Example of Proof: Software Verification Course

Martin Nordio

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

2011

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

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

$$\dfrac{\dfrac{\dfrac{}{\{a > 0\}\ \mathit{Result} := a\ \{a > 0 \wedge \mathit{Result} = a\}}\ \text{Assig. Rule} \qquad \dfrac{}{\{a \leq 0\}\ \mathit{Result} := 1\ \{a \leq 0 \wedge \mathit{Result} = 1\}}\ \text{Assig. Rule}}{\{true\}\ \mathit{if}_1 \left\{\begin{array}{l} a > 0 \Rightarrow \mathit{Result} = a \wedge \\ a \leq 0 \Rightarrow \mathit{Result} = 1 \end{array}\right\}}\ \text{if Rule} \qquad \dfrac{\dfrac{}{\left\{\begin{array}{l} a > 0 \Rightarrow \mathit{Result} = a \wedge \\ a \leq 0 \Rightarrow \mathit{Result} = 1 \wedge \\ b \leq 0 \end{array}\right\} \mathit{Result} := \mathit{Result} + 1 \left\{\begin{array}{l} b \leq 0 \wedge\ \ a > 0 \Rightarrow \mathit{Result} = a + 1 \wedge \\ b < 0 \wedge\ \ a \leq 0 \Rightarrow \mathit{Result} = 2 \end{array}\right\}}\ \text{Assig. Rule} \qquad \dfrac{}{\left\{\begin{array}{l} a > 0 \Rightarrow \mathit{Result} = a \wedge \\ a \leq 0 \Rightarrow \mathit{Result} = 1 \wedge \\ b < 0 \end{array}\right\} \mathit{Result} := \mathit{Result} + b \left\{\begin{array}{l} b > 0 \wedge\ \ a > 0 \Rightarrow \mathit{Result} = a + b \wedge \\ b > 0 \wedge\ \ a \leq 0 \Rightarrow \mathit{Result} = 1 + b \end{array}\right\}}\ \text{Assig. Rule}}{\left\{\begin{array}{l} a > 0 \Rightarrow \mathit{Result} = a \wedge \\ a \leq 0 \Rightarrow \mathit{Result} = 1 \end{array}\right\} \mathit{if}_2\ \{POST\}}\ \text{if Rule}}{\{true\}\ \mathit{if}_1; \mathit{if}_2\ \{POST\}}\ \text{comp Rule}$$

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

$$\left\{\ a > 0 \land b > 0 \quad \Rightarrow \mathit{Result} = a + b\ \right\}$$

Let $POST_E$ be defined as

$$\left\{\ a \leq \lor b \leq 0\ \right\}$$

$$\dfrac{\dfrac{\dfrac{}{\{a > 0\}\ \ \mathit{Result} := a\ \ \{a > 0 \land \mathit{Result} = a\ ,\ \mathit{false}\}}\ \text{Assig. Rule} \qquad \dfrac{}{\{a \leq 0\}\ \ \mathit{Raise}\ \ \{\mathit{false}\ ,\ \ a \leq 0\}}\ \text{Assig. Rule}}{\{\mathit{true}\}\ \ \mathit{if}_1\ \ \{\ \ a > 0 \Rightarrow \mathit{Result} = a\quad ,\ \ a \leq 0\}}\ \text{if Rule} \qquad \dfrac{\dfrac{}{\left\{\begin{array}{l} a > 0 \Rightarrow \mathit{Result} = a\ \land \\ b \leq 0 \end{array}\right\}\ \mathit{Raise}\ \ \{\ \ \mathit{false}\ ,\ \ a > 0 \land\ \ b \leq 0\ \ \}}\ \text{Assig. Rule} \qquad \dfrac{}{\left\{\begin{array}{l} a > 0 \Rightarrow \mathit{Result} = a\ \land \\ b < 0 \end{array}\right\}\ \mathit{Result} := \mathit{Result} + b\ \ \{\ \ b > 0 \land\ \ a > 0 \Rightarrow \mathit{Result} = a + b\ ,\ \ \mathit{false}\ \ \}}\ \text{Assig. Rule}}{\{\ \ a > 0 \Rightarrow \mathit{Result} = a\ \ \}\ \ \mathit{if}_2\ \ \{POST_N\ ,\ \ POST_E\}}\ \text{if Rule}}{\{\mathit{true}\}\ \ \mathit{if}_1; \mathit{if}_2\ \ \{POST_N\ ,\ \ POST_E\}}\ \text{comp Rul}$$