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

Marcus Ritt
mrpritt@inf.ufrgs.br

04/10/2006

## Introdução



### Agenda

Última aula:

- Introdução à semântica axiomática.

Hoje:

- Semântica axiomática: Condicional, laços. Exemplos.



## O condicional



### Trabalhar com o condicional

- Começando com a pós-condição, cada alternativa leva para uma pré-condição $\Phi_1$, $\Phi_2$.
- Logo, se a pré-condição do condicional implica $b \to \Phi_1$ e $\neg b \to \Phi_2$ conseguimos uma prova (porque?)

$$\{\Phi\}$$
$$\{b \to \Phi_1 \wedge \neg b \to \Phi_2\}$$
```
if b then (
```
$$\{\Phi_1\}$$
$$\cdots$$
$$\{\Psi\}$$
```
) else (
```
$$\{\Phi_2\}$$
$$\cdots$$
$$\{\Psi\}$$
```
)
```
$$\{\Psi\}$$

## Exemplo

**Entrada** $x$
**Pré-condição** $\text{true}$
**Saida** $y$
**Pós-condição** $y = x + 1.$

```
a := x+1;
if (a-1=0) then
  y := 1
else
  y := a
```



## Exemplo...

Prova?

$$\{\text{true}\}$$
$$\{x = 0 \to x = 0 \land \neg(x = 0) \to 0 = 0\}$$
$$\{x + 1 - 1 = 0 \to 1 = x + 1 \land \neg(x + 1 - 1 = 0) \to x + 1 = x + 1\}$$
```
a := x+1
```
$$\{a - 1 = 0 \to 1 = x + 1 \land \neg(a - 1 = 0) \to a = x + 1\}$$
```
if (a-1=0) then (
```
$$\{1 = x + 1\}$$
```
y := 1
```
$$\{y = x + 1\}$$
```
) else (
```
$$\{a = x + 1\}$$
```
y := a
```
$$\{y = x + 1\}$$
```
)
```
$$\{y = x + 1\}$$

## Condição

**Entrada** $x$
**Pré-condição** true
**Saida** $x, y$
**Pós-condição** ?

```
if (x>0) then (
  y := 1
) else (
  x := 0-x
)
```



## Exemplo...

Prova?

$$\{x = n\}$$
$$\{(x > 0 \to x > 0) \land (x \leq 0 \to (x \leq 0 \land x = n))\}$$
`if x>0 then (`
$$\{x > 0\}$$
$$\{x \geq 0 \land (n > 0 \to 1 = 1)\}$$
`y := 1`
$$\{x \geq 0 \land (n > 0 \to y = 1)\}$$
`) else (`
$$\{x \leq 0 \land x = n\}$$
$$\{x \leq 0 \land (n > 0 \to y = 1)\}$$
$$\{0 - x \geq 0 \land (n > 0 \to y = 1)\}$$
`x := 0-x`
$$\{x \geq 0 \land (n > 0 \to y = 1)\}$$
`)`
$$\{x \geq 0 \land (n > 0 \to y = 1)\}$$

## Trabalhar com o laço

$$\frac{\{\eta \wedge b\}\mathbf{c}\{\eta\}}{\{\eta\}\texttt{while b do c}\{\eta \wedge \neg b\}}\ \text{while}$$

- $\Phi$ é a *invariante* do laço.
- Para provar

$$\{\Phi\}\texttt{while b do c}\{\Psi\}$$

  temos que achar uma invariante tal que

$$\vdash \Phi \to \eta \quad \{\eta\}\texttt{while b do c}\{\eta \wedge \neg b\} \quad \vdash \eta \wedge \neg b \to \Psi.$$

- Achar a invariante precisa criatividade e entendimento do laço ("entender um laço significa conhecer a invariante").
- As vezes um *trace* da execução do programa ajuda.



