# Formální Metody a Specifikace (LS 2011)
# Přednáška 8:
# Ověření neomezené správnosti programů

Stefan Ratschan

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

8. duben 2011

# Příklad

$r \leftarrow$ **false**
**for** $i \leftarrow 1$ **to** $10$ **do**
    **if** $a[i] = 7$ **then** $r \leftarrow$ **true**
**return** $r$

# Příklad

```
1: r ← false
2: for i ← 1 to 10 do
3:     if a[i] = 7 then r ← true
4: return r
```

$$I \quad :\Leftrightarrow \quad pc = 1$$

# Příklad

```
1: r ← false
2: for i ← 1 to 10 do
3:     if a[i] = 7 then r ← true
4: return r
```

$$I \quad :\Leftrightarrow \quad pc = 1$$

$$O \quad :\Leftrightarrow \quad pc = 4 \Rightarrow \Big[r \Leftrightarrow \big[\exists k \, . \, 1 \leq k \leq 10 \land a[k] = 7\big]\Big]$$

# Zopakování: Operační sémantika

Stav programu je valuací (tj. funkcí která přiřazuje proměnným hodnoty) která

- přiřazuje speciální proměnné *pc* číslo řádku,
- každé proměnné programu hodnotu odpovídajícího typu.

Množina všech stavů $S$.

# Zopakování: Operační sémantika

Stav programu je valuací (tj. funkcí která přiřazuje proměnným hodnoty) která

- přiřazuje speciální proměnné *pc* číslo řádku,
- každé proměnné programu hodnotu odpovídajícího typu.

Množina všech stavů $S$.

Pro stavy $s, s' \in S$, $s \to s'$
pokud program může dělat krok ze stavu $s$ do stavu $s'$
(*přechodová relace*)

# Zopakování: Operační sémantika

Stav programu je valuací (tj. funkcí která přiřazuje proměnným hodnoty) která

- přiřazuje speciální proměnné $pc$ číslo řádku,
- každé proměnné programu hodnotu odpovídajícího typu.

Množina všech stavů $S$.

Pro stavy $s, s' \in S$, $s \rightarrow s'$
pokud program může dělat krok ze stavu $s$ do stavu $s'$
(*přechodová relace*)

Místo vstupní/výstupní specifikaci používáme

- podmínku $I$ na počáteční stav (např. $pc = 1 \land x \leq 10$)
- podmínku $O$ specifikující správnost stavů (např. $pc = 7 \Rightarrow x \neq 0$)

# Zopakování: Ověření omezené správnosti programů

Pokud program udělal $n$ kroků, pak výsledek splňuje specifikaci:

# Zopakování: Ověření omezené správnosti programů

Pokud program udělal $n$ kroků, pak výsledek splňuje specifikaci:

Pro každý stav $s$ tak, že $s \models I$,
pro každý stav $s'$ tak, že $s \to^n s'$,
$s' \models O$

# Zopakování: Ověření omezené správnosti programů

Pokud program udělal $n$ kroků, pak výsledek splňuje specifikaci:

Pro každý stav $s$ tak, že $s \models I$,
pro každý stav $s'$ tak, že $s \rightarrow^n s'$,
$s' \models O$

Jako formule v predikátové logice (po zjednodušení):

$$\neg \exists v_1, \ldots, v_n \,.\, I[v \leftarrow v_1] \wedge \bigwedge_{i=1,\ldots,n-1} \Phi_P[v \leftarrow v_i, v' \leftarrow v_{i+1}] \wedge \neg O[v \leftarrow v_n]$$

# Zopakování: Ověření omezené správnosti programů

Pokud program udělal $n$ kroků, pak výsledek splňuje specifikaci:

Pro každý stav $s$ tak, že $s \models I$,
pro každý stav $s'$ tak, že $s \rightarrow^n s'$,
$s' \models O$

Jako formule v predikátové logice (po zjednodušení):

$$\neg\exists v_1, \dots, v_n \,.\, I[v \leftarrow v_1] \wedge \bigwedge_{i=1,\dots,n-1} \Phi_P[v \leftarrow v_i, v' \leftarrow v_{i+1}] \wedge \neg O[v \leftarrow v_n]$$

Protipříklad (counter-example), chybná stopa (error trace),
chybná trajektorie (error trajectory).

