INF05516 - Semântica formal N
Ciência da Computação - UFRGS
2006-2

Marcus Ritt
mrpritt@inf.ufrgs.br

14/03/2006

Agenda

Última aula:

- Semântica operacional natural de uma linguagem pequena

Hoje:

- A base de raciocínio formal: Provas
- Aplicações da semântica: Características de IMP e de programas

Equivalências: Notação

Lembre-se de $\mathbf{a} \sim \mathbf{a}'$?

$$\forall n \in \mathbb{Z}, \sigma \in \Sigma : \mathbf{a}, \sigma \Downarrow n \leftrightarrow \mathbf{a}', \sigma \Downarrow n.$$

Da mesma maneira podemos definir

$$\mathbf{b} \sim \mathbf{b}' : \forall t \in \{\text{true}, \text{false}\}, \sigma \in \Sigma : \mathbf{b}, \sigma \Downarrow t \leftrightarrow \mathbf{b}', \sigma \Downarrow t$$
$$\mathbf{c} \sim \mathbf{c}' : \forall \sigma \in \Sigma, \sigma' \in \Sigma : \mathbf{c}, \sigma \Downarrow \sigma' \leftrightarrow \mathbf{c}', \sigma \Downarrow \sigma'$$

Motivação

Queremos raciocinar sobre as linguagens é provar propriedades deles:

- A avaliação é determinístico (uma expressão tem um único valor)?
- A avaliação é total (cada expressão tem um valor)?
- O laço `while b do c` é equivalente a `if b then (c; while b do c) else skip`?

Mas: para isso precisamos técnicas de prova!

Indução natural

Para provar uma proposição $P(n)$ sobre $\mathbb{N}$

1. Base: Prova que $P(0)$
2. Passo: Prova que $P(n) \to P(n+1)$

ou em breve

$$\forall n \in \omega . P(n) \leftrightarrow P(0) \wedge P(n) \to P(n+1)$$

Exemplo $P(n) = \left(\sum_{0 \leq i \leq n} i^2 = n(n+1/2)(n+1)/3\right)$:

1. Base: $P(0) = \left(\sum_{0 \leq i \leq 0} i^2 = 0(0+1/2)(0+1)/3\right)$
2. Passo: Supõe $P(n)$.

$$\sum_{0 \leq i \leq n+1} i^2 = \sum_{0 \leq i \leq n} i^2 + (n+1)^2 =$$
$$n(n+1/2)(n+1)/3 + (n+1)^2 = (n+1)(n+3/2)(n+2)/3.$$

Logo $P(n+1)$.

Indução bem fundada

Suponha um conjunto C com uma relação

$$\prec \subseteq C \times C$$

tal que não tem cadeias descendentes infinitas

$$\cdots \prec c_n \prec c_{n-1} \prec \cdots \prec c_1 \prec c_0$$

$\prec$ se chama *bem fundada*. Por exemplo $<$ sobre $\mathbb{N}$ é bem fundada (mas não sobre $\mathbb{Z}$!). Uma relação bem fundada permite o seguinte princípio de indução bem fundada:

$$\forall c \in C.P(c) \leftrightarrow \forall c \in C.\,(\forall b \in C.b \prec c.P(b)) \rightarrow P(c)$$

Observa: Com $\prec = \{(n, n+1) | n \in \mathbb{N}\}$ obtemos o princípio de indução natural!

Emmy Noether
(*1882, +1935)

Definições indutivas

Lembre-se da definição de expressões aritméticas?

$$\mathbf{a} ::= \mathbf{n} | \mathbf{x} | \mathbf{a}\text{+}\mathbf{a}' | \mathbf{a}\text{–}\mathbf{a}' | \mathbf{a}\times\mathbf{a}'.$$

É uma definição indutiva do conjunto Aexp:

1. Base
   - $\forall n \in \mathrm{Int} : n \in \mathrm{Aexp}$
   - $\forall l \in \mathrm{Ident} : l \in \mathrm{Aexp}$
2. Passo
   - $a \in \mathrm{Aexp} \wedge a' \in \mathrm{Aexp} \rightarrow a + a' \in \mathrm{Aexp}$
   - $a \in \mathrm{Aexp} \wedge a' \in \mathrm{Aexp} \rightarrow a - a' \in \mathrm{Aexp}$
   - $a \in \mathrm{Aexp} \wedge a' \in \mathrm{Aexp} \rightarrow a \times a' \in \mathrm{Aexp}$
3. Nada mais é in Aexp.

Semântica da definição indutiva

- Queremos uma solução que é fechado: se $X \subseteq A$ e as regras permitem concluir c de X, então $c \in A$.
- Mas não é suficiente! Queremos uma solucão mínima...

