

Die Modellierung der Robotik-Domäne von SAMS im Theorembeweiser Isabelle

Christoph Hertzberg
Universität Bremen – Fachbereich 3 Mathematik und Informatik

Universität Bremen, Cartesium, 13.10.09



- 1 Was ist ein Theorembeweiser?
 - Ein Theorembeweiser ist kein ...
 - Ein Theorembeweiser ist ...
- 2 Beispiele
 - Einführungsbeispiel
 - Beispiele aus der Domäne
- 3 Fazit

Computer-Algebra-System

- Programm zum Rechnen mit symbolischen Ausdrücken
 - Mathematica, Derive, Maxima, ...
- Eignet sich zum Lösen von algebraischen Problemen
- Beispiel: `solve(a*x^2+b*x+c=0, x)`

Computer-Algebra-System

- Programm zum Rechnen mit symbolischen Ausdrücken
 - Mathematica, Derive, Maxima, ...
- Eignet sich zum Lösen von algebraischen Problemen
- Beispiel: `solve(a*x^2+b*x+c=0, x)`
 - $x = -\frac{\sqrt{b^2-4ac+b}}{2a} \vee x = \frac{\sqrt{b^2-4ac-b}}{2a}$
 - Stimmt das?

Computer-Algebra-System

- Programm zum Rechnen mit symbolischen Ausdrücken
 - Mathematica, Derive, Maxima, ...
- Eignet sich zum Lösen von algebraischen Problemen
- Beispiel: `solve(a*x^2+b*x+c=0, x)`
 - $x = -\frac{\sqrt{b^2-4ac+b}}{2a} \vee x = \frac{\sqrt{b^2-4ac-b}}{2a}$
 - Stimmt das? Immer?

Computer-Algebra-System

- Programm zum Rechnen mit symbolischen Ausdrücken
 - Mathematica, Derive, Maxima, ...
- Eignet sich zum Lösen von algebraischen Problemen
- Beispiel: `solve(a*x^2+b*x+c=0, x)`
 - $x = -\frac{\sqrt{b^2-4ac+b}}{2a} \vee x = \frac{\sqrt{b^2-4ac-b}}{2a}$
 - Stimmt das? Immer?
 - **Gegenbeispiel:** $a = 0$, Division durch 0

Computer-Algebra-System

- Programm zum Rechnen mit symbolischen Ausdrücken
 - Mathematica, Derive, Maxima, ...
- Eignet sich zum Lösen von algebraischen Problemen
- Beispiel: `solve(a*x^2+b*x+c=0, x)`
 - $x = -\frac{\sqrt{b^2-4ac+b}}{2a} \vee x = \frac{\sqrt{b^2-4ac-b}}{2a}$
 - Stimmt das? Immer?
 - **Gegenbeispiel:** $a = 0$, Division durch 0
 - Wenn $b^2 - 4ac < 0$, keine reelle Lösung.

Computer-Algebra-System

- Programm zum Rechnen mit symbolischen Ausdrücken
 - Mathematica, Derive, Maxima, ...
- Eignet sich zum Lösen von algebraischen Problemen
- Beispiel: `solve(a*x^2+b*x+c=0, x)`
 - $x = -\frac{\sqrt{b^2-4ac+b}}{2a} \vee x = \frac{\sqrt{b^2-4ac-b}}{2a}$
 - Stimmt das? Immer?
 - **Gegenbeispiel:** $a = 0$, Division durch 0
 - Wenn $b^2 - 4ac < 0$, keine reelle Lösung.
- Korrektheit der Lösung nicht garantiert
 - Falsche Lösungen können sich einschleichen
 - Faktoren können weggekürzt werden
- CAS sind aber gut geeignet zum Suchen von Lösungen

Ein Theorem (auch Satz oder Lemma)

- ist eine im Sinne der Logik widerspruchsfreie **Aussage**, die mittels eines **Beweises** als wahr erkannt, das heißt, aus **Axiomen** und bereits bewiesenen Sätzen hergeleitet werden kann.

