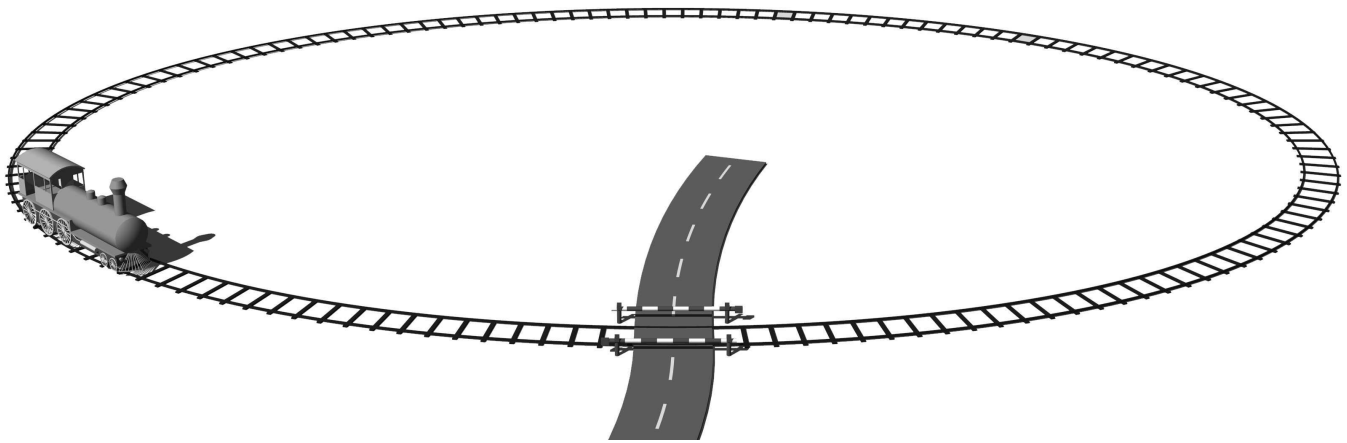
Algebraische Kalküle für hybride Systeme

Peter Höfner

Universität Augsburg



Motivation

Fehlerhafte Software

- fordert Menschenleben
- ruft Umweltschäden hervor
- führt zu wirtschaftlichen Verlusten

Flughafen Heathrow (Terminal 5, April 2008)

- über 500 gestrichene Flüge,
- über 28.000 Koffer falsch sortiert,
- über $£16$ Mio. Schaden

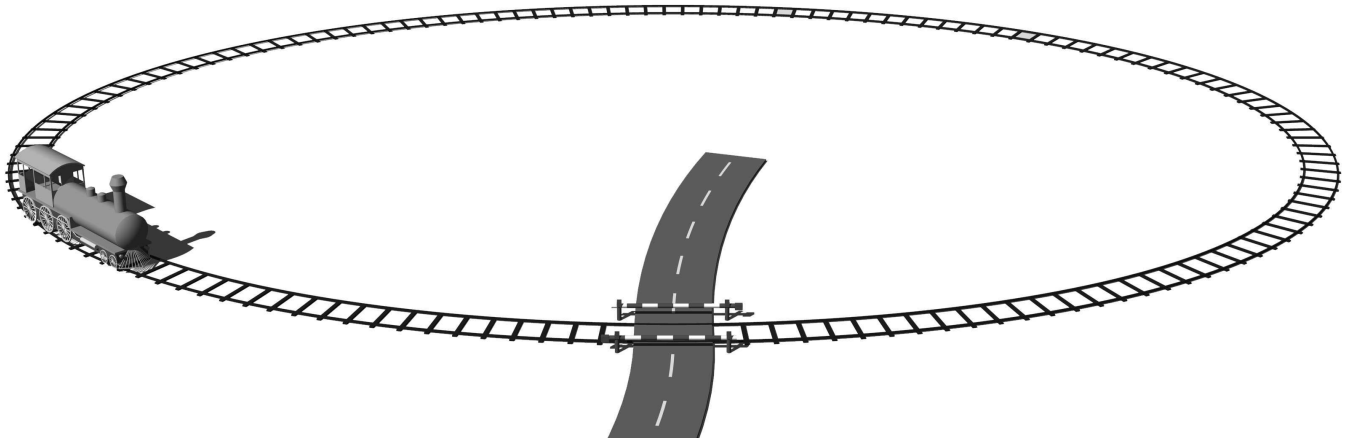
(trotz mehr als 400.000 Stunden Entwicklungszeit der Software)

Hybride Systeme

Interaktion mit ihrer Umgebung

- Anwendungsgebiete: Steuerungselemente, Medizintechnik, Avionik, Raumfahrt, Biologie, etc.
- allein ein Auto hat heutzutage mehr als 60 Prozessoren (z.B. Airbag)
- weniger als 1% aller Prozessoren arbeiten in PCs
  über 98% sind Kontrollsysteme von hybriden Systemen

