

4. Übungsblatt

Ausgabe: 12.01.06

Abgabe: 09.02.06

Nach dem Ende des Studiums heuern Sie für großes Geld¹ bei einem großen deutschen Automobilkonzern an, der das Garantiert Sichere AutoTM entwickeln will. Grob gesprochen handelt es sich dabei um ein Autos, welches mit Sensoren sicherstellt und einem Kontrollprogramm sicherstellt, dass es nie mit einem Hinderniss kollidiert.

Man hat Ihrer Bewerbung entnommen, dass Sie sich an der Universität Bremen in Ihrem Studium mit der formalen Spezifikation und Verifikation von Software beschäftigt haben, und betreut Sie deshalb mit der Verifikation des zentralen Kontrollalgorithmus.

Modellbildung.

Etwas idealisierend können wir ein Auto als ein Rechteck betrachten, welches sich auf einer Kreisbahn bewegt. Das Auto hat als Parameter einen Radstand R_s (Abstand Vorderachse zu Hinterachse), einen maximalen Lenkwinkel ϕ_{max} , sowie eine bedeckte Fläche A_s ; diese sind Parameter der Spezifikation.

Wir betrachten die Bewegung nicht kontinuierlich, sondern in kleinen Schritten der Zeiteinheit Δt . Dieses vereinfacht zum einen die Betrachtung, zum anderen aber ist Δt der interne Takt ('Tick') des Controllers: dieser wird alle Δt Sekunden aufgerufen mit den Eingabedaten (s.u.) aufgerufen, und kann dann die Ausgabedaten für den nächsten Tick setzen.

Die Eingabedaten sind hierbei zum einen die Steuerbefehle des Benutzers (Bremsen, Lenkung, Gas), zum anderen (später) die Sensordaten. Die Ausgabedaten sind der aktuelle Lenkwinkel sowie die Motor- und Bremssteuerung.

Das Verhalten des Autos kann idealisierend wie folgt beschrieben werden: zu jedem Zeitpunkt t wird der Zustand des Autos beschrieben durch eine Position p , die Orientierung ω , die momentane Geschwindigkeit v und den Lenkwinkel ϕ . Das Auto fährt dann auf einer Kreisbahn mit dem Radius r um den Lenkmittelpunkt M (vgl. Abb. 1). M ergibt sich als Ortsvektor $\vec{M}$ wie folgt aus p , ω , ϕ und R_s :

$$r = \frac{R_s}{\tan \phi} \quad (1)$$

$$\vec{M} = (r, \omega_A) + \vec{p} \quad (2)$$

$$\omega_A = \omega + \phi + \frac{\pi}{2} \quad (3)$$

Hierbei ist $\vec{p}$ der Ortsvektor des Punktes p (d.h. der Vektor vom Ursprung zu diesem Punkt), und (r, ω) der durch die Polarkoordinaten (r, ω) beschriebene Punkt (siehe Anhang).

In der Zeit ΔT bewegt sich das Auto auf einer Kreisbahn um den Mittelpunkt M . Mit einer Geschwindigkeit v legt es dabei eine Strecke $l = v\Delta t$, welches einer Drehung um

$$\zeta = \frac{v\Delta t}{r} \quad (4)$$

¹Achtung: fiktives Szenario!

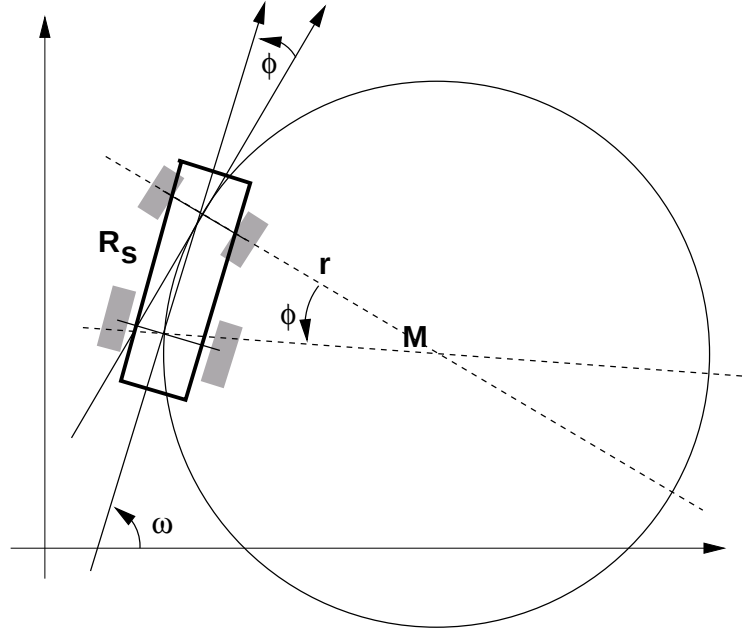


Abbildung 1: Das Auto

entspricht (da $\frac{l}{2\pi r} = \frac{\zeta}{2\pi}$). Nach der Zeit ΔT ergeben sich damit als neue Position $\vec{p}'$ und Orientierung ω'

