarrow\; \bigvee_{i=1}^{n} \left(s_i \prec_i t_i \wedge \bigwedge_{j=1}^{i-1} s_j = t_j \right)$$

Pokud $\prec_1, \ldots, \prec_n$ jsou fundované relace přes $S_1, \ldots, S_n$, pak $\prec$ je také fundovanou relací přes $S_1 \times \cdots \times S_n$.

Cíl: Důkaz: Pro daný program $\rightarrow$ je fundovanou relací.

Příklad: Hledaní v seřazeném poli

Pro $a \in \mathcal{A}_n$, $\mathrm{sorted}(a) :\Leftrightarrow \forall i \in \{1, \dots, n-1\} \,.\, a[i] \leq a[i+1]$

@ $a \in \mathcal{A}_n(\mathcal{N})$, $\mathrm{sorted}(a)$, $x \in \mathcal{N}$, $\exists i \in \{1, \dots, n\} \,.\, a[i] = x$
$l \leftarrow 1$; $u \leftarrow n$
@ $\exists i \in \{l, \dots, u\} \,.\, a[i] = x$
while $a[(l+u)/2] \neq x$ **do**
    @ $\exists i \in \{l, \dots, u\} \,.\, a[i] = x$
    if $a[(l+u)/2] < x$ **then** $l \leftarrow (l+u)/2$
    else $u \leftarrow (l+u)/2$
    @ $\exists i \in \{l, \dots, u\} \,.\, a[i] = x$
@ $a[(l+u)/2] = x$
$r \leftarrow (l+u)/2$
@ $a[r] = x$
return r

$$\left[\exists i \in \{l, \dots, u\} \,.\, a[i] = x \wedge a[\frac{l+u}{2}] < x\right] \Rightarrow \exists i \in \{\frac{l+u}{2}, \dots, u\} \,.\, a[i] = x$$

$$\left[\exists i \in \{l, \dots, u\} \,.\, a[i] = x \wedge a[\frac{l+u}{2}] \geq x\right] \Rightarrow \exists i \in \{l, \dots, \frac{l+u}{2}\} \,.\, a[i] = x \text{ ?}$$

Terminace

@ $a \in \mathcal{A}_n(\mathcal{N})$, $\mathrm{sorted}(a)$, $x \in \mathcal{N}$, $\exists i \in \{1, \dots, n-1\} \,.\, a[i] = x$
$l \leftarrow 1;\ u \leftarrow n$
@ $\exists i \in \{l, \dots, u\} \,.\, a[i] = x \wedge u - l \geq 0$
while $a[(l+u)/2] \neq x$ **do**
    @ $\exists i \in \{l, \dots, u\} \,.\, a[i] = x \wedge u - l \geq 0$
    $v \leftarrow u - l$
    if $a[(l+u)/2] < x$ **then** $l \leftarrow (l+u)/2$
    else $u \leftarrow (l+u)/2$
    @ $\exists i \in \{l, \dots, u\} \,.\, a[i] = x \wedge u - l \geq 0 \wedge u - l < v$
@ $a[(l+u)/2] = x$
$r \leftarrow (l+u)/2$
@ $a[r] = x$
return r

$u - l$ klesá, ale vždy $u - l \geq 0$,
    $<$ je fundovanou relací přes přirozená čísla

Terminologie

Pro danou fundovanou relaci $<$ přes množinu S takový term

- který během cyklu vždy má hodnotu ve množině S, a
- jeho hodnota se snižuje ohledně $<$

se jmenuje *variant cyklu* (angl. i *ranking function*)

Podobný pojem pro spojité systémy: *Ljapunovova funkce*

Vložené cykly

@ $a \in \mathcal{A}_n, s \in \mathcal{A}_r$
$\mathrm{prefix}(a, s, p, l) :\Leftrightarrow l \leq r \wedge p + l - 1 \leq n \wedge \forall i \in \{1, \dots, l\} \,.\, a[p + i - 1] = s[i]$
$\mathrm{contains}(a, s, p) :\Leftrightarrow \mathrm{prefix}(a, s, p, r)$

$i \leftarrow 0;\ l \leftarrow 0$
while $i \leq n - r + 1 \wedge l \leq r$ **do**
  @ $i \leq n - r + 1 \wedge \forall p \in \{1, \dots, i\} \,.\, \neg\mathrm{contains}(a, s, p)$
  $w_1 \leftarrow i;\ i \leftarrow i + 1;\ l \leftarrow 1$
  while $l \leq r \wedge a[i + l - 1] = s[l]$ **do**
    @ $l \leq r \wedge \mathrm{prefix}(a, s, i, l)$
    $w_2 \leftarrow l \wedge l \leftarrow l + 1$
    @ $l \leq r + 1 \wedge l > w_2 \wedge \mathrm{prefix}(a, s, i, l - 1)$
  @ $i \leq n - r + 2 \wedge i > w_1$
  @ $\forall p \in \{1, \dots, i - 1\} \,.\, \neg\mathrm{contains}(a, s, p) \wedge \mathrm{prefix}(a, s, i, l - 1) \wedge \neg\mathrm{prefix}(a, s, i, l)$
@ $\forall p \in \{1, \dots, i - 1\} \,.\, \neg\mathrm{contains}(a, s, p) \wedge$
 $[l > r \Rightarrow \mathrm{contains}(a, s, i)] \wedge [l \leq r \Rightarrow \neg\mathrm{contains}(a, s, i)]$
if $l > r$ **then**
  @ $\mathrm{contains}(a, s, i)$
  return i
else
  @ $\forall p \,.\, \neg\mathrm{contains}(a, s, p)$
  return 0

Automatizace nalezení variantů

Terminator

Předpověď přednášek

- Správnost volání funkce, správnost objekt-orientovaných programů
- Automatizace: Rozhodovací procedury

Literature I

A. M. Turing. On computable numbers, with an application to the entscheidungsproblem. *Proceedings of the London Mathematical Society*, s2-42(1):230–265, 1937.