Berechenbarkeit

Vorlesung 11: Polynomielle Entscheidbarkeit

3. Juli 2025

Termine — Modul Berechenbarkeit

Übungen	Prüfung	Vorlesung
1.7. Übung 6 A-Woche	2.7. ———	3.7. Klasse P
8.7. Abschlussübung (beide Wochen) (Mo+Di FKH, Mi Hs.8)	9.7. ———	10.7. NP-Vollständigkeit
15.7. ———	16.7. Prüfung ab 13:30 Uhr in AudiMax & Hs. 9	17.7. ———

Raumänderung Übungen letzte Woche

Montag (7.7.)	Dienstag (8.7.)	Mittwoch (9.7.)
Felix-Klein-Hörsaal		Hörsaal 8

Beweissystem

Notizen

- **Beweissystem** = Formelmenge $\mathcal{F}$ + Inferenzregeln $\mathcal{R}$
- **Beweis** = Folge $(F_1, \ldots, F_n)$ von Formeln aus $\mathcal{F}$; für alle $1 \leq i \leq n$ Formel F_i vermittels Regel aus $\mathcal{R}$ aus $\{F_1, \ldots, F_{i-1}\}$ herleitbar

Beweissystem

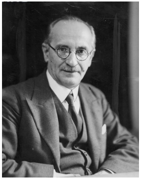
Łukasiewicz-Logik

- Formelmenge $\mathcal{F}$ = aussagenlogische Formeln über $\rightarrow$ und $\neg$
- Inferenzregeln $\mathcal{R}$

$$
\begin{aligned}
&\vdash F \rightarrow (F' \rightarrow F) \\
&\vdash (F \rightarrow (F' \rightarrow F'')) \rightarrow ((F \rightarrow F') \rightarrow (F' \rightarrow F'')) \\
&\vdash (\neg F \rightarrow \neg F') \rightarrow (F' \rightarrow F) \\
\{F, F \rightarrow F'\} &\vdash F' \qquad \text{(modus ponens)}
\end{aligned}
$$

Jan Łukasiewicz (* 1878; † 1956)

- Poln. Logiker & Philosoph
- Beiträge Aussagenlogik & mehrwertiger Logik
- Erfinder polnischer Notation



Beweissystem

§11.1 Definition (abstraktes Beweissystem; *abstract proof system*)

Abstraktes Beweissystem über Γ^* ist Paar $(\mathcal{B}, f)$ mit

- $\mathcal{B} \subseteq \Sigma^*$ entscheidbar (Menge gültiger Beweise)
- $f\colon \mathcal{B} \to \Gamma^*$ berechenbar und total (Zuordnung Beweis zu Aussage)

Beweissystem

§11.1 Definition (abstraktes Beweissystem; *abstract proof system*)

Abstraktes Beweissystem über Γ^* ist Paar $(\mathcal{B}, f)$ mit

- $\mathcal{B} \subseteq \Sigma^*$ entscheidbar (Menge gültiger Beweise)
- $f : \mathcal{B} \to \Gamma^*$ berechenbar und total (Zuordnung Beweis zu Aussage)

Łukasiewicz-Logik

- Beweise $\mathcal{B}$ offenbar entscheidbar
- Bewiesene Aussage = letztes Element des Beweises
  Damit f berechenbar

Beweissystem

§11.2 Definition (korrekt, vollständig; *sound, complete*)

Abstraktes Beweissystem $(\mathcal{B}, f)$ über Γ^* ist für Aussagen $\mathcal{T} \subseteq \Gamma^*$

- **korrekt** falls $f(B) \in \mathcal{T}$ für alle $B \in \mathcal{B}$
  (jeder Beweis "beweist" Aussage aus $\mathcal{T}$)

Beweissystem

§11.2 Definition (korrekt, vollständig; *sound, complete*)

Abstraktes Beweissystem $(\mathcal{B}, f)$ über Γ^* ist für Aussagen $\mathcal{T} \subseteq \Gamma^*$

- **korrekt** falls $f(B) \in \mathcal{T}$ für alle $B \in \mathcal{B}$
  (jeder Beweis "beweist" Aussage aus $\mathcal{T}$)
- **vollständig** falls $B \in \mathcal{B}$ mit $f(B) = F$ für alle $F \in \mathcal{T}$ existiert
  (jede Aussage aus $\mathcal{T}$ beweisbar)

Beweissystem

§11.2 Definition (korrekt, vollständig; *sound, complete*)

