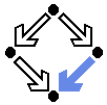
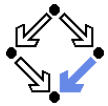
Berechenbarkeit und Komplexität

Wolfgang Schreiner
Wolfgang.Schreiner@risc.jku.at

Research Institute for Symbolic Computation (RISC)
Johannes Kepler University, Linz, Austria
http://www.risc.jku.at



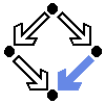
Die Grenzen der Informatik



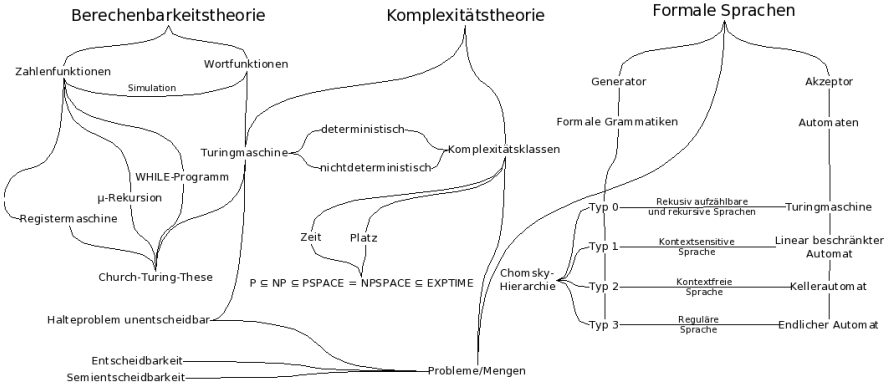
- Physik: das Perpetuum Mobile.
  Bauen Sie eine Maschine, die einmal in Gang gesetzt, ohne Zufuhr von Energie ewig in Bewegung bleibt.
  - Unmöglich: Verletzung des zweiten Hauptsatzes der Thermodynamik!
    - Die Entropie nimmt immer zu.
- Mathematik: die Quadratur des Kreises.
  Konstruieren Sie, nur mit Lineal und Zirkel, aus einem gegebenen Kreis ein Quadrat mit dem gleichen Flächeninhalt.
  - Unmöglich: π ist keine algebraische Zahl!
    - Nur Nullstellen von Polynomen mit rationalen Koeff. konstruierbar.
- Informatik: das Halteproblem.
  Schreiben Sie ein Programm, das entscheidet, ob ein beliebiges Programm für eine gegebene Eingabe terminiert.
  - Unmöglich: die Sprache L_h ist nicht rekursiv.
    - Es gibt keine Turing-Maschine, die die Sprache $L_h = \{(\langle M \rangle, w) \mid M \text{ hält bei Eingabe } w \text{ an}\}$ entscheidet.

Man sollte die Gesetze und Grenzen des jeweiligen Fachbereichs kennen.

Das Große Bild

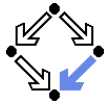


Aus Wikipedia (Urheber: Matthias Kleine).



Wir werden uns mit ausgewählten Punkten aus diesem Bild beschäftigen.

Grundlegende Fragestellungen

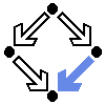


Die Suche nach den ewigen Wahrheiten in der Informatik.

- Der Begriff des Algorithmus:
  - Was heißt eigentlich "Rechnen" und wann ist etwas "berechenbar"?
- Die Komplexität von Algorithmen:
  - Mit welchem Aufwand (Rechenzeit und Speicherplatz) wird eine Berechnung ausgeführt?
- Entscheidbarkeit und Unentscheidbarkeit:
  - Welche Probleme sind durch Algorithmen grundsätzlich lösbar und welche nicht?
- Problemkomplexität:
  - Wie kann man Probleme nach dem für ihre Lösung erforderlichen Aufwand (bzw. nach dem Grad ihrer Unlösbarkeit) klassifizieren?

Die Antworten auf diese Fragen sind im wesentlichen unabhängig von dem jeweils aktuellen Stand der Informationstechnik.

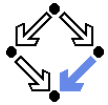
Wesentliche Persönlichkeiten



- Kurt Gödel (1906-1978)
  - Unbeweisbarkeit arithmetischer Sätze.
    Gödelscher Unvollständigkeitssatz.
- Alonzo Church (1903-1995)
  - Entscheidbarkeit, λ-Kalkül.
    Church'sche These (Church-Turing These).
- Alan M. Turing (1912-1954)
  - Berechenbarkeit, Kryptographie, Künstliche Intelligenz.
    Turing-Maschine, Turing-Test, Turing-Award.
- Stephen C. Kleene (1909–1994)
  - Formale Sprachen, Automatentheorie.
- Richard M. Karp (1935-)
  - Komplexitätstheorie, $\mathcal{NP}$-Vollständigkeit.
- Stephen A. Cook (1939-)
  - Komplexitätstheorie, $\mathcal{NP}$-Vollständigkeit.
- ...

Bahnbrechende Arbeiten bereits *vor* der Entwicklung des Computers.

Praktische Ergebnisse

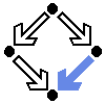


Die theoretische Informatik ... bietet Grundlagen für den Bau von Compilern von Programmiersprachen und die mathematische Formalisierung von Problemstellungen. Sie ist somit das formale Rückgrat der Informatik. Dabei werden formale Systeme, Automaten, Graphen und Syntaxdiagramme dazu genutzt, die innere Logik eines formalen Problems exakt wiederzugeben. Oft ist dieser formale Schritt ein wesentlicher Teil zur Lösung der eigentlichen Problemstellung und erschließt eine durch Maschinensemantik noch bequemer gewordene Welt der Mathematik und Computerei. (Wikipedia)

- Compilerbau, Sprachverarbeitung.
  - Analyse und Übersetzung formaler Sprachen.
- Spezifikation und Modellierung von Systemen.
  - Hardware, Software, Kombinationen aus Hard- und Software.
- Verifikation von System-Eigenschaften.
  - Extended static checking, model checking, automated reasoning.

Die Fähigkeit zum Modellieren und Schließen über IT-Systeme wird in Zukunft einen entscheidenden Wettbewerbsvorteil ausmachen.

Organisation der Lehrveranstaltung



- Web-Seite: siehe KUSSS.

  `http://www.risc.jku.at`
  `/people/schreine/courses/ws2010/bekomp`

  - Ankündigungen, Übungsaufgaben, Probeklausuren.
  - Registierung als Benutzer: Fragen im Forum, Antworten per Email.
- Vorlesung: Wolfgang Schreiner.
  - Skriptum, Folien.
  - Klausur: 4. Februar 2011 (Unterlagen erlaubt).
- Übungen: Ralf Hemmecke und Burkhard Zimmermann.
  - 3 Gruppen.
  - Wöchentliche Aufgaben.
  - 2 Übungsklausuren (keine Unterlagen erlaubt).

Fragen (vorzugsweise) im Forum oder per Email bzw. vor/nach jeder Lehrveranstaltung (sonstige Termine per Email vereinbaren).