$$\vec{p}' = \text{rot}(\vec{M}, \zeta, \vec{p}), \quad (5)$$

$$\omega' = \omega + \zeta. \quad (6)$$

Hierbei ist $\text{rot}(\vec{M}, \zeta, \vec{p})$ die Rotation des Punktes $\vec{p}$ mit den Winkel ζ um den Mittelpunkt $\vec{M}$ (siehe Anhang). Ein gesondert zu behandelnder Grenzfall ist der Lenkwinkel $\phi = 0$ (Geradeausfahrt), für den Gleichung (1) undefiniert ist. Die neue Geschwindigkeit ergibt sich als

$$v' = v + a\Delta T \quad (7)$$

wobei a die momentane Beschleunigung ist. Diese ergibt sich aus den Benutzereingaben: wenn gerade gebremst wird, wirkt eine Bremsbeschleunigung (negativ) $a_{brk}(v)$, die von der Geschwindigkeit abhängt; wenn beschleunigt wird (mit einem Faktor F zwischen 0 und 1, wobei $F = 1$ Maximalbeschleunigung ist, also Gaspedal voll durchgetreten), wirkt eine (konstante) Beschleunigung $a = Fa_{max}$ (wir berücksichtigen also keine Gänge), und es wirkt auf jeden Fall eine Bremsreibung (als negative Beschleunigung) von $a_{fr}(v)$, die auch von der Geschwindigkeit abhängig ist (und zwar quadratisch: $a_{fr}(v) = \alpha_{fr}v^2 + \beta_{fr}v + \gamma_{fr}$).

Die Geschwindigkeit ist nie kleiner als 0 (Vereinfachung: kein Rückwärtsgang).

6 Anforderungsspezifikation

10 Punkte

Hindernisse werden einfach als Menge von Punkten betrachtet, die sich nicht bewegen (eine etwas idealisierte Darstellung der Zustände auf deutschen Autobahnen). ‘Sicherheit’ soll heißen, dass zum einen das Auto nie mit einem Hinderniss kollidiert, und zum anderen das Auto auch noch fährt.

Spezifizieren Sie diese Anforderungen formal. Dazu müssen Sie auch eine formale Spezifikation des Verhaltens des Autos angeben.

7 Entwurfsspezifikation

30 Punkte

Um Hindernisse zu erkennen hat das Auto einen Sensor, zum Beispiel einen Laserscanner. Idealisiert gibt ein Laserscanner eine Liste von Paaren (α, d) zurück, wobei α der Orientierungswinkel und d die Entfernung ist, in der ein Hinderniss geortet wird; ist d dabei eine festgelegte Maximalentfernung d_{max} , dann kann in dieser Entfernung kein Hinderniss geortet werden.

Geben Sie eine Entwurfsspezifikation eines Kontrollprogrammes an, welches aus Eingabe- und Sensordaten einen im Sinne der Anforderungsspezifikation sicheren Steuerbefehl generiert, und beweisen Sie die Sicherheit formal. Dabei werden Sie Annahmen über die Hindernisse und den Sensor machen müssen, zum Beispiel dass der Sensor alle Hindernisse erkennt.

8 Prototyp

20 Punkte

Entwickeln Sie eine Implementation entweder einer imperativen Sprache ihrer Wahl an oder in der funktionalen Untermenge von HOL. Verifizieren Sie diese Implementation gegen die Entwurfsspezifikation.

9 Produktion

20 Bonuspunkte

Aus Kostengründen enthält die Serienproduktion des Garantiert Sicheren Autos einen Sensor, der an der Vorderfront des Autos montiert ist, und nur einen Winkel Ξ abdeckt. Wann kann das Auto damit immer noch sicher fahren? Modifizieren Sie das Kontrollprogramm, Beweis und Implementation entsprechend.

Mathematischer Anhang

rot_ϕ bezeichnet die Drehung des Koordinatensystems mit einem Winkel ϕ um den Ursprung:

$$rot_\phi \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x \cos \phi - y \sin \phi \\ x \sin \phi + y \cos \phi \end{pmatrix} \quad (8)$$

$rot(\vec{m}, \phi, \vec{p})$ bezeichnet die Drehung eines Punktes $\vec{p}$ mit dem Winkel ϕ um einen Mittelpunkt $\vec{m}$, und berechnet sich wie folgt:

$$rot(\vec{m}, \phi, \vec{p}) = \vec{m} + rot_\phi(\vec{p} - \vec{m}) \quad (9)$$

Um einen in Polarkoordinaten (r, ϕ) angegebenen Punkt in kartesische Koordinaten $\vec{p}$ umzuwandeln, rotieren wir um den Winkel ϕ :

$$\vec{p} = rot_\phi \begin{pmatrix} r \\ 0 \end{pmatrix} \quad (10)$$