Example of Proof: Software Verification Course

Martin Nordio

ETH Zurich, Switzerland
Martin.Nordio@inf.ethz.ch

Abstract

Example of proof

1 First Example

1.1 Source code

```
foo (a, b: INTEGER): INTEGER
    do
      if a > 0 then
        Result := a
      else
        Result := 1
      end
      if b > 0 then
        Result := Result + b
      else
        Result := Result + 1
      end
    ensure
      post1: a > 0  and b > 0 implies Result = a+b
      post2: a <= 0 and b > 0 implies Result = 1+b
      post3: a > 0  and b<=0 implies Result = a+1
      post4: a <= 0 and b<=0 implies Result = 2
    end
```

1.2 Proof Example 1

Let $POST$ be defined as

$$\left\{ \begin{array}{ll} (a > 0 \wedge b > 0 & \Rightarrow Result = a + b) \wedge \\ (a \leq 0 \wedge b > 0 & \Rightarrow Result = 1 + b) \wedge \\ (a > 0 \wedge b \leq 0 & \Rightarrow Result = a + 1) \wedge \\ (a \leq 0 \wedge b \leq 0 & \Rightarrow Result = 2) \wedge \end{array} \right\}$$

$$\dfrac{\dfrac{\dfrac{}{\{a > 0\}\ Result := a\ \{a > 0 \wedge Result = a\}}\ \text{Assig. Rule} \qquad \dfrac{}{\left\{ \begin{array}{l} a > 0 \Rightarrow Result = a \wedge \\ a \leq 0 \Rightarrow Result = 1 \wedge \\ b \leq 0 \end{array} \right\}\ Result := Result + 1\ \left\{ \begin{array}{l} b \leq 0 \wedge\ a > 0 \Rightarrow Result = a + 1 \wedge \\ b < 0 \wedge\ a \leq 0 \Rightarrow Result = 2 \end{array} \right\}}\ \text{Assig. Rule}}{\left\{ \begin{array}{l} a > 0 \Rightarrow Result = a \wedge \\ a \leq 0 \Rightarrow Result = 1 \end{array} \right\}\ if_1\ \left\{ \begin{array}{l} a > 0 \Rightarrow Result = a \wedge \\ a \leq 0 \Rightarrow Result = 1 \end{array} \right\}}\ \text{if Rule}$$

$$\dfrac{\dfrac{\dfrac{}{\{a \leq 0\}\ Result := 1\ \{a \leq 0 \wedge Result = 1\}}\ \text{Assig. Rule} \qquad \dfrac{}{\left\{ \begin{array}{l} a > 0 \Rightarrow Result = a \wedge \\ a \leq 0 \Rightarrow Result = 1 \wedge \\ b < 0 \end{array} \right\}\ Result := Result + b\ \left\{ \begin{array}{l} b > 0 \wedge\ a > 0 \Rightarrow Result = a + b \wedge \\ b > 0 \wedge\ a \leq 0 \Rightarrow Result = 1 + b \end{array} \right\}}\ \text{Assig. Rule}}{\left\{ \begin{array}{l} a > 0 \Rightarrow Result = a \wedge \\ a \leq 0 \Rightarrow Result = 1 \end{array} \right\}\ if_2\ \{POST\}}\ \text{if Rule}$$

$$\dfrac{\{true\}\ if_1 \left\{ \begin{array}{l} a > 0 \Rightarrow Result = a \wedge \\ a \leq 0 \Rightarrow Result = 1 \end{array} \right\} \qquad \left\{ \begin{array}{l} a > 0 \Rightarrow Result = a \wedge \\ a \leq 0 \Rightarrow Result = 1 \end{array} \right\}\ if_2\ \{POST\}}{\{true\}\ if_1; if_2\ \{POST\}}\ \text{comp Rule}$$

2 Second Example: Exceptions

2.1 Source code

```
foo (a, b: INTEGER): INTEGER
    do
      if a > 0 then
        Result := a
      else
        Raise
      end
      if b > 0 then
        Result := Result + b
      else
        Raise
      end
    end
```

2.2 Proof Example 2

Let $POST_N$ be defined as

$$\left\{ \;\; a > 0 \wedge b > 0 \quad \Rightarrow Result = a + b \;\; \right\}$$

Let $POST_E$ be defined as

$$\left\{ \;\; a \leq \vee b \leq 0 \;\; \right\}$$

$$\dfrac{\dfrac{}{\{a \leq 0\} \;\; Raise \;\; \{false \;,\; a \leq 0\}} \text{ Assig. Rule} \qquad \dfrac{\dfrac{}{\{a > 0\} \;\; Result := a \;\; \{a > 0 \wedge Result = a \;,\; false\}} \text{ Assig. Rule} \qquad \dfrac{}{\left\{ \begin{array}{l} a > 0 \Rightarrow Result = a \wedge \\ b \leq 0 \end{array} \right\} \; Raise \;\; \left\{ \;\; false \;,\; a > 0 \wedge \;\; b \leq 0 \;\; \right\}} \text{ Assig. Rule}}{\{true\} \;\; if_1 \;\; \left\{ \;\; a > 0 \Rightarrow Result = a \quad , \; a \leq 0 \right\}} \text{ if Rule} \qquad \dfrac{\dfrac{}{\left\{ \begin{array}{l} a > 0 \Rightarrow Result = a \wedge \\ b < 0 \end{array} \right\} \; Result := Result + b \;\; \left\{ \;\; b > 0 \wedge \;\; a > 0 \Rightarrow Result = a + b \;,\; false \;\; \right\}} \text{ Assig. Rule}}{\left\{ \;\; a > 0 \Rightarrow Result = a \;\; \right\} \;\; if_2 \;\; \{POST_N \;,\; POST_E\}} \text{ if Rule}}{\{true\} \;\; if_1; if_2 \;\; \{POST_N \;,\; POST_E\}} \text{ comp Rul}$$