# Neomezená správnost

Chceme dokázat že

pro každý stav $s$ tak, že $s \models I$,

pro každý stav $s'$ tak, že $s \rightarrow^{*} s'$

$s' \models O$

# Neomezená správnost

Chceme dokázat že

pro každý stav $s$ tak, že $s \models I$,

pro každý stav $s'$ tak, že $s \rightarrow^{*} s'$

$s' \models O$

Zobrazení všech výpočtů určitého programu:

*Výpočetní strom* (tj. les):

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

# Neomezená správnost

Chceme dokázat že

pro každý stav $s$ tak, že $s \models I$,

pro každý stav $s'$ tak, že $s \rightarrow^* s'$

$s' \models O$

Zobrazení všech výpočtů určitého programu:

*Výpočetní strom* (tj. les):

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

Nekonečná délka cest, (ne)determinismus,

nekonečný počet hran z jednotlivých uzlů.

# Neomezená správnost

Chceme dokázat že

pro každý stav $s$ tak, že $s \models I$,

pro každý stav $s'$ tak, že $s \rightarrow^* s'$

$s' \models O$

Zobrazení všech výpočtů určitého programu:

*Výpočetní strom* (tj. les):

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

Nekonečná délka cest, (ne)determinismus, nekonečný počet hran z jednotlivých uzlů.

Chceme dokázat že pro každý uzel $s$ tohoto stromu, $s \models O$

# Neomezená správnost

Chceme dokázat že

pro každý stav $s$ tak, že $s \models I$,

pro každý stav $s'$ tak, že $s \rightarrow^* s'$

$s' \models O$

Zobrazení všech výpočtů určitého programu:

*Výpočetní strom* (tj. les):

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

Nekonečná délka cest, (ne)determinismus,
nekonečný počet hran z jednotlivých uzlů.

Chceme dokázat že pro každý uzel $s$ tohoto stromu, $s \models O$

Takovou formuli $O$ také nazýváme *invariantem*

# Důkazy neomezené správnosti

Indukce (*Strukturální indukce* přes výpočetní strom):

# Důkazy neomezené správnosti

Indukce (*Strukturální indukce* přes výpočetní strom): Dokážeme:

- Pro každý kořen $s$ výpočetního stromu $s \models O$

# Důkazy neomezené správnosti

Indukce (*Strukturální indukce* přes výpočetní strom): Dokážeme:

- Pro každý kořen $s$ výpočetního stromu $s \models O$
- Pro každý uzel $s$ pro který $s \models O$,
  pro každé dítě $s'$ tohoto uzlů, $s' \models O$.

# Důkazy neomezené správnosti

Indukce (*Strukturální indukce* přes výpočetní strom): Dokážeme:

- Pro každý kořen $s$ výpočetního stromu $s \models O$
- Pro každý uzel $s$ pro který $s \models O$,
  pro každé dítě $s'$ tohoto uzlů, $s' \models O$.

Jinak řečeno, tj. po substituci definice výpočetního stromu:

- Pro každý stav $s$, pokud $s \models I$ pak $s \models O$
- Pro každý stav $s, s'$, pokud $s \models O$ a $s \rightarrow s'$, pak $s' \models O$

# Důkazy neomezené správnosti

Indukce (*Strukturální indukce* přes výpočetní strom): Dokážeme:

- Pro každý kořen $s$ výpočetního stromu $s \models O$
- Pro každý uzel $s$ pro který $s \models O$,
  pro každé dítě $s'$ tohoto uzlů, $s' \models O$.