Abstraktes Beweissystem $(\mathcal{B}, f)$ über Γ^* ist für Aussagen $\mathcal{T} \subseteq \Gamma^*$

- **korrekt** falls $f(B) \in \mathcal{T}$ für alle $B \in \mathcal{B}$
  (jeder Beweis "beweist" Aussage aus $\mathcal{T}$)
- **vollständig** falls $B \in \mathcal{B}$ mit $f(B) = F$ für alle $F \in \mathcal{T}$ existiert
  (jede Aussage aus $\mathcal{T}$ beweisbar)

Notiz

- Łukasiewicz-Logik für aussagenlog. Tautologien über $\rightarrow$ und $\neg$
  - Korrekt — nur Tautologien beweisbar
  - Vollständig — jede Tautologie beweisbar

Satz von Gödel

§11.3 Theorem (Unvollständigkeitssatz von Gödel)

Jedes abstrakte Beweissystem ist für WA inkorrekt oder unvollständig

Satz von Gödel

§11.3 Theorem (Unvollständigkeitssatz von Gödel)

Jedes abstrakte Beweissystem ist für WA inkorrekt oder unvollständig

Beweis

Sei $(\mathcal{B}, f)$ korrektes und vollständiges abstraktes Beweissystem für WA. Da $\mathcal{B} \neq \emptyset$ und $\mathcal{B}$ entscheidbar, ist $\mathcal{B}$ rekursiv aufzählbar. Also existiert $g\colon \mathbb{N} \to \mathcal{B}$ surjektiv und berechenbar.

Satz von Gödel

§11.3 Theorem (Unvollständigkeitssatz von Gödel)

Jedes abstrakte Beweissystem ist für WA inkorrekt oder unvollständig

Beweis

Sei $(\mathcal{B}, f)$ korrektes und vollständiges abstraktes Beweissystem für WA. Da $\mathcal{B} \neq \emptyset$ und $\mathcal{B}$ entscheidbar, ist $\mathcal{B}$ rekursiv aufzählbar. Also existiert $g \colon \mathbb{N} \to \mathcal{B}$ surjektiv und berechenbar. Dann $(g\,;f) \colon \mathbb{N} \to \Gamma^*$ berechenbar.

Satz von Gödel

§11.3 Theorem (Unvollständigkeitssatz von Gödel)

Jedes abstrakte Beweissystem ist für WA inkorrekt oder unvollständig

Beweis

Sei $(\mathcal{B}, f)$ korrektes und vollständiges abstraktes Beweissystem für WA. Da $\mathcal{B} \neq \emptyset$ und $\mathcal{B}$ entscheidbar, ist $\mathcal{B}$ rekursiv aufzählbar. Also existiert $g \colon \mathbb{N} \to \mathcal{B}$ surjektiv und berechenbar. Dann $(g\,;f) \colon \mathbb{N} \to \Gamma^*$ berechenbar. Aus Korrektheit folgt $f \colon \mathcal{B} \to \mathsf{WA}$ und aus Vollständigkeit folgt Surjektivität von $f \colon \mathcal{B} \to \mathsf{WA}$. Also $(g\,;f) \colon \mathbb{N} \to \mathsf{WA}$ surjektiv.

Satz von Gödel

§11.3 Theorem (Unvollständigkeitssatz von Gödel)

Jedes abstrakte Beweissystem ist für WA inkorrekt oder unvollständig

Beweis

Sei $(\mathcal{B}, f)$ korrektes und vollständiges abstraktes Beweissystem für WA. Da $\mathcal{B} \neq \emptyset$ und $\mathcal{B}$ entscheidbar, ist $\mathcal{B}$ rekursiv aufzählbar. Also existiert $g\colon \mathbb{N} \to \mathcal{B}$ surjektiv und berechenbar. Dann $(g\,;f)\colon \mathbb{N} \to \Gamma^*$ berechenbar. Aus Korrektheit folgt $f\colon \mathcal{B} \to \mathsf{WA}$ und aus Vollständigkeit folgt Surjektivität von $f\colon \mathcal{B} \to \mathsf{WA}$. Also $(g\,;f)\colon \mathbb{N} \to \mathsf{WA}$ surjektiv. Damit WA rekursiv aufzählbar im Widerspruch zu Theorem §10.15 ↯ $\square$

Satz von Gödel

Konsequenzen

- Jedes vollständige Beweissystem für WA ist inkorrekt
- Jedes korrekte Beweissystem für WA ist unvollständig
  (nicht alle wahren Sätze von WA lassen sich beweisen)