Regras permitem dar uma semântica formal à definição indutiva. Exemplo:

$$\frac{}{n \in \text{Aexp}}\, n \in \text{Int}$$

$$\frac{}{l \in \text{Aexp}}\, l \in \text{Ident}$$

$$\frac{a \in \text{Aexp} \qquad a' \in \text{Aexp}}{a + a' \in \text{Aexp}}$$

$$\ldots$$

Semântica da definição indutiva...

Seja R um conjunto de regras e

$$\hat{R}(C) = \{c | \exists (P/c) \in R, P \subseteq C\}.$$

Um conjunto C é *fechado* (com respeito a R) se $\hat{R}(C) \subseteq C$. Consideramos

$$I_R = \bigcap \{Q | Q \text{ é fechado}\}$$

I_R existe porque existe, por exemplo, o conjunto fechado

$$\{c | \exists (P/c) \in R\}$$

e, seguinda a definição do I_R é o conjunto fechado mínimo

$$\forall Q.Q \text{ é fechado}.I_R \subseteq Q.$$

Indução estrutural

Como provar alguma proposição sobre Aexp?
Usa a indução bem fundada com a relação $\prec_1$:

$$(\mathbf{a}, \mathbf{a}') \in \prec_1 \leftrightarrow \mathbf{a} \text{ é uma subexpressão imediata de } \mathbf{a}'.$$

Por que funciona? $\prec_1$ é bem-fundada porque sub-expressões são mais curtos.
Então, o princípio da indução bem fundada resulta em:

$$\begin{aligned} \forall a \in \mathrm{Aexp}.P(a) \quad \leftrightarrow \quad & \forall n \in \mathrm{Int}.P(n) \wedge \\ & \forall x \in \mathrm{Ident}.P(x) \wedge \\ & \forall a = a_1 + a_2 : P(a_1) \wedge P(a_2) \rightarrow P(a) \wedge \\ & \forall a = a_1 - a_2 : P(a_1) \wedge P(a_2) \rightarrow P(a) \wedge \\ & \forall a = a_1 \times a_2 : P(a_1) \wedge P(a_2) \rightarrow P(a) \end{aligned}$$

Exemplo: Expressões aritméticas

Seja a propriedade $P(a) =$"o número dos operadores sempre é menos um que o número dos argumentos (números inteiros, locais)".

$n \in \mathrm{Int}$ A expressão tem um argumento e nenhum operador.
$x \in \mathrm{Ident}$ A expressão tem um argumento e nenhum operador.
$a = a_1 + a_2$ Suponha que a_1 tem n_1 operadores e $n_1 + 1$ argumentos e a_2 tem n_2 operadores e $n_2 + 1$ argumentos (hipótese). Então a tem $n_1 + n_2 + 1$ operadores e $n_1 + n_2 + 2$ argumentos.
(O resto de casos e similar).

Valor das provas

- A semântica nos dá as regras formais
- Ela nos permite *provar* caraterísticas
  - dos programas individuais
    O programa está correto?
  - da uma linguagem
    IMP é determinístico?
- As provas frequentemente usam indução.

Exemplo: Um laço

Suponha

$$\mathbf{w} \equiv \textbf{while } \mathrm{x}{<}6 \textbf{ do } \mathrm{x}{:=}\mathrm{x}{+}1$$

Nos queremos provar

$$\sigma(x) \leq 6 \rightarrow \mathbf{w}, \sigma \Downarrow \sigma[x \mapsto 6].$$

Seja

$$P(n) = (\sigma(x) = 6 - n \rightarrow \mathbf{w}, \sigma \Downarrow \sigma[x \mapsto 6])$$

Exemplo: Um laço...

1. Base: $P(0) = (\sigma(x) = 6 \to \mathtt{w}, \sigma \Downarrow \sigma[x \mapsto 6])$. Suponhando $\sigma(x) = 6$ temos $\sigma = \sigma[x \mapsto 6]$ e

$$\dfrac{\dfrac{\mathtt{x}, \sigma \Downarrow 6 \qquad 5, \sigma \Downarrow 5}{\mathtt{x{<}5}, \sigma \Downarrow \text{false}}}{\mathtt{w}, \sigma \Downarrow \sigma}\ \text{while}$$

2. Passo: Temos $n \geq 0$ é $P(n)$. Suponha $\sigma(x) = 6 - (n+1)$

$$\dfrac{\dfrac{\mathtt{x}, \sigma \Downarrow 6-(n+1) \qquad \cdots}{\mathtt{x{\leq}5}, \sigma \Downarrow \text{true}} \qquad \dfrac{\mathtt{x:=x+1}, \sigma \Downarrow \sigma[x \mapsto 6-n] \qquad \mathtt{w}, \sigma[x \mapsto 6-n] \Downarrow \sigma[x \mapsto 6]}{\mathtt{x:=x+1;w}, \sigma \Downarrow \sigma[x \mapsto 6]}}{\mathtt{w}, \sigma \Downarrow \sigma[x \mapsto 6]}$$