Jinak řečeno, tj. po substituci definice výpočetního stromu:

- Pro každý stav $s$, pokud $s \models I$ pak $s \models O$
- Pro každý stav $s, s'$, pokud $s \models O$ a $s \rightarrow s'$, pak $s' \models O$

Překlad do predikátové logiky:

- $\models \forall r \,.\, I \Rightarrow O$
- $\models \forall r, r' \,.\, [O \wedge \Phi_P] \Rightarrow O[r \leftarrow r']$

přičemž $r$ stoji pro všechno programové proměnný včetně $pc$,
a $r'$ pro jejich čárkovanou verzi.

# Podmínky induktivity

- $\models \forall r \,.\, I \Rightarrow O$
- $\models \forall r, r' \,.\, [O \wedge \Phi_P] \Rightarrow O[r \leftarrow r']$

# Podmínky induktivity

- $\models \forall r \,.\, I \Rightarrow O$
- $\models \forall r, r' \,.\, [O \wedge \Phi_P] \Rightarrow O[r \leftarrow r']$

Intuice na základě množin

# Podmínky induktivity

- $\models \forall r \, . \, I \Rightarrow O$
- $\models \forall r, r' \, . \, [O \wedge \Phi_P] \Rightarrow O[r \leftarrow r']$

Intuice na základě množin

Můžeme v rozhodnutelných teoriích můžeme automaticky dokázat

# Podmínky induktivity

- $\models \forall r\ .\ I \Rightarrow O$
- $\models \forall r, r'\ .\ [O \wedge \Phi_P] \Rightarrow O[r \leftarrow r']$

Intuice na základě množin

Můžeme v rozhodnutelných teoriích můžeme automaticky dokázat

Tj., v rozhodnutelných teoriích můžeme
automaticky dokázat neomezenou správnost!?

# Příklad

```
1: r ← false
2: for i ← 1 to 10 do
3:     if a[i] = 7 then r ← true
4: return r
```

$$I \quad :\Leftrightarrow \quad pc = 1$$

$$O \quad :\Leftrightarrow \quad pc = 4 \Rightarrow \Big[ r \Leftrightarrow \big[ \exists k \,.\, 1 \leq k \leq 10 \wedge a[k] = 7 \big] \Big]$$

# Příklad

```
1:  r ← false
2:  for i ← 1 to 10 do
3:      if a[i] = 7 then r ← true
4:  return r
```

$$I \quad :\Leftrightarrow \quad pc = 1$$

$$O \quad :\Leftrightarrow \quad pc = 4 \Rightarrow \Big[ r \Leftrightarrow \big[ \exists k \;.\; 1 \leq k \leq 10 \land a[k] = 7 \big] \Big]$$

Podmínky induktivity:

- Pro každý stav $s$, pokud $s \models I$ pak $s \models O$
- Pro každý stav $s, s'$, pokud $s \models O$ a $s \to s'$, pak $s' \models O$

# Induktivní verifikace bezpečnosti

Naše překlady nebyly ekvivalence? Kde jsme něco ztratili?

# Induktivní verifikace bezpečnosti

Naše překlady nebyly ekvivalence? Kde jsme něco ztratili?

Intuice na základě množin

# Induktivní verifikace bezpečnosti

Naše překlady nebyly ekvivalence? Kde jsme něco ztratili?

Intuice na základě množin

$O$ sice je invariantem, ale
nemůžeme tuto skutečnost dokázat našimi podmínkami induktivity

# Induktivní verifikace bezpečnosti

Naše překlady nebyly ekvivalence? Kde jsme něco ztratili?

Intuice na základě množin

$O$ sice je invariantem, ale
nemůžeme tuto skutečnost dokázat našimi podmínkami induktivity

Jinak řečeno: $O$ sice je invariantem ale není *induktivním invariantem*.

# Induktivní verifikace bezpečnosti

Naše překlady nebyly ekvivalence? Kde jsme něco ztratili?

Intuice na základě množin

$O$ sice je invariantem, ale
nemůžeme tuto skutečnost dokázat našimi podmínkami induktivity

Jinak řečeno: $O$ sice je invariantem ale není *induktivním invariantem*.

Co dělat?

# Induktivní verifikace bezpečnosti

Naše překlady nebyly ekvivalence? Kde jsme něco ztratili?

