Foundations of Computing

Modul 14 (v1.0)

Kanonikvorlesung: Foundations of Computing

Heiko Mantel

MAIS, TU Darmstadt, WS10/11

Übersicht: Modul 14

Zusammenfassung der Vorlesung

- Modellierung
- Spezifikation
- Analyse

Lehrangebot im Bereich FoC

- relevanter Pflichtbereich
- Wahlpflichtbereich

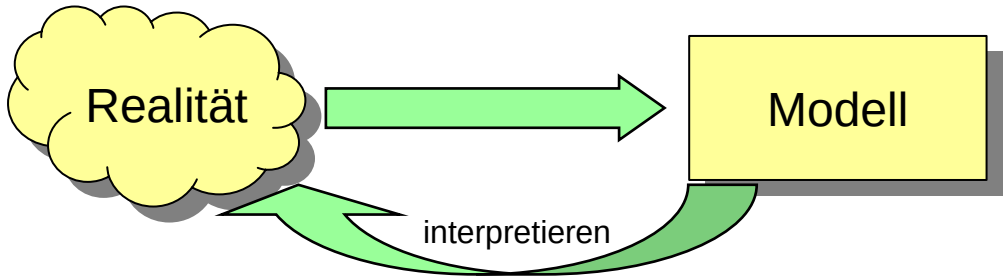
Klausur

- Erinnerung

Modell und Realität (1)

Ein Modell

- hebt bestimmte Aspekte der Realität deutlicher hervor,
- ist absichtlich nicht originalgetreu.



Angemessenheit

- Sind alle relevanten Aspekte des gegebenen Sachverhaltes so wiedergegeben, dass Beobachtungen, die am Modell gemacht werden, auch für den realen Sachverhalt nützlich sind.

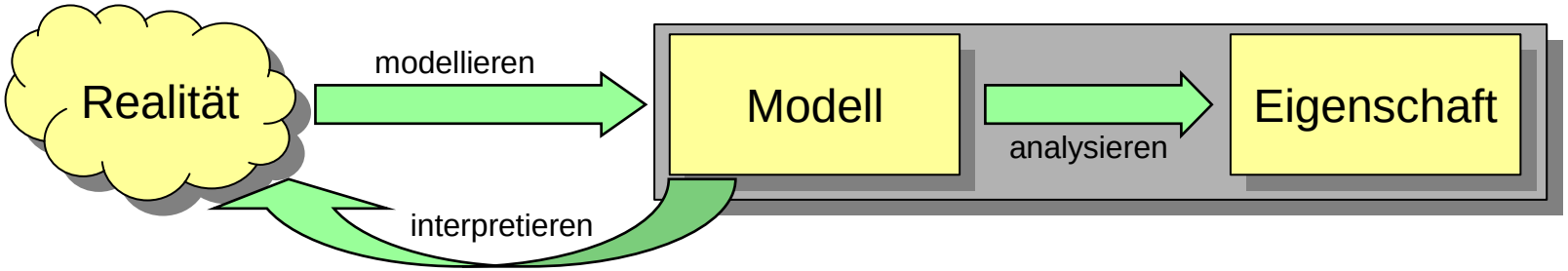
Angemessenheit ist ein Muss-Kriterium für eine Modellierung!

Modell und Realität (2)

Was ist ein Modell eines Informationssystems?

eine Beschreibung des Informationssystems (Hard- und Software)

- aus einer gegebenen Perspektive und
- auf einer gegebenen Abstraktionsstufe



Ein Modell ist absichtlicht nicht originalgetreu, um bestimmte Aspekte der Realität deutlicher hervorzuheben. Daher können nicht alle Eigenschaften des Modells der Realität entsprechen.

Alle relevanten Eigenschaften sollten der Realität entsprechen.

Formale Modelle

Wie beschreibt man ein Modell formal?

- durch Verwendung von Konzepten der Mathematik

Welche Konzepte sollte man bei der Modellierung verwenden?

- Das Modell muss für die relevanten Fragen angemessen sein.
- Ein einfaches Modell ist einem komplizierten vorzuziehen.
- Bei der Modellierung sollte man die Zielgruppe berücksichtigen:
  - Wer verwendet das Modell?
  - Wer evaluiert das Modell?
- Informelle Beschreibungen oder graphische Illustrationen als Ergänzungen zum formalen Modell sind meist wünschenswert.
  - Der Bezugspunkt ist das formale Modell, nicht die Beschreibung!

Was hat man von einer formalen Modellierung?

