Reasoning on programs

The INFDEV Team @ HR

Hogeschool Rotterdam
Rotterdam, Netherlands

Introduction

Lecture topics

- We introduce conditional expressions
- We show how to verify properties on complex expressions

Conditional expressions

Conditional expressions

- Sometimes we can make decisions within an expression
- The general form is `VALUE if CONDITION else VALUE'` ($if_{VCV'}$)
- If the condition is true, then we return `VALUE`, otherwise `VALUE'`

$$\begin{cases} (PC, S) \overset{if_{V \underset{\rightarrow}{C} V'}}{} V & when \quad (PC, S) \overset{C}{\rightarrow} TRUE \\ (PC, S) \overset{if_{V \underset{\rightarrow}{C} V'}}{} V' & when \quad (PC, S) \overset{C}{\rightarrow} FALSE \end{cases}$$

Conditional expressions

Conditional expressions

- `"adult" if age >= 18 else "minor" = ?`
- **Can you guess the results for** `age = 18` and `age = 16`**?**

Conditional expressions

Conditional expressions

- `"adult" if age >= 18 else "minor" = ?`
- **Can you guess the results for** `age = 18` and `age = 16`**?**
- `age = 16`: `"minor"`
- `age = 18`: `"adult"`

Reasoning on programs

Reasoning on programs

- Sometimes we do not know exactly the values of all variables at all times
- The program may be too complex to allow it

Consider a throttle control system.

The throttle may never go under 1000RPM, or the engine stops and everybody dies.
The temperature must be kept under control, or the engine blows up and everybody dies.

```
1 throttle = throttle - 1000 if (temp > 350.0) & (
      throttle > 2500) else throttle
```

The question thus is: **could the code above cause everyone to die?**

throttle	temp
1000..10000	-20.0..400.0

```
1 throttle = throttle - 1000 if (temp > 350.0) & (
      throttle > 2500) else throttle
```

throttle	temp
1000..10000	-20.0..400.0

```
1 throttle = throttle - 1000 if (temp > 350.0) & (
      throttle > 2500) else throttle
```

throttle	temp
?!?!?	-20.0..400.0

Reasoning on programs

Reasoning on programs

- We cannot list all possible combinations of variable values
- We cannot just “hope it works”

Reasoning on programs

Reasoning on programs

- We cannot list all possible combinations of variable values
- We cannot just “hope it works”
- We can reason in terms of conditions on variables

Reasoning on programs

Reasoning on programs

- We partition the state based on the conditional
- `(temp > 350.0) & (throttle > 2500)` generates four states
  - `temp > 350` and `throttle > 2500`
  - `temp <= 350` and `throttle > 2500`
  - `temp > 350` and `throttle <= 2500`
  - `temp <= 350` and `throttle <= 2500`
- We study the semantics on each of these four states

`temp > 350` **and** `throttle > 2500`

throttle	temp
>2500.0 ..10000	>350.0 ..400.0

```
1 throttle = throttle - 1000 if (temp > 350.0) & (
      throttle > 2500) else throttle
```

`temp > 350` **and** `throttle > 2500`

throttle	temp
>2500.0 ..10000	>350.0 ..400.0

```
1 throttle = throttle - 1000 if (temp > 350.0) & (
      throttle > 2500) else throttle
```

throttle	temp
>1500.0..9000.0	>350.0..400.0

`temp <= 350` **and** `throttle > 2500`

throttle	temp
>2500.0..10000	-20.0..350.0

```
1 throttle = throttle - 1000 if (temp > 350.0) & (
      throttle > 2500) else throttle
```

`temp <= 350` **and** `throttle > 2500`

throttle	temp
>2500.0..10000	-20.0..350.0

```
1 throttle = throttle - 1000 if (temp > 350.0) & (
      throttle > 2500) else throttle
```

throttle	temp
>2500.0..10000.0	-20.0..350.0

`temp > 350` **and** `throttle <= 2500`

throttle	temp
1000..>2500.0	>350..400.0

```
1 throttle = throttle - 1000 if (temp > 350.0) & (
      throttle > 2500) else throttle
```

`temp > 350` **and** `throttle <= 2500`

throttle	temp
1000..>2500.0	>350..400.0

```
1 throttle = throttle - 1000 if (temp > 350.0) & (
      throttle > 2500) else throttle
```

throttle	temp
1000..>2500.0	>350..400.0

`temp <= 350` **and** `throttle <= 2500`

throttle	temp
1000..>2500.0	-20.0..350.0

```
1 throttle = throttle - 1000 if (temp > 350.0) & (
      throttle > 2500) else throttle
```

`temp <= 350` **and** `throttle <= 2500`

throttle	temp
1000..>2500.0	-20.0..350.0

```
1 throttle = throttle - 1000 if (temp > 350.0) & (
      throttle > 2500) else throttle
```

throttle	temp
1000..>2500.0	-20.0..350.0

Reasoning on programs

Reasoning on programs

- Each of the four states has a result
- We now merge the results

We now merge these states, knowing that each of them may actually happen:

throttle	temp
>1500.0..9000.0	>350.0..400.0
>2500.0..10000.0	-20.0..350.0
1000.0..>2500.0	>350..400.0
1000.0..>2500.0	-20.0..350.0

We now merge these states, knowing that each of them may actually happen:

throttle	temp
>1500.0..9000.0	>350.0..400.0
>2500.0..10000.0	-20.0..350.0
1000.0..>2500.0	>350..400.0
1000.0..>2500.0	-20.0..350.0

throttle	temp
1000.0..10000.0	-20.0..400.0

We know that the throttle will never go below 1500RPM, and we also know that if the temperature is above 350 degrees then maximum throttle is never above 9000RPM.

Conclusion?

Nobody dies :)

This is it!

The best of luck, and thanks for the attention!