Serge Autexier
Christoph Lüth

6. Übungsblatt

Ausgabe: 10.07.14
Abgabe: 24.07.14

6.1 *Ein Sicherer Roboter* *10 Punkte*

Wir modellieren jetzt den sich bewegenden Roboter und seine Umgebung. Folgende Daten beschreiben den Roboter und die Welt, in der er sich bewegt:

- die aktuelle Geschwindigkeit, bestehend aus einem Einheitsrichtungsvektor und einer skalaren Geschwindigkeit;
- die aktuelle Position des Roboters (als Ortsvektor eines Referenzpunktes der Kontur);
- die Bremsbeschleunigung;
- die Kontur des Roboters als Polygon;
- die Menge von Hindernissen (als Menge von Punkten).

Einige dieser Daten sind zeitvariant (sie ändern sich über der Zeit, bspw. die Position), andere sind zeitinvariant (konstant, bspw. die Menge der Hindernisse). Die letzteren werden einfach als Konstanten modelliert, für die ersten definieren wir Zeit als eine Sequenz von "Ticks" in einem Abstand Δt Zeiteinheiten

```
type_synonym Time = nat
```

so dass eine zeitvariante Größe r vom Typ t als Funktion $r : \texttt{Time} \Longrightarrow t$ modelliert wird.

Hieraus können folgende Daten berechnet werden:

- die momentan vom Roboter eingenommene Fläche (als Menge von Punkten), und
- die beim Bremsen mit der momentanen Geschwindigkeit bis zum Stillstand überstrichene Fläche.

Das System (der Roboter) besteht aus einer Serie von Zustandsübergängen (von jeweils Δt Zeiteinheiten): Definieren Sie die folgenden zwei Prädikate:

- der Roboter ist sicher (`safe`), wenn die beim Bremsen mit der momentanen Geschwindigkeit bis zum Stillstand überstrichene Fläche frei von Hindernissen ist;
- der Roboter ist im Folgezustand sicher (`nextsafe`), wenn die bei der Bewegung mit der momentanen Geschwindigkeit in Δt Zeiteinheiten und anschließendem Bremsen mit der momentanen Geschwindigkeit bis zum Stillstand überstrichene Fläche frei von Hindernissen ist.

1. Formalisieren sie diese Konzepte, ausgehend von Ihrer Formalisierung aus dem letzten Übungsblatt.
2. Zeigen Sie, dass `nextsafe t safe (t+ Δt)` impliziert, wenn sich die Geschwindigkeit nicht ändert; nötige Hilfssätze können gegebenfalls in Isabelle als mit `sorry` angenommen werden.
3. Wie müßte das Prädikat `nextsafe` verändert werden, wenn sich die momentane Geschwindigkeit ändern kann?

6.2 *Zwei Sichere Roboter* *10 Punkte*

Wenn jetzt mehrere Roboter herumfahren, dann ist die obige Formulierung nicht mehr ausreichend, die Roboter vor gegenseitigen Zusammenstößen zu schützen (weil sie von statischen Hindernissen ausgeht). Zum Glück bewegen sich die Roboter auf bestimmten Straßen. Wo sich diese kreuzen, werden Ampelanlagen eingerichtet. Diese funktionieren wie folgt:

- Die Ampeln können grün und rot sein; initial sind sie grün.
- Roboter können eine Ampel (Kreuzung) nur passieren, wenn sie grün ist.
- Wenn ein Roboter sich auf eine Kreuzung zubewegt, wird per Funk die andere Ampel auf rot geschaltet; wenn der Roboter sie wieder verlassen hat, wird die Ampel wieder grün geschaltet.

Modellieren Sie dieses Verhalten der Ampel und der Roboter als Finite State Machine. Formulieren Sie für eine Kreuzung mit zwei Robotern folgende Sicherheits- und Verfügbarkeitseigenschaften:

- Es können nie zwei Roboter gleichzeitig auf der Kreuzung sein.
- Jeder Roboter kann (irgendwann) die Kreuzung überqueren.

Formulieren Sie diese Eigenschaften in temporaler Logik (LTL oder CTL?). Gelten diese Eigenschaften für Ihr Modell? Geben Sie entweder eine Beweisskizze oder ein Gegenbeispiel. Falls die Eigenschaften nicht gelten, wie können Sie das System abändern, so dass sie gelten?

Alternativ formulieren Sie ihr Modell in NuSMV, und widerlegen oder beweisen Sie die Eigenschaften mit NuSMV.

(*5 Bonuspunkte*)