CS 4110 - 9/26/25
Lab # 14 - Axiomatic Semantics

We have two relations involving partial correctness statements

1) $\models \{P\}\ c\ \{Q\}$
2) $\vdash \{P\}\ c\ \{Q\}$

How do they relate to each other?

Theorem [Soundness]
If $\vdash \{P\}\ c\ \{Q\}$ then $\models \{P\}\ c\ \{Q\}$

Proof By induction...

Theorem* [Completeness]
If $\models \{P\}\ c\ \{Q\}$ then $\vdash \{P\}\ c\ \{Q\}$

But, notice that consequence forces us to show validity of assertions...

For example, consider $\{true\}$ skip $\{P\}$.

More on this next Monday...

# Annotated programs

$$\frac{}{\vdash \{P\}\ \mathrm{skip}\ \{P\}}$$

```
{P}
skip
{P}
```

$$\frac{\vdash \{P\}\ c_1\ \{R\} \qquad \vdash \{R\}\ c_2\ \{Q\}}{\vdash \{P\}\ c_1 ; c_2\ \{R\}}$$

```
{P}
c1;
{R}
c2
{Q}
```

$$\frac{}{\vdash \{P[a/x]\}\ x := a\ \{P\}}$$

```
{P[a/x]}
x:=a
{P}
```

$$\frac{\vdash \{P \land b\}\ c_1\ \{Q\} \qquad \vdash \{P \land \neg b\}\ c_2\ \{Q\}}{\vdash \{P\}\ \mathrm{if}\ b\ \mathrm{then}\ c_1\ \mathrm{else}\ c_2\ \{Q\}}$$

```
{P}
if b then
   {P∧b}
   c1
   {Q}
else {P∧¬b}
   c2
   {Q}
```

$$\frac{\vdash \{P \land b\}\ c\ \{P\}}{\vdash \{P\}\ \mathrm{while}\ b\ \mathrm{do}\ c\ \{P \land \neg b\}}$$

```
{P}
while b do
   {P∧b}
   c
   {P}
{P∧¬b}
```

$$\frac{\vDash P \Rightarrow P' \qquad \vdash \{P'\}\, c\, \{Q\}}{\vdash \{P\}\, c\, \{Q\}}$$

$\{P\} \Rightarrow$
$\{P'\}$
$c$
$\{Q\}$

Can also omit further annotations when clear from context!

## Example

$\boxed{I = x+y=m+n \wedge y \geq 0}$

$\{x=m \wedge y=n \wedge 0 \leq n\} \Rightarrow$
$\{I\}$
while $y>0$ do (
  $\{I \wedge y>0\} \Rightarrow$
  $\{x+1+y-1=m+n \wedge 0 \leq y-1\}$
  $x:=x+1;$
  $\{x+y-1=m+n \wedge 0 \leq y-1\}$
  $y:=y-1;$
  $\{x+y=m+n \wedge 0 \leq y\} = I$
)
$\{I \wedge \neg(y>0)\} \Rightarrow$
$\{I \wedge y=0\} \Rightarrow$
$\{x=m+n\}$

If we replace the While rule with this one,

$$\frac{\vdash \{P\}\ c\ \{P\}}{\vdash \{P\}\ \text{while } b \text{ do } c\ \{P \land \neg b\}}$$

What do we lose? (If anything?)

<u>Counterexample</u>

$$\{x \geq 0\}\ \text{while } x > 0 \text{ do } x := x-1\ \{x = 0\}$$

would need

$$\{x \geq 0\}\ x := x-1\ \{x \geq 0\}$$

which is not valid!

---

$\boxed{I = 2*s = i*(i+1) \land i \leq x \land x = n}$

Example: Gauss's summation formula.

$\{x = n \land n \geq 0\} \Rightarrow$
$\{2*0 = 0*(0+1) \land 0 \leq x \land x = n\}$
$s := 0;$
$i := 0$
$\{2*s = i*(i+1) \land i \leq x \land x = n\}$
while $i < x$ do (
  $\{2*s = i*(i+1) \land i \leq x \land x = n \land i < x\} \Rightarrow$
  $\{2*(s+i) = (i+1)*(i+1+1) \land i+1 \leq x \land x = n\}$
  $s := s+i;$
  $i := i+1$
  $\{2*s = i*(i+1) \land i \leq x \land x = n\}$
)
$\{2*s = i*(i+1) \land i \leq x \land x = n \land \neg(i < x)\} \Rightarrow$
$\{2*s = n*(n+1)\}$