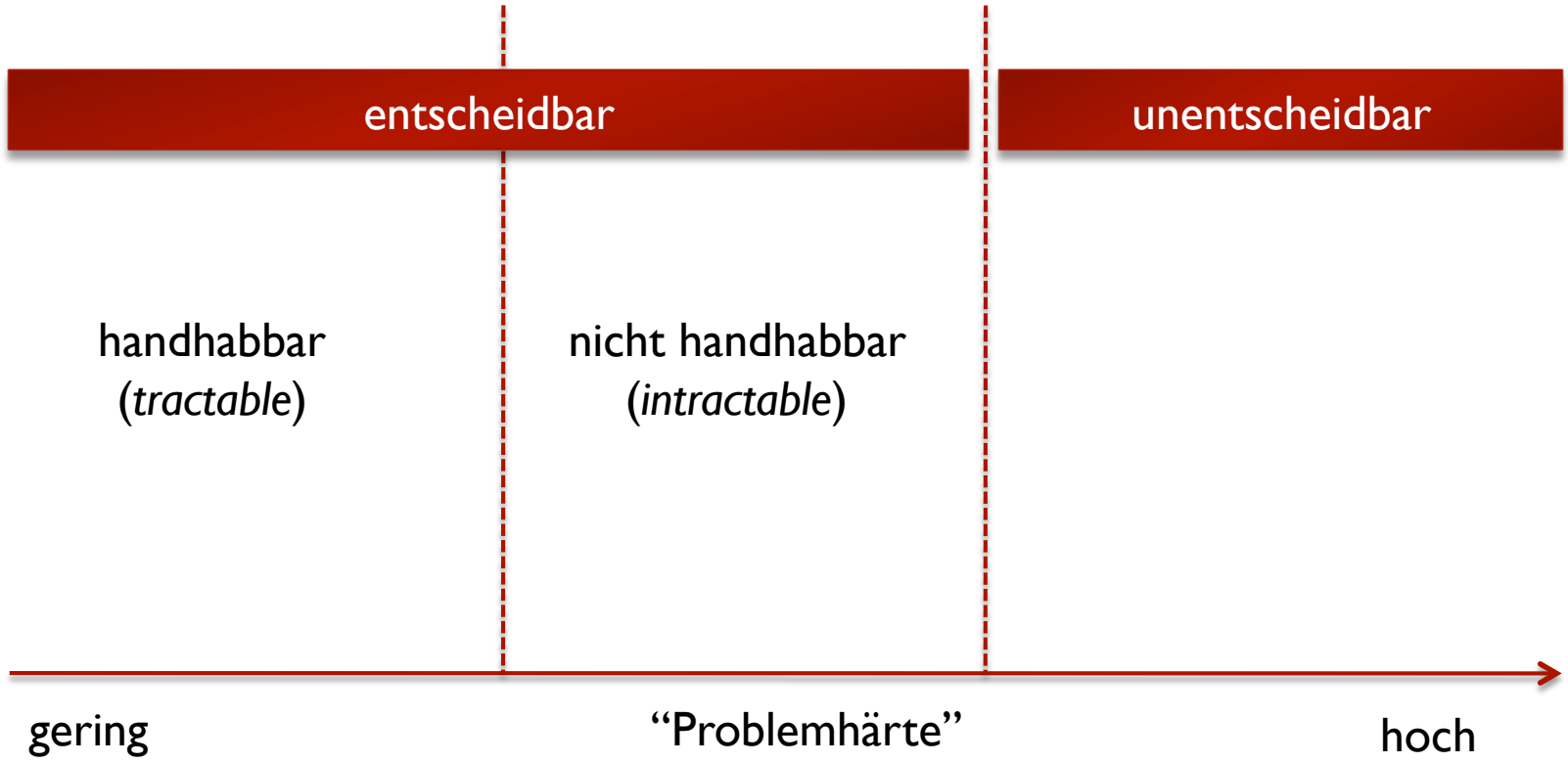
Entscheidungsverfahren für die Software-Verifikation

2 - Grundlagen

Entscheidungsverfahren

- Gegeben:
  1. Grundmenge M = { $P_1, P_2, \ldots$ } von Probleminstanzen
  2. Eigenschaft E einer Probleminstanz
- Gefragt:
  - Gilt E für eine Instanz P_i?
  - Gibt es einen Algorithmus, der für alle $P_i \in M$ diese Frage beantworten kann?
- Formale Definition von Entscheidbarkeit:
  - Eine Teilmenge T (über die Eigenschaft E definiert) einer Menge M heißt entscheidbar, wenn ihre charakteristische Funktion $\chi_T: M \rightarrow \{0,1\}$ berechenbar ist.
- Entscheidungsproblem:
  - Ist für eine Grundmenge M eine Eigenschaft E entscheidbar?
- Entscheidungsverfahren:
  - Algorithmus, der χ_T berechnet.

Problemhärte / Entscheidbarkeit



Beispiele für Entscheidungsprobleme

Grundmenge	Eigenschaft
Graphen	Ist derGraph k-färbbar / enthält er eine k-Clique?
(Syntaktisch korrekte) Formeln der Aussagenlogik	Ist die Formel erfüllbar / allgemeingültig?
Paare (F,G) von Formeln der Prädikatenlogik erster Stufe	Folgt G aus F?
(Syntaktisch korrekte) C-Programme	Terminiert das Programm?
(Syntaktisch korrekte) C-Programme	Terminiert das Programm in höchstens k Schritten?
Turingmaschinen-Programme	Benötigt das Programm höchstens k Zellen auf dem Band?

Aussagenlogische Erfüllbarkeit

- M: Wohlgeformte aussagenlogische Formeln in konjunktiver Normalform (CNF)
- T: Erfüllbare Formeln (T = SAT)
- Wie sieht ein Entscheidungsverfahren für SAT aus?
  - Aufzählungsverfahren
    - Z.B. anhand der Wahrheitstafel
  - Deduktionsverfahren
    - Z.B. Hilbertkalkül, Modus-Ponens (beide eher für TAUT), Resolution

Bedeutung SAT

- **Theoretisch:** SAT NP-vollständig
  - D.h. jedes NP-schwere Entscheidungsproblem lässt sich mittels SAT lösen
- **Praktisch:** Anwendungen in…
  - Hardware-Design-Verifikation
  - Software-Verifikation
  - Planung (auch Zeitplanung / Ablaufplanung)
  - Existenz von endlichen mathematischen Strukturen
- SAT wird als Basisverfahren in vielen Bereichen eingesetzt!