Writing proofs

Proof trees:

$$\frac{\dfrac{}{\text{Premise}_1}\ \text{axiom} \quad \dfrac{}{\text{Premise}_2}\ \text{axiom}}{\text{Conclusion}}$$

Ex.

$$\frac{\dfrac{}{x=y \Rightarrow x+1=y+1}\ \text{axiom} \quad \dfrac{}{\vdash \{x+1=y+1\}\ x := x+1\ \{x=y+1\}}\ \text{Assign} \quad \dfrac{}{\vdash \{x=y+2-1\}\ y := y+2\ \{x=y-1\}}\ \text{Assign}}{\vdash \{x=y\}\ x := x+1;\ y := y+2\ \{x=y-1\}}$$

$$\frac{\dfrac{}{\vdash \{T\}\ x := 1\ \{x=1\}}\ \text{Assign} \quad \dfrac{}{T \Rightarrow 1=1}\ \text{axiom} \quad \dfrac{}{\vdash \{x=1\}\ z := 1\ \{z=1\}}\ \text{Assign} \quad \dfrac{}{\vdash \{x>0\}\ \text{if} \ldots\ \{z=1\}}}{\vdash \{T\}\ x := 1;\ \text{if } x>0 \{z:=1\} \text{ else } \{z:=0\}\ \{z=1\}}$$

$$\frac{\vdash \{p\}\ S\ \{q\} \quad p' \Rightarrow p \quad q \Rightarrow q'}{\vdash \{p'\}\ S\ \{q'\}}\ \text{weaken}$$

Can always make precondition stronger

Can always make postcond weaker

$$\frac{\dfrac{}{\vdash \{1=1\}\ x := 1\ \{x=1\}}\ \text{Assign} \quad \dfrac{}{T \Rightarrow 1=1}\ \text{axiom} \quad \dfrac{}{x=1 \Rightarrow x>0}\ \text{axiom}}{\vdash \{T\}\ x := 1\ \{x>0\}}\ \text{weaken}$$

$$\frac{\dfrac{\dfrac{}{\{1=1\}\ z := 1\ \{z=1\}}\ \text{Assign}}{\{x>0 \wedge x>0\}\ z := 1\ \{z=1\}}\ \text{weaken} \quad \dfrac{}{\{x>0 \wedge x \le 0\}\ z := 0\ \{F\}}\ F}{\{x>0\}\ \text{if } x>0 \{z:=1\} \text{ else } \{z:=0\}\ \{z=1 \vee F\}}\ \text{Weak}$$

$$\frac{\dfrac{}{\vdash \{T\}\ x := 1\ \{x>0\}} \quad \{x>0\}\ \text{if } x>0 \{z:=1\} \text{ else } \{z:=0\}\ \{z=1\}}{\vdash \{T\}\ x := 1;\ \text{if } x>0 \{z:=1\} \text{ else } \{z:=0\}\ \{z=1\}}$$

Alternative Proof styles.
Hilbert-style

1. $\{1=1\}\ x:=1\ \{x=1\}$ Assign
2. $\{T\}\ x:=1\ \{x>0\}$ Weaken 1
3. $\{1=1\}\ z:=1\ \{z=1\}$ Assign
4. $\{x>0 \wedge x>0\}\ z:=1\ \{z=1\}$ Weaken 3
5. $\{F\}\ z:=0\ \{F\}$ Assign
6. $\{x>0 \wedge x\leq 0\}\ z:=0\ \{F\}$ Weaken 5
7. $\{x>0\}$ if $(x>0)$ then $\{z:=1\}$ else $\{z:=0\}$ $\{z=1\}$ If 4,5
8. $\{T\}\ x:=1;$ if ... $\{z=1\}$ Sequence 2,7

Proof Outlines - Annotate the program

```
                                {T} ⇒ {1=1}
x := 1;                         {x=1} ⇒ {x>0}
if (x>0) then {                 {x>0 ∧ x>0} ⇒ {1=1}
z := 1                          {z=1}
} else {                        {x>0 ∧ x≤0} ⇒ {F}
  z := 0                        {F}
}                               {z=1 ∨ F} ⇒ {z=1}
```

$\{T\}$ if $(x>0)$ then $\{y:=1\}$ else $\{y:=2\}$; if $(y>0)$ then $\{z:=1\}$ else $\{z:=0\}$ $\{z=1\}$

1. $\{1>0\}\ y:=1\ \{y>0\}$ Assign
2. $\{2>0\}\ y:=2\ \{y>0\}$ Assign
3. $\{T \wedge x>0\}\ y:=1\ \{y>0\}$ Weaken 1
4. $\{T \wedge x>0\}\ y:=2\ \{y>0\}$ Weaken 2
5. $\{T\}$ if $x>0$ then $\{y:=1\}$ else $\{y:=2\}$ $\{y>0 \vee y>0\}$ If 3, 4
6. $\{1=1\}\ z:=1\ \{z=1\}$ Assign
7. $\{y>0 \wedge y>0\}\ z:=1\ \{z=1\}$ Weaken 6
8. $\{F\}\ z:=0\ \{F\}$ Assign
9. $\{y>0 \wedge y\leq 0\}\ z:=0\ \{F\}$ Weaken 8
10. $\{y>0\}$ if $(y>0)$ then $\{z:=1\}$ else $\{z:=0\}$ $\{z=1 \vee F\}$ If 7, 9
11. $\{y>0\}$ if ... $\{z=1\}$ Weaken 10
12. $\{T\}$ if $(x>0)$ ... $\{y>0\}$ Weaken 5
13. $\{T\}$ if $(x>0)$ ... ; if $(y>0)$ ... $\{z=1\}$ Sequence 12, 11

Alternate rule for if: $$\frac{\{p \wedge e\}\ s_1\ \{q\} \qquad \{p \wedge \neg e\}\ s_2\ \{q\}}{\{p\}\ \text{if } e \text{ then } \{s_1\} \text{ else } \{s_2\}\ \{q\}}$$

Would let us conclude 12 w/o weakening
What if postconditions of s_1 and s_2 don't match? Weaken!

$\{x>0 \wedge y\leq 0\}\ z:=0\ \{z=1\}$ Weaken 9 (b.c. $F \Rightarrow z=1$)

No loss of generality since $q_1 \Rightarrow q_1 \vee q_2$ and $q_2 \Rightarrow q_1 \vee q_2$