Kurt Gödel (* 1906; † 1978)

- Öster.-amer. Logiker, Mathematiker & Philosoph
- Bedeutendster Logiker; Gödel-Nummern
- Widerlegte Hilbertsche Grundsatzprogramm
  (alle Sätze basierend auf Arithmetik ableitbar)

Komplexitätstheorie

Entscheidbarkeit

- Grundlegende Problem-Lösbarkeit
- Keine Beschränkung der Ressourcen (Zeit, Speicher)
- Entscheidbar $\neq$ praktisch lösbar

Komplexitätstheorie

Entscheidbarkeit

- Grundlegende Problem-Lösbarkeit
- Keine Beschränkung der Ressourcen (Zeit, Speicher)
- Entscheidbar $\neq$ praktisch lösbar

Komplexitätstheorie

- Obere & untere Schranken Ressourcen für jedwede Problemlösung
- Genauere Charakterisierung (Unterteilung) der Entscheidbarkeit
  (effizient, ineffizient lösbar, praktisch unlösbar, unentscheidbar)

Komplexitätstheorie

Problem des Handelsreisenden

- Geg. n Orte, Distanzmatrix $D \in \mathbb{N}^{n \times n}$ für Orte & Länge $\ell \in \mathbb{N}$
- Existiert Permutation $\pi = (\pi_1, \dots, \pi_n)$ von $(1, \dots, n)$ mit $D(\pi) \leq \ell$

$$D(\pi) = \left(\sum_{i=1}^{n-1} D_{\pi_i, \pi_{i+1}} \right) + D_{\pi_n, \pi_1} \quad \text{(Summe Distanzen in Rundreise)}$$

Komplexitätstheorie

Problem des Handelsreisenden

- Geg. n Orte, Distanzmatrix $D \in \mathbb{N}^{n \times n}$ für Orte & Länge $\ell \in \mathbb{N}$
- Existiert Permutation $\pi = (\pi_1, \ldots, \pi_n)$ von $(1, \ldots, n)$ mit $D(\pi) \leq \ell$

$$D(\pi) = \left(\sum_{i=1}^{n-1} D_{\pi_i, \pi_{i+1}}\right) + D_{\pi_n, \pi_1} \quad \text{(Summe Distanzen in Rundreise)}$$

- Entscheidbar per Berechnung $D(\pi)$ für alle $n!$ Permutationen π

Komplexitätstheorie

Problem des Handelsreisenden

- Geg. n Orte, Distanzmatrix $D \in \mathbb{N}^{n \times n}$ für Orte & Länge $\ell \in \mathbb{N}$
- Existiert Permutation $\pi = (\pi_1, \ldots, \pi_n)$ von $(1, \ldots, n)$ mit $D(\pi) \leq \ell$

$$D(\pi) = \left(\sum_{i=1}^{n-1} D_{\pi_i, \pi_{i+1}}\right) + D_{\pi_n, \pi_1} \quad \text{(Summe Distanzen in Rundreise)}$$

- Entscheidbar per Berechnung $D(\pi)$ für alle $n!$ Permutationen π
- Sei $n = 40$ und berechne $D(\pi)$ für 10^{11} Permutationen π pro s
- Laufzeit ca. $2,6 \cdot 10^{29}$ Jahre (Alter Universum ca. $1,4 \cdot 10^{10}$ Jahre)

Komplexitätstheorie

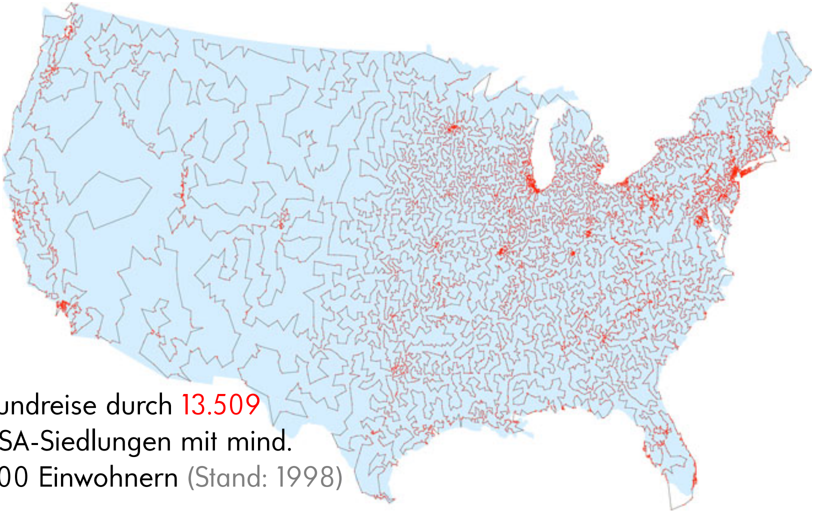
Optimale Rundreise
durch 15 größte
Städte Deutschlands