Intuice na základě množin

$O$ sice je invariantem, ale
nemůžeme tuto skutečnost dokázat našimi podmínkami induktivity

Jinak řečeno: $O$ sice je invariantem ale není *induktivním invariantem*.

Co dělat?

Zkusíme najít jinou formuli $V$ tak, že

- $\models \forall r \,.\, V \Rightarrow O$, a navíc
- $V$ je induktivním invarianten, tj. splňuje podmínky induktivity

# Induktivní verifikace bezpečnosti

Naše překlady nebyly ekvivalence? Kde jsme něco ztratili?

Intuice na základě množin

$O$ sice je invariantem, ale
  nemůžeme tuto skutečnost dokázat našimi podmínkami induktivity

Jinak řečeno: $O$ sice je invariantem ale není *induktivním invariantem*.

Co dělat?

Zkusíme najít jinou formuli $V$ tak, že

- $\models \forall r \,.\, V \Rightarrow O$, a navíc
- $V$ je induktivním invarianten, tj. splňuje podmínky induktivity

Příklad

# Automatizace

Důkaz induktivních podmínek lze částečně dělat automaticky.

Ale: Potřebujeme induktivní invariant

# Automatizace

Důkaz induktivních podmínek lze částečně dělat automaticky.

Ale: Potřebujeme induktivní invariant

Automatizace nalezení induktivních invariant

- těžký problém
- současný výzkum (viz. `http://www.absint.com/astree/`)

# Automatizace

Důkaz induktivních podmínek lze částečně dělat automaticky.

Ale: Potřebujeme induktivní invariant

Automatizace nalezení induktivních invariant

- těžký problém
- současný výzkum (viz. `http://www.absint.com/astree/`)

Existuje vždy

- invariant
- pro každý invariant $O$, induktivní invariant $V$ tak, že $V \Rightarrow O$?

# Úplnost

**Theorem**

*Pokud $V$ je formulí tak, že*
*pro každý stav $s$, $s \models V$ přesně když*
*existuje stav $s_0$ tak, že $s_0 \models I$ a $s_0 \to^* s$,*
*pak je $V$ induktivním invariantem.*

# Úplnost

## Theorem

*Pokud $V$ je formulí tak, že*
*pro každý stav $s$, $s \models V$ přesně když*
*existuje stav $s_0$ tak, že $s_0 \models I$ a $s_0 \rightarrow^* s$,*
*pak je $V$ induktivním invariantem.*

**Důkaz**: Předpokládáme že pro každý stav $s$, $s \models V$ přesně když existuje $s_0$ tak, že $s_0 \models I$ a $s_0 \rightarrow^* s$. Musíme dokázat že $V$ splňuje podmínky induktivity:

- Pro každý stav $s$, pokud $s \models I$ pak $s \models V$: Nechť $s$ je libovolný pevný stav tak, že $s \models I$. Dokážeme že i $s \models V$ tj. dokážeme že existuje stav $s_0$ tak, že $s_0 \models I$ a $s_0 \rightarrow^* s$. To platí pro volbu $s_0 \leftarrow s$.
- Pro každý stav $s, s'$, pokud $s \models V$ a $s \rightarrow s'$, pak $s' \models V$. Nechť $s$, $s'$ jsou libovolné pevné stavy tak, že $s \models V$ a $s \rightarrow s'$. Dokážeme, že $s' \models V$. Kvůli $s \models V$ víme že existuje $s_0$ tak, že $s_0 \models I$ a $s_0 \rightarrow^* s$. Z $s_0 \rightarrow^* s$ a $s \rightarrow s'$ plyne že $s_0 \rightarrow^* s'$, a kvůli tomu $s' \models V$.

$\square$

# Závěr

Indukce je k něčemu!

# Závěr

Indukce je k něčemu!

Pomoci indukce můžeme
ověřit nekonečný počet cest nekonečné délky!

# Závěr

Indukce je k něčemu!

Pomoci indukce můžeme

ověřit nekonečný počet cest nekonečné délky!

Příště: Strategie pro nalezení induktivních invariant, terminace