Isabelle bekommt

- Axiome
 - Als elementar richtig angesehene Aussagen, die sich nicht beweisen lassen (z. B. $x = x$).
- Definitionen
- Darauf aufbauende Lemmas und Theoreme mit Beweisen

In Isabelle bereits umgesetzt

- die klassischen Axiomensysteme (ZFC, HOL)
- darauf aufbauend Definitionen und Theoreme für
 - Natürliche, Ganze, Rationale, Reelle und Komplexe Zahlen
 - Funktionen, Grenzwerte, Ableitungen, . . .
 - Vorhandene Definitionen entsprechen Lehrbuchdefinitionen

Isabelle prüft

- ob die Beweise korrekt sind

Isabelle prüft nicht

- ob die verwendeten Axiome sinnvoll und widerspruchsfrei sind
- ob die verwendeten Definitionen sinnvoll sind
 - „Sinnlose“ Definitionen erzeugen keinen Widerspruch

Lösung der Quadratischen Gleichung

- Ziel: $ax^2 + bx + c = 0 \iff x = -\frac{\sqrt{b^2-4ac}+b}{2a} \vee x = \frac{\sqrt{b^2-4ac}-b}{2a}$
- ohne zusätzliche Annahme nicht beweisbar

lemma

$$\begin{aligned} \llbracket a \neq 0; b^2 - 4 * a * c \geq 0 \rrbracket &\implies a * x^2 + b * x + c = 0 \iff \\ x &= (\text{sqrt}(b^2 - 4 * a * c) - b) / (2 * a) \\ \vee x &= (-\text{sqrt}(b^2 - 4 * a * c) - b) / (2 * a) \end{aligned}$$

- Beweis erfolgt, indem zunächst p, q -Formel bewiesen wird

Konvexe Mengen

- Eine Menge ist **konvex**, wenn zu je zwei Punkten aus der Menge auch ihre Verbindungsgerade in der Menge enthalten ist.

`definition` konvex :: "Punkt set \Rightarrow bool" `where`

- `"konvex K \leftrightarrow ($\forall x \in K. \forall y \in K. \forall t \in \{0..1\}. (t *_{\mathbb{R}} x + (1-t) *_{\mathbb{R}} y) \in K$)"`

Konvexe Hülle

- Die **konvexe Hülle** einer Menge X ist der Schnitt aller konvexen Mengen, die X enthalten.

`definition` konvexe_huelle :: "Punkt set \Rightarrow Punkt set" `where`

- `"konvexe_huelle X = $\bigcap \{K. \text{konvex } K \wedge X \subseteq K\}$ "`

Typen

SO2 2. Spezielle Orthogonale Gruppe (Rotation/Orientierung in der Ebene)

SKT Starrkörpertransformationen (Position und Orientierung)

Funktionen

sinc Sinus cardinalis:
$$\text{sinc } x = \begin{cases} \frac{\sin x}{x} & x \neq 0 \\ 1 & x = 0 \end{cases}$$

transformiere Wende eine Starrkörpertransformationen auf einen Punkt an

bogen Gibt zu Strecke s , Winkel α und Startpunkt P die zugehörige Punktmenge

lemma kreis_konvex: "konvex { q . norm $q \leq r$ }"

Beweisziel:

- konvex { q . norm $q \leq r$ }

```
lemma kreis_konvex: "konvex {q. norm q <= r}"  
  apply(simp add: konvex_def)
```

Beweisziel:

- $\forall x. \text{norm } x \leq r \longrightarrow (\forall y. \text{norm } y \leq r$
 $\longrightarrow (\forall t \in \{0..1\}. \text{norm}(t *_R x + (1 - t) *_R y) \leq r))$

```
lemma kreis_konvex: "konvex {q. norm q <= r}"  
  apply(simp add: konvex_def)  
  apply auto
```

Beweisziel:

- $\bigwedge x y t. [\text{norm } x \leq r; \text{norm } y \leq r; 0 \leq t; t \leq 1] \implies \text{norm}(t *_R x + (1 - t) *_R y) \leq r$

```
lemma kreis_konvex: "konvex {q. norm q <= r}"  
  apply(simp add: konvex_def)  
  apply auto  
  apply(rule real_le_trans[OF norm_triangle_ineq])
```