$15! \approx 1,3 \cdot 10^{12}$

(© Amirki)

Komplexitätstheorie

(© David Applegate, Robert Bixby, Vasek Chvatal und William Cook)



Rundreise durch 13.509 USA-Siedlungen mit mind. 500 Einwohnern (Stand: 1998)

Komplexitätstheorie

Notizen

- Obere Schranke: Analyse “guter” Lösungsalgorithmus
- Untere Schranke: Problemanalyse & Reduktionen

Komplexitätstheorie

Notizen

- Obere Schranke: Analyse “guter” Lösungsalgorithmus
- Untere Schranke: Problemanalyse & Reduktionen

Beobachtung

- Effizientere Algorithmen für Handelsreisenden-Problem bekannt
- Problem bleibt “schwierig”

Komplexitätstheorie

Kürzester Weg

- Geg. Orte $s, z \in \{1, \dots, n\}$, Distanzmatrix $D \in \mathbb{N}^{n \times n}$, Länge $\ell \in \mathbb{N}$
- Existiert Pfad π von s nach z mit Länge $D(\pi) \leq \ell$

Komplexitätstheorie

Kürzester Weg

- Geg. Orte $s, z \in \{1, \ldots, n\}$, Distanzmatrix $D \in \mathbb{N}^{n \times n}$, Länge $\ell \in \mathbb{N}$
- Existiert Pfad π von s nach z mit Länge $D(\pi) \leq \ell$

- Entscheidbar per Berechnung kürzester Pfad von s nach z
- <u>Effizient</u> und selbst für sehr große n lösbar

Komplexitätstheorie

Kürzester Weg

- Geg. Orte $s, z \in \{1, \ldots, n\}$, Distanzmatrix $D \in \mathbb{N}^{n \times n}$, Länge $\ell \in \mathbb{N}$
- Existiert Pfad π von s nach z mit Länge $D(\pi) \leq \ell$

- Entscheidbar per Berechnung kürzester Pfad von s nach z
- Effizient und selbst für sehr große n lösbar

Notizen

- Entscheidbarkeit unterscheidet beide Probleme nicht
- Unterscheidung effizient lösbar & schwierig (aber lösbar) gesucht

Polynomielle Berechenbarkeit

§11.4 Definition (Notation für obere Schranken; *big-O notation*)

Gegeben Funktion $f\colon \mathbb{N} \to \mathbb{N}$

$$\mathcal{O}(f) = \left\{ g\colon \mathbb{N} \to \mathbb{N} \mid \exists x_0, a, b \in \mathbb{N}, \forall x \geq x_0 \colon g(x) \leq a \cdot f(x) + b \right\}$$

Polynomielle Berechenbarkeit

§11.4 Definition (Notation für obere Schranken; *big-O notation*)

Gegeben Funktion $f \colon \mathbb{N} \to \mathbb{N}$

$$\mathcal{O}(f) = \left\{g \colon \mathbb{N} \to \mathbb{N} \mid \exists x_0, a, b \in \mathbb{N}, \forall x \geq x_0 \colon g(x) \leq a \cdot f(x) + b\right\}$$

Notizen

- $4x^2 + 3x + 3 \in \mathcal{O}(x^2)$
- $x \cdot \log x \in \mathcal{O}(x^2)$
- $\sqrt{x} \in \mathcal{O}(x)$

Polynomielle Berechenbarkeit

§11.5 Definition (polyn. berechenbar; *polynomially computable*)

(Totale) Funktion $g \colon \Sigma^* \to \Gamma^*$ **polynomiell berechenbar**
falls det. TM M und Polynom P existieren mit

- $T(M) = g$ und
- M hält auf Eingabe $w \in \Sigma^*$ nach höchstens $P(|w|)$ Schritten

Polynomielle Berechenbarkeit

§11.5 Definition (polyn. berechenbar; *polynomially computable*)

(Totale) Funktion $g\colon \Sigma^* \to \Gamma^*$ **polynomiell berechenbar** falls det. TM M und Polynom P existieren mit

- $T(M) = g$ und
- M hält auf Eingabe $w \in \Sigma^*$ nach höchstens $P(|w|)$ Schritten

