

6. Übungsblatt

Ausgabe: 19.01.16**Abgabe:** 02.02.16

6.1 Italienische Zahlen

8 Punkte

Aus nicht ganz nachvollziehbaren Gründen¹ findet sich in dem Quellcode für das Projekt A^2 eine Routine, welche angeblich angeblich in der Variablen y die Fibonacci-Zahl $\text{fib}(n)$ in linearer Zeit berechnet (so der rudimentäre Kommentar):

```
/* Calculates the Fibonacci number of n in y */
y := 0;
x := 1;
i := 0;
while (i < n) {
  aux := y;
  y := x;
  x := x + aux;
  i := i + 1
}
```

Zeigen Sie, dass dem wirklich so ist, indem Sie Vor- und Nachbedingungen formulieren, eine geeignete Invariante finden, und die Beweisverpflichtungen berechnen. Zeigen Sie dann die Beweisverpflichtungen (solange diese nicht trivial sind).

Sie für den Korrektheitsbeweis annehmen, dass in der Logik die Funktion $\text{fib} : \mathbb{Z} \rightarrow \mathbb{Z}$ wie folgt rekursiv definiert ist:

$$\text{fib}(n) = \begin{cases} 0 & n = 0 \\ 1 & n = 1 \\ \text{fib}(n-1) + \text{fib}(n-2) & n > 1 \end{cases}$$

6.2 Ampeln und Kreuzungen

12 Punkte

Nachdem es bei den erste Probefahrten mit A^2 beinahe einen Unfall an einer Kreuzung mit einer Fußgängerampel gegeben hat, wollen wir prototypisch eine sichere Ampelkreuzung formalisieren, und ihre Sicherheit beweisen.

Unsere Kreuzung besteht aus zwei sich kreuzenden Straßen und einer Fußgängerampel. Fußgänger können die Straße überqueren, indem sie einen Knopf an der Fußgängerampel betätigen und darauf warten, dass die Ampel grün wird. (Fußgänger überqueren die Straße nicht bei rot.)

Die Straßenampeln haben folgende Zustände (die sie in dieser Reihenfolge durchlaufen): Rot, Rotgelb, Grün, Gelb (und dann wieder Rot); die Fußgängerampel hat nur Rot und Grün. Die Autos können entweder auf der vertikalen oder horizontalen Straße die Kreuzung passieren (natürlich nur, wenn die Ampel nicht Rot zeigt).

¹Sie erinnern sich an die unglückliche Outsourcing-Episode vom letzten Übungsblatt?

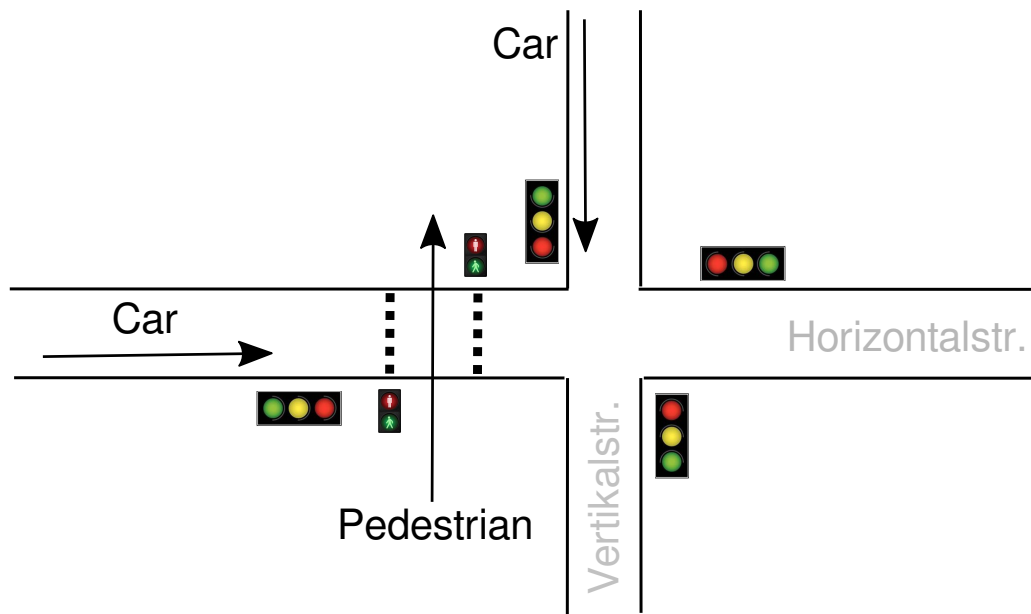


Abbildung 1: Die autonome Straßenkreuzung

Der Sicherheitsnachweis für die Straßenkreuzung besteht aus folgenden Schritten:

1. Modellieren Sie die Straßenkreuzung als endlichen Zustandsautomat.
2. Formulieren Sie folgende Sicherheitseigenschaften in linearer Temporallogik:
 - (SR-1) Fußgänger und Autos kreuzen niemals den Fußgängerüberweg zur selben Zeit.
 - (SR-2) Es können nie zwei Autos gleichzeitig die Kreuzung passieren.
 - (SR-3) Es kann nie gleichzeitig die Fußgängerampel und die Straßenampel auf der Horizontalstraße gleichzeitig grün sein.
 - (SR-4) Es können nie die beiden Straßenampeln auf Horizontal- und Vertikalstraße gleichzeitig grün sein.
3. Implementieren Sie ihr Modell in nuSMV, und untersuchen Sie, ob ihre Sicherheitseigenschaften erfüllt sind.

Sie können in erster Näherung annehmen, dass die Autos nicht abbiegen, und später Ihre Lösung so erweitern, dass das abbiegen von der Horizontal- in die Vertikalstraße und umgekehrt erlaubt ist.