## A invariante trivial

- O que acontece, se escolhemos $\eta = \text{true}$?
- $\text{true}$ sempre é satisfeito!
- Obtemos a pós-condição trivial:

$$\frac{\{b\}\mathbf{c}\{\text{true}\}}{\{\text{true}\}\texttt{while b do c}\{\neg b\}}\ \text{while}$$

## Exemplo: Fatorial

**Entrada** $x$
**Pré-condição** $x \geq 0 \wedge x = n$
**Saida** $y$
**Pós-condição** $y = n!$

```
y := 1
while ¬(x=0) do
  y := y × x;
  x := x − 1
```



## Exemplo...

Finalmente, vamos provar nosso exemplo do inicio!

$$\{x = n \wedge x \geq 0\}$$
$$\{x! = n! \wedge x \geq 0\}$$

```
y := 1;
```

$$\{yx! = n! \wedge x \geq 0\}$$

```
while ¬(x=0) do (
```

$$\{yx! = n! \wedge x > 0\}$$

```
y := y*x;
```

$$\{y(x-1)! = n! \wedge x > 0\}$$

```
x := x-1
```

$$\{yx! = n! \wedge x \geq 0\}$$

```
)
```

$$\{yx! = n! \wedge x \geq 0 \wedge x = 0\}$$
$$\{y = n!\}$$

## Exemplo: Collatz

**Entrada** $x$
**Pré-condição** $x \geq 0$
**Saida** $x$
**Pós-condição** $x = 1$

```
C ≡
while ¬(x=1) do (
  y:=2; z:=1;
  while y < x do ( y:=y+2; z:=z+1 );
  if (y = x) then (
    x := z
  ) else (
    x := 3*x+1
  )
)
```



## Exemplo...

Um caso para a invariante trivial!

$$\{\text{true}\}$$

```
while ¬(x=1) do (
...
)
```

$$\{x = 1\}$$

## Exemplo: Parte do Collatz

Divisão inteira por dois:

**Entrada** $x$
**Pré-condição** $x > 0$
**Saida** $y, z$
**Pós-condição** $?$

```
y:=2;
z:=1;
while y < x do (
  y:=y+2; z:=z+1
)
```

Trace:

| x | y | z |
|---|---|---|
| 11 | - | - |
| 11 | 2 | 1 |
| 11 | 4 | 2 |
| 11 | 6 | 3 |
| 11 | 8 | 4 |
| 11 | 10 | 5 |
| 11 | 12 | 6 |



## Exemplo...

Invariante: $y = 2z \wedge y < x + 2$.

$$\{x > 0\}$$
$$\{2 = 2 \wedge 2 < x + 2\}$$
`y:=2;`
$$\{y = 2 \wedge y < x + 2\}$$
`z:=1;`
$$\{y = 2z \wedge y < x + 2\}$$
`while y<x do (`
$$\{y = 2z \wedge y < x\}$$
$$\{y + 2 = 2(z + 1) \wedge y + 2 < x + 2\}$$
`y:=y+2;`
$$\{y = 2(z + 1) \wedge y < x + 2\}$$
`z:=z+1`
$$\{y = 2z \wedge y < x + 2\}$$
`)`
$$\{y = 2z \wedge x \leq y \wedge y < x + 2\}$$
$$\{y = 2z \wedge (y = x \vee y = x + 1)\}$$
$$\{z = \lfloor x/2 \rfloor\}$$

## Exemplo: Multi

**Entrada** $x, y$
**Pré-condição** $y \geq 0$
**Saida** $z$
**Pós-condição** $z = xy$

```
a := 0;
z := 0;
while ¬(a=y) do (
   z := z + x;
   a := a + 1
)
```



## Exemplo...

Invariante: $z = ax$.

$\{y \geq 0\}$
$\{0 = 0\}$
`a:=0;`
$\{0 = ax\}$
`z:=0;`
$\{z = ax\}$
`while ¬(a=y) do`
$\{z = ax \wedge a \neq y\}$
$\{z = ax\}$
$\{z + x = (a+1)x\}$
`z:=z+x`
$\{z = (a+1)x\}$
`a := a+1`
$\{z = ax\}$`)`
$\{a = y \wedge z = ax\}$
$\{z = xy\}$