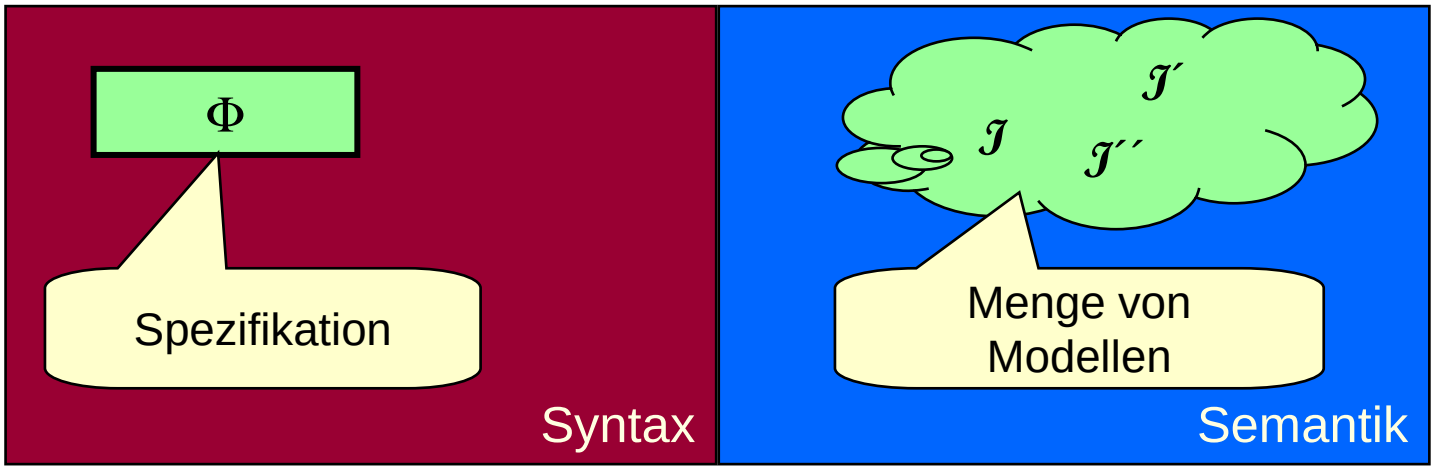
- Präzise Beschreibung des Modells erlaubt Benennung von Fehlern.
- Qualitätskontrolle durch formale Verifikation wird möglich.

Modelle und Spezifikationen (1)

Was ist eine formale Spezifikationssprache?

Eine Sprache mit formal definierter Syntax und Semantik.

- Syntax
  - Welche Ausdrücke sind als Spezifikationen zulässig?
- Semantik
  - Welches Modell (oder welche Menge von Modellen) wird durch eine gegebene Spezifikation beschrieben?
  - Diese Zuordnung muss für jede Spezifikation eindeutig sein!



Modelle und Spezifikationen (2)

Ausdrucksmächtigkeit einer Spezifikationssprache

- Welche Klasse von Modellen kann durch Spezifikationen in dieser Sprache beschrieben werden?

Unterschiedliche Spezifikationssprachen können

- unterschiedliche Ausdrucksmächtigkeit haben
  - z.B. reguläre Grammatiken und kontextfreie Grammatiken
- dieselbe Ausdrucksmächtigkeit haben
  - z.B. reguläre Ausdrücke, reguläre Grammatiken und DFAs

Einer Spezifikationssprache können

- unterschiedliche Semantiken zugeordnet werden
  - siehe z.B. Diskussion endlicher Automaten am Ende von Modul 4

Formale Spezifikationssprachen

Modul 1

- Aussagen- und Prädikatenlogik

Modul 4

- reguläre Ausdrücke, reguläre Grammatiken, DFAs, NDFAs
- kontextfreie Grammatiken, Kellerautomaten

Modul 5-8

- Aexp: Spezifikationssprache für arithmetische Ausdrücke
- Bexp: Spezifikationssprache für boolsche Ausdrücke
- Com: Spezifikationssprache für Algorithmen
- Kalküle: Spezifikationssprache für operationelle Semantik

Modul 12-13

- Prozessausdrücke (Teilsprache der Prozessalgebra CSP)

Es gibt sehr viele weitere Spezifikationssprachen:

❒ Beispiele: CCS, Pi-Kalkül, LTL, CTL, TLA, Z, CASL, …

Freiheitsgrade in der Modellierung

Beobachtung

Oft gibt es mehr als eine Möglichkeit, eine informelle Beschreibung angemessen zu formalisieren.

Das heißt konkret:

- es kann mehrere gleich gute Modelle oder Spezifikationen geben.

Beispiele

- Modul 3
  - Arbeitskreise der EU
- Modul 8
  - alternative Semantik für die Programmiersprache IMP
- weitere Beispiele in den Übungen

Achtung, nicht jede Modellierung/Spezifikation ist gleich gut!
❒ Für Kriterien für die Güte von Modellen siehe z.B. Folie 5.

Einsatz formaler Modellierung

Formale Spezifikation von Anforderungen

- dient zur Kommunikation zwischen Auftraggebern und Entwicklern.
- Vermeidung von Missverständnissen
  - Formale Spezifikationssprachen haben eine eindeutige Semantik, wodurch Mehrdeutigkeiten vermieden werden.

Formale Spezifikation des Systems während der Entwicklung

- dient vor allem zur Kommunikation zwischen Entwicklern
- Vermeidung von Missverständnissen
  - Formale Spezifikationssprachen haben eine eindeutige Semantik, wodurch Mehrdeutigkeiten vermieden werden.
- Generierung von Programmteilen aus Spezifikationen ist möglich.

Formale Modelle werden z.B. im Rahmen von Evaluierungen sicherheitskritischer Software verlangt (Common Criteria).