Notizen

- Polynom sichert (weitreichende) Modellunabhängigkeit
- Polynom separiert exponentielles (und schlimmeres) Verhalten
- Polynomiell berechenbar impliziert berechenbar & total

Polynomielle Berechenbarkeit

§11.6 Definition (polyn. entscheidbar; *polynomially decidable*)

Problem $L \subseteq \Sigma^*$ **polynomiell entscheidbar**
falls charakteristische Funktion χ_L polynomiell berechenbar

$$\chi_L \colon \Sigma^* \to \{0,1\} \qquad \text{mit} \qquad \chi_L(w) = \begin{cases} 1 & \text{falls } w \in L \\ 0 & \text{sonst} \end{cases}$$

Polynomielle Berechenbarkeit

§11.6 Definition (polyn. entscheidbar; *polynomially decidable*)

Problem $L \subseteq \Sigma^*$ **polynomiell entscheidbar**
falls charakteristische Funktion χ_L polynomiell berechenbar

$$\chi_L \colon \Sigma^* \to \{0,1\} \qquad \text{mit} \qquad \chi_L(w) = \begin{cases} 1 & \text{falls } w \in L \\ 0 & \text{sonst} \end{cases}$$

Notizen

- Gleiche Begriffe für While-Programme, μ-Rekursion, etc.
  (polynomielle Transformationen)
- Berühmte Komplexitätsklasse **P**

$$\mathbf{P} = \{L \mid L \text{ polynomiell entscheidbar}\}$$

Nichtdeterminismus

Ausnahme

- Transformation TM in det. TM exponentiell
- Anderer Begriff polynomieller Entscheidbarkeit für nichtdet. TM
- Definition über Zertifikatverifikation
  (Alternative im Schöning-Buch)

Nichtdeterminismus

§11.7 Definition *(nondeterministically polynomially decidable)*

Problem $L \subseteq \Sigma^*$ **nichtdeterministisch polynomiell entscheidbar** falls Alphabet Γ, Relation $R \subseteq \Sigma^* \times \Gamma^*$ und $k \in \mathbb{N}$ existieren mit

- $\{w\#z \mid (w, z) \in R\} \in \mathrm{P}$ polynomiell entscheidbar und
- $w \in L$ gdw. $z \in \Gamma^*$ existiert mit $(w, z) \in R$ und $|z| \leq |w|^k$ für jedes $w \in \Sigma^*$

Nichtdeterminismus

§11.7 Definition *(nondeterministically polynomially decidable)*

Problem $L \subseteq \Sigma^*$ **nichtdeterministisch polynomiell entscheidbar** falls Alphabet Γ, Relation $R \subseteq \Sigma^* \times \Gamma^*$ und $k \in \mathbb{N}$ existieren mit

- $\{w\#z \mid (w, z) \in R\} \in \mathsf{P}$ polynomiell entscheidbar und
- $w \in L$ gdw. $z \in \Gamma^*$ existiert mit $(w, z) \in R$ und $|z| \leq |w|^k$ für jedes $w \in \Sigma^*$

Notizen

- Polynomiell entscheidbare Zertifikatrelation R
- Zertifikate polynomieller Länge
- 2 berühmte Klassen

$$\begin{aligned} \mathbf{P} &= \{L \mid L \text{ polynomiell entscheidbar}\} \\ \mathbf{NP} &= \{L \mid L \text{ nichtdeterministisch polynomiell entscheidbar}\} \end{aligned}$$

Nichtdeterminismus

Rucksack-Problem

- Geg. $n_1, \ldots, n_k \in \mathbb{N}$ und $n \in \mathbb{N}$ in Binärkodierung
  (Gegenstandsgrößen & Rucksackgröße)
- Existiert $I \subseteq \{1, \ldots, k\}$ mit $\sum_{i \in I} n_i = n$?
  (Kann Rucksack vollständig gefüllt werden?)