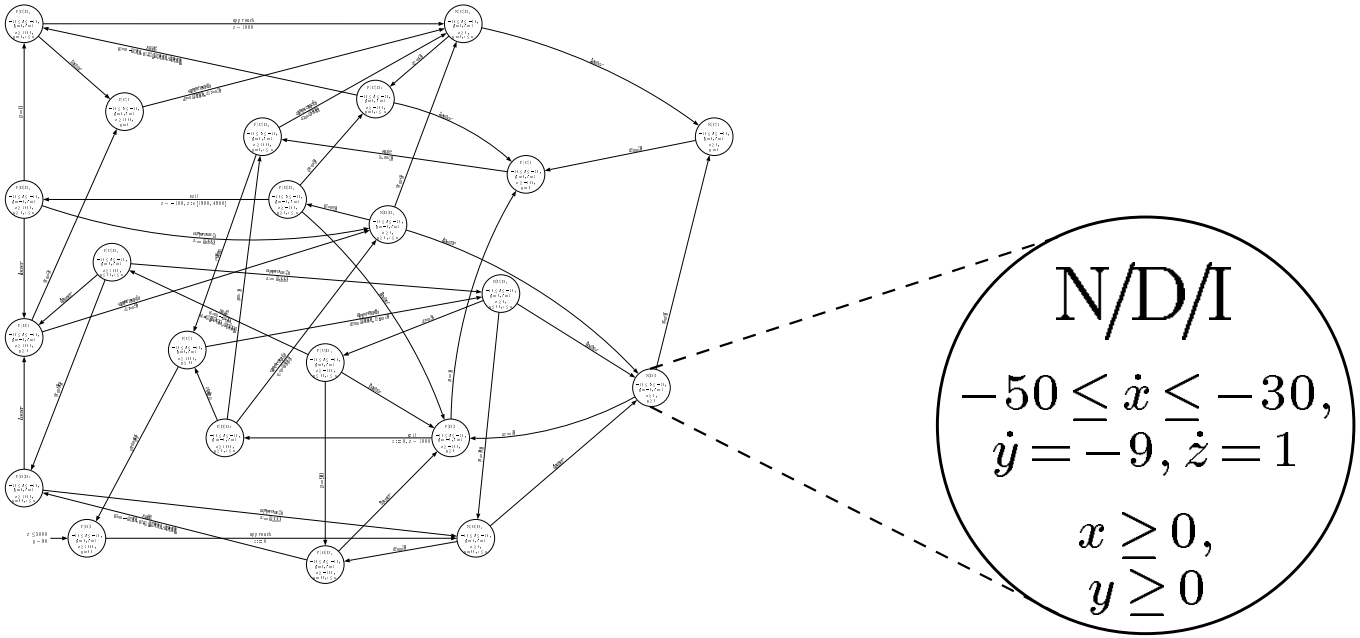
Ein einfaches hybrides System



Kontrollsystem für einen beschrankten Bahnübergang

- Bahnschranken müssen geschlossen sein, sobald der Zug den Bahnübergang passiert
- Steuerung des Schrankensystems durch einen Computer
- Gleichungen beschreiben Schranke und Zug

Hybride Automaten



Vorhandenes Standardwerkzeug

- beschreiben systematisch alle Abläufe
- Knoten enthalten unterschiedlichste Eigenschaften
- Verifikation von Eigenschaften of kompliziert
- enorme Rechenleistung wird benötigt

Algebraischer Ansatz

$$\big(O||(P_1 \cdot T_1 \cdot P_2)\big) \cdot$$
$$\Big(\big((M_1 \cdot C)||(T_2 \cdot P_3)\big) \cdot \big(C||(T_2 \cdot P_4)_{\asymp}\big) \cdot \big((M_2 \cdot O)||(T_1 \cdot P_2)\big)\Big)^{\omega}$$

Vorteile

- präzise und kompakte Beschreibung
- Verwendung von Standard-Computer-Algebrasystemen
- Gleichungsregeln zur Überprüfung von Sicherheitsaspekten (z.B. Schranke geschlossen)
- Modellierung von Lebendigkeit und Invarianten

Algebraischer Ansatz

$$\big(O||(P_1 \cdot T_1 \cdot P_2)\big) \cdot$$
$$\Big(\big((M_1 \cdot C)||(T_2 \cdot P_3)\big) \cdot \big(C||(T_2 \cdot P_4)_{\asymp}\big) \cdot \big((M_2 \cdot O)||(T_1 \cdot P_2)\big)\Big)^{\omega}$$

Vorteile

- präzise und kompakte Beschreibung
- Verwendung von Standard-Computer-Algebrasystemen
- Gleichungsregeln zur Überprüfung von Sicherheitsaspekten (z.B. Schranke geschlossen)
- Modellierung von Lebendigkeit und Invarianten

Wichtiges algebraisches Konstrukt

$$P_1 \cdot T \cdot P_2$$

Vor- und Nachbedingungen

- Falls das hybride System die Vorbedingungen von P_1 vor der Ausführung von T erfüllt, dann gilt danach P_2
- eng verwandt mit "Wenn-dann-Konstrukten" (Logik)
- Beispiel: Wenn der Zug $50\,\frac{\mathrm{km}}{\mathrm{h}}$ fährt und 5 Minuten beschleunigt, dann fährt er danach $100\,\frac{\mathrm{km}}{\mathrm{h}}$

Zusammenfassung

Forschungsergebnisse

- kohärente Familie algebraischer Kalküle für hybride Systeme
- kompakte und einheitliche Behandlung von diversen Logiken
- erste Fallstudien
- Computerunterstützung zur Verifikation

Weitere Forschungsvorhaben

- hybride Systeme können auch als Spiele aufgefasst werden (Zwei- und Mehr-Personen-Spiele)

If you are faced by a difficulty or a controversy in science,
an ounce of algebra is worth a ton of verbal argument.

J.B.S. Haldane