Analyse formaler Modelle

formale Verifikation

- Mathematischer Beweis von Eigenschaften eines formalen Modells oder von Beziehungen zwischen mehreren Modellen.

Beispiel für Beweistechniken (siehe Modul 7 und 8)

- Fallunterscheidung
- Widerspruchsbeweis
- strukturelle Induktion
- Induktion über Herleitungen

Es gibt auch Kalküle zur formalen Verifikation.

- z.B. Kalkül des natürlichen Schließens, Sequenzenkalkül oder Resolution für die Prädikatenlogik (siehe Modul 1)
- Programmlogiken wie z.B. den Hoare Kalkül (skizziert in Modul 9)

Werkzeugunterstützung

Werkzeuge werden eingesetzt z.B.

- um die Verwendung von formalen Methoden zu erleichtern oder
- um die Qualität der Verwendung zu erhöhen.

In welchen Bereichen ist Werkzeugunterstützung hilfreich?

- Editieren von formalen Spezifikation
- Überprüfen, ob eine Spezifikation gemäß der Syntax gültig ist
- Editieren und Konstruieren von formalen Beweisen
- Unterstützung bei der Beweissuche
- Verwaltung von Spezifikationen und Beweisen
  - Welche Beweise werden durch eine gegebene Änderung der Spezifikation ungültig?

Beispiele für Werkzeuge für formale Methoden

- B-tool, ISABELLE, PVS, VeriFun, VSE,..

Übersicht: Modul 14

Zusammenfassung der Vorlesung

- Modellierung
- Spezifikation
- Analyse

Lehrangebot im Bereich FoC

- relevanter Pflichtbereich
- Wahlpflichtbereich

Klausur

- Erinnerung

Angebot in der Kanonik FoC (1)

relevante Veranstaltungen im Pflichtbereich

FGdI 1

- formale Sprachen und Automaten

FGdI 2

- Aussagen- und Prädikatenlogik
- Logikkalküle

FGdI 3

- Algebra und abstrakte Datentypen
- Theorembeweisen und Model Checking

Kanonikvorlesung FoC

- formale Modellierung und Spezifikation
- Syntax und Semantik von Programmier- und Spezifikationssprachen

Angebot in der Kanonik FoC (2)

relevante Vorlesungen der Fachgebiete im Wahlpflichtbereich

Algorithmik (K. Weihe)

- Algorithmische Modellierung (2+2)

Programmiermethodik (C. Walther)

- Berechenbarkeitstheorie (2+1)
- Semantik und Programmverifikation (3+1) – Trusted Systems
- Termersetzungssysteme (4+2) – Trusted Systems
- Verfahren zur automatischen Verifikation (3+1) – Trusted Systems

Modellierung und Analyse von Informationssystemen (H. Mantel)

- Formale Methoden der Informationssicherheit (4+2)
- Statische und dynamische Programmanalyse (voraussichtlich IV 4)

Formal Methods in Systems Engineering (H. Veith)

- Komplexitätstheorie (2+2)
- Model Checking (2+2)

Darüberhinaus

- Vorlesungen von Privatdozenten und Lehrbeauftragten

Mein Lehrangebot

in Sommersemestern

Formale Methoden der Informationssicherheit (V4+Ü2)
Praktikum: Proof-Carrying-Code auf mobilen Endgeräten (P4)
Seminar: Proof-Carrying-Code (S2)
Current Topics in Usage Control (S2)
weitere Seminare zu wechselnden Themen

in Wintersemestern

Kanonikvorlesung FoC (IV3) / Formale Grundlagen der Informatik 3
Statische und dynamische Programmanalyse (voraussichtlich IV 4)
Modellierungspraktikum (P4)
Seminar: Formale Spezifikation (S2)
Praktikum Sichere Informationssysteme (P4)
Current Topics in Information Flow Control (S2)
weitere Seminare zu wechselnden Themen

Vorkenntnisse:
❒ FoC und FGDI 2 für die meisten Veranstaltungen

Info: Nicht alle Veranstaltungen finden in jedem Jahr statt.

Übersicht: Modul 14

Zusammenfassung der Vorlesung

- Modellierung
- Spezifikation
- Analyse

Lehrangebot im Bereich FoC

- relevanter Pflichtbereich
- Wahlpflichtbereich

Klausur

- Erinnerung

Klausur (Erinnerung)

Klausur

- Datum: 16. März 2011, 8:00-10:30
  (bitte in TUCAN nach Änderungen schauen!)
- Ort: Zuordnung wird später bekannt gegeben.
- Regeln:
  - keine Unterlagen, elektronischen Hilfsmittel, …
  - 1 beidseitig handbeschriebene DIN A4 Seite ist erlaubt
    - **keine Ausdrucke! keine Kopien!**
    - muss **deutlich lesbar** mit Name und Matrikelnummer **am oberen Rand** auf **beiden** Seiten markiert sein
  - mitzubringen sind
    - **Personalausweis** oder **Reisepass** mit Lichtbild
    - **Studierendenausweis** im Original
    - **Kugelschreiber/Füller**
    - **Uhr**
  - Papier wird gestellt (sowohl für Antworten als auch für Notizen)