Beweisziel:

- $\bigwedge x y t. [\text{norm } x \leq r; \text{norm } y \leq r; 0 \leq t; t \leq 1] \implies \text{norm}(t *_R x) + \text{norm}((1 - t) *_R y) \leq r$

```
lemma kreis_konvex: "konvex {q. norm q <= r}"  
  apply(simp add: konvex_def)  
  apply auto  
  apply(rule real_le_trans[OF norm_triangle_ineq])  
  apply(simp add: norm_scaleR)
```

Beweisziel:

- $\bigwedge x y t. [\text{norm } x \leq r; \text{norm } y \leq r; 0 \leq t; t \leq 1] \implies t * \text{norm } x + (1 - t) * \text{norm } y \leq r$

```
lemma kreis_konvex: "konvex {q. norm q <= r}"  
  apply(simp add: konvex_def)  
  apply auto  
  apply(rule real_le_trans[OF norm_triangle_ineq])  
  apply(simp add: norm_scaleR)  
  apply(drule_tac c=t in mult_left_mono, simp)
```

Beweisziel:

- $\bigwedge x y t. [\text{norm } y \leq r; 0 \leq t; t \leq 1; t * \text{norm } x \leq t * r] \implies t * \text{norm } x + (1 - t) * \text{norm } y \leq r$

```
lemma kreis_konvex: "konvex {q. norm q <= r}"  
  apply(simp add: konvex_def)  
  apply auto  
  apply(rule real_le_trans[OF norm_triangle_ineq])  
  apply(simp add: norm_scaleR)  
  apply(drule_tac c=t in mult_left_mono, simp)  
  apply(drule_tac c="1-t" in mult_left_mono, simp)
```

Beweisziel:

- $\bigwedge x y t. [0 \leq t; t \leq 1; t * \text{norm } x \leq t * r; (1 - t) * \text{norm } y \leq (1 - t) * r]$
 $\implies t * \text{norm } x + (1 - t) * \text{norm } y \leq r$

```
lemma kreis_konvex: "konvex {q. norm q <= r}"  
  apply(simp add: konvex_def)  
  apply auto  
  apply(rule real_le_trans[OF norm_triangle_ineq])  
  apply(simp add: norm_scaleR)  
  apply(drule_tac c=t in mult_left_mono, simp)  
  apply(drule_tac c="1-t" in mult_left_mono, simp)  
  apply(simp add: ring_simps)
```

Beweisziel:

- No Subgoals!

```
lemma kreis_konvex: "konvex {q. norm q <= r}"  
  apply(simp add: konvex_def)  
  apply auto  
  apply(rule real_le_trans[OF norm_triangle_ineq])  
  apply(simp add: norm_scaleR)  
  apply(drule_tac c=t in mult_left_mono, simp)  
  apply(drule_tac c="1-t" in mult_left_mono, simp)  
  apply(simp add: ring_simps)  
done
```

Beweisziel:

- No Subgoals!

`bogenpunkt_in_konvexer_huelle` Beweist, dass Bogen im berechneten Dreieck liegt

`bogen_n_aufgeteilt` Beweist, dass sich Bogen in Teilbögen zerlegen lässt

`sin_cos_le_poly_trigpoly` Sinus und Cosinus lassen sich durch Taylorentwicklung abschätzen

Isabelle

- Isabelle erspart es nicht den Beweis vorher manuell zu führen, bzw. eine Beweisidee zu kennen
 - viele grundlegende Dinge sind schon bewiesen
 - vieles „triviales“ muss man noch beweisen
- Nachdem man sich eingearbeitet hat, lassen sich viele Beweise relativ komfortabel umsetzen
- Termumformungen sind z. T. etwas anstrengend
- Keine „offensichtlich gilt“- oder „andere Fälle analog“-Beweise

SAMS-Domäne

- Über 15 000 Zeilen an Definitionen und Lemmas und Beweisen
- Domäne kann für spätere Projekte wiederverwendet werden

Vielen Dank!

Fragen?