Nichtdeterminismus

Rucksack-Problem

- Geg. $n_1, \ldots, n_k \in \mathbb{N}$ und $n \in \mathbb{N}$ in Binärkodierung
  (Gegenstandsgrößen & Rucksackgröße)
- Existiert $I \subseteq \{1, \ldots, k\}$ mit $\sum_{i \in I} n_i = n$?
  (Kann Rucksack vollständig gefüllt werden?)
- Polynomielle Entscheidbarkeit

Nichtdeterminismus

Rucksack-Problem

- Geg. $n_1, \dots, n_k \in \mathbb{N}$ und $n \in \mathbb{N}$ in Binärkodierung
  (Gegenstandsgrößen & Rucksackgröße)
- Existiert $I \subseteq \{1, \dots, k\}$ mit $\sum_{i \in I} n_i = n$?
  (Kann Rucksack vollständig gefüllt werden?)
- Polynomielle Entscheidbarkeit unklar
- Nichtdet. polynomielle Entscheidbarkeit

Nichtdeterminismus

Rucksack-Problem

- Geg. $n_1, \ldots, n_k \in \mathbb{N}$ und $n \in \mathbb{N}$ in Binärkodierung
  (Gegenstandsgrößen & Rucksackgröße)
- Existiert $I \subseteq \{1, \ldots, k\}$ mit $\sum_{i \in I} n_i = n$?
  (Kann Rucksack vollständig gefüllt werden?)
- Polynomielle Entscheidbarkeit   unklar
- Nichtdet. polynomielle Entscheidbarkeit   ja, in **NP**

Nichtdeterminismus

Rucksack-Problem

- Geg. $n_1, \dots, n_k \in \mathbb{N}$ und $n \in \mathbb{N}$ in Binärkodierung
  (Gegenstandsgrößen & Rucksackgröße)
- Existiert $I \subseteq \{1, \dots, k\}$ mit $\sum_{i \in I} n_i = n$?
  (Kann Rucksack vollständig gefüllt werden?)
- Polynomielle Entscheidbarkeit unklar
- Nichtdet. polynomielle Entscheidbarkeit ja, in **NP**
  - Zertifikatrelation mit $\Gamma = \{0, 1\}$

$$R = \Big\{ \big(\mathrm{bin}(n_1) \# \cdots \# \mathrm{bin}(n_k) \# \mathrm{bin}(n), i_1 \cdots i_k\big) \;\Big|\; \sum_{\substack{\ell=1 \\ i_\ell \neq 0}}^{k} n_\ell = n \Big\}$$

  - R polynomiell entscheidbar (While-Programm überprüft Summe)
  - Instanz w lösbar gdw. $\exists z \in \Gamma^k$ mit $(w, z) \in R$

Determinismus vs. Nichtdeterminismus

§11.8 Theorem

$\mathbf{P} \subseteq \mathbf{NP}$

Beweis

Sei $L \in \mathbf{P}$. Wähle $\Gamma = \Sigma$, $R = \{(w, w) \mid w \in L\}$ und $k = 1$

Determinismus vs. Nichtdeterminismus

§11.8 Theorem

$\mathbf{P} \subseteq \mathbf{NP}$

Beweis

Sei $L \in \mathbf{P}$. Wähle $\Gamma = \Sigma$, $R = \{(w, w) \mid w \in L\}$ und $k = 1$

$$\begin{aligned} w \in L &\iff (w, w) \in R \\ &\iff \exists z\colon (w, z) \in R \text{ und } |z| \leq |w| \end{aligned}$$

$\{w\#w \mid w \in L\}$ polynomiell entscheidbar, da $L \in \mathbf{P}$ $\square$

Determinismus vs. Nichtdeterminismus

Notizen

- Nichtdet. TM rät & überprüft “kurzen” Lösungsnachweis (Zertifikat)
- Nichtdet. TM benötigt keine Suche
  Det. TM benötigt aktuell Suche nach solchen Zertifikaten

Determinismus vs. Nichtdeterminismus

Notizen

- Nichtdet. TM rät & überprüft “kurzen” Lösungsnachweis (Zertifikat)
- Nichtdet. TM benötigt keine Suche
  Det. TM benötigt aktuell Suche nach solchen Zertifikaten

- Polynomiell berechenbar $\approx$ effizient berechenbar
- Nichtdeterminismus vermutlich nicht effizient simulierbar

Determinismus vs. Nichtdeterminismus

$\mathbf{P} \subseteq \mathbf{NP}$ gilt, aber

Beweis $\mathbf{NP} \subseteq \mathbf{P}$ oder $\mathbf{P} \subsetneq \mathbf{NP}$ 1 Million USD wert

- Wichtigstes Problem der theoretischen Informatik
- 1 der 7 Milleniumprobleme der Mathematik

Zusammenfassung

- Unvollständigkeitssatz von Gödel
- Polynomielle Entscheidbarkeit (Klasse **P**)
- Nichtdet. polynomielle Entscheidbarkeit (Klasse **NP**)

Sechste Übungsserie bereits im Moodle