# Vorlesung vom 24.10.05: Einführung

## Organisatorisches

- *Veranstalter*: Christoph Lüth

  `cxl@informatik.uni-bremen.de`

  `http://www.informatik.uni-bremen.de/~cxl`

  MZH 8050, Tel. 7585

- *Termine*: Vorlesung: Montag 15– 17 MZH 7260

  Übung: Donnerstag 9 s.t. – 10 8090
  Donnerstag 10 – 11 MZH 8090



## Therac-25

- Neuartiger *Linearbeschleuniger* in der Strahlentherapie.
  - *Computergesteuert* (PDP-11, Assembler)
- Fünf Unfälle mit *Todesfolge* (1985– 1987)
  - Zu hohe *Strahlendosis* (4000 – 20000 rad, letal 1000 rad)
- Problem: *Softwarefehler*
  - Ein einzelner *Programmierer* (fünf Jahre)
  - Alles in *Assembler*, kein *Betriebssystem*
  - *Programmierer* auch *Tester* (Qualitätskontrolle)



## Ariane-5



## Die Vasa



## Lernziele

1. *Modellierung* — *Formulierung* von Spezifikationen
2. *Verifikation* — Beweis von *Korrektheit*
3. *Formale Entwicklung* und formaler *Beweis*

Darüber hinaus:

- Vertrautheit mit *aktuellen Techniken* (Isabelle, Z, CASL)



## Themen

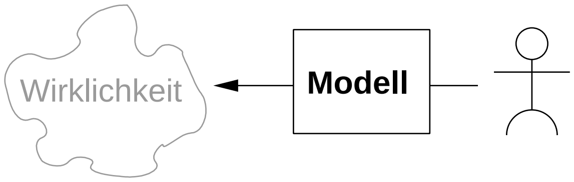
- *Grundlagen*:
  - Formale *Logik*, formales *Beweisen*
- Formale *Spezifikation*
  - *Modellbasiert*: Z
  - *Axiomatisch*: CASL
- *Verifikation* vs. *formale Entwicklung*
  - Nicht *notwendigerweise* ein *Gegensatz* (Djikstra, Gries)



## Plan

- Nächste *fünf Wochen*:
  - *Formale Logik*, funktionale Programmierung (Isabelle)
- Bis *Weihnachten*:
  - Spezifikation *imperativer* Programme (Z)
- Nach *Weihnachten*:
  - *Grundlagen* der *Verifikation*: weakest precondition
  - Entwicklung durch *Verfeinerung* und *Transformation*
  - *Software Modelchecking* (wenn Zeit)

## Das Problem






## Formale Logik

- *Formale* (*symbolische*) Logik: *Rechnen* mit *Symbolen*
- *Programme*: *Symbolmanipulation*
- *Auswertung*: *Beweis*
- *Curry-Howard-Isomorphie*: funktionale Programme $\cong$ konstruktiver Beweis



## Geschichte

- Gottlob *Frege* (1848– 1942)
  - *'Begriffsschrift, eine der arithmetischen nachgebildete Formelsprache des reinen Denkens'* (1879)
- Georg *Cantor* (1845– 1918), Bertrand *Russel* (1872– 1970), Ernst *Zermelo* (1871– 1953)
  - Einfache Mengenlehre: inkonsistent (Russel's Paradox)
  - Axiomatische Mengenlehre: Zermelo-Fränkel
- David *Hilbert* (1862– 1943)
  - *Hilbert's Programm*: 'mechanisierte' Beweistheorie
- Kurt *Gödel* (1906– 1978)
  - *Vollständigkeitssatz*, *Unvollständigkeitssätze*



## Grundbegriffe der formalen Logik

- *Ableitbarkeit* $\mathcal{T}h \vdash P$
  - *Syntaktische* Folgerungung
- *Gültigkeit* $\mathcal{T}h \models P$
  - *Semantische* Folgerung — hier *nicht* relevant
- *Klassische* Logik: $P \vee \neg P$
- *Entscheidbarkeit*
  - *Aussagenlogik*
- *Konsistenz*: $\mathcal{T}h \not\vdash \bot$
  - *Nicht alles* ableitbar
- *Vollständigkeit*: *jede gültige Aussage* ableitbar
  - *Prädikatenlogik* erster Stufe



## Unvollständigkeit

- Gödels 1. *Unvollständigkeitssatz*:
  - Jede *Logik*, die *Peano-Arithmetik* formalisiert, ist entweder *inkonsistent* oder *unvollständig*.
- Gödels 2. *Unvollständigkeitssatz*:
  - Jeder *Logik*, die ihre eigene *Konsistenz* beweist, ist *inkonsistent*.
- Auswirkungen:
  - *Hilbert's Programm* terminiert nicht.
  - *Programme* nicht vollständig spezifierbar.
  - *Spezifikationssprachen* immer *unvollständig* (oder uninteressant).
  - Mit *anderen Worten*: *Es bleibt spannend*.