Polynomielle Berechenbarkeit

Wortproblem kontextsensitiver Sprache

- Ist geg. $w \in \Sigma^*$ in Sprache $L(G)$ kontextsensitiver Grammatik $G = (N, \Sigma, S, P)$?
- Problem $L(G)$

- Entscheidbarkeit von $L(G)$ entscheidbar
- Polynomielle Entscheidbarkeit von $L(G)$ unklar
- Nichtdet. polynomielle Entscheidbarkeit von $L(G)$ unklar

Polynomielle Berechenbarkeit

Sei $G = (N, \Sigma, S, P)$ kontextsensitive Grammatik

1. Setze $\mathcal{F} = \{S\}$ (nur Startsymbol)
2. Setze $\mathcal{F}' = \mathcal{F} \cup \{v \in (N \cup \Sigma)^{\leq |w|} \mid \exists u \in \mathcal{F} \colon u \Rightarrow_G v\}$ (füge Nachfolger der Länge höchstens $|w|$ hinzu)
3. Falls $\mathcal{F} \subsetneq \mathcal{F}'$, dann setze $\mathcal{F} = \mathcal{F}'$ und gehe zu 2.
4. Liefere Wahrheitswert von $w \in \mathcal{F}'$

Komplexität

- Potentiell $\sum_{i=0}^{|w|} (|N| + |\Sigma|)^i$ Elemente; exponentiell
- Ableitung als Zertifikat potentiell zu lang

Polynomielle Berechenbarkeit

Wortproblem kontextfreier Sprache

- Ist geg. $w \in \Sigma^*$ in Sprache $L(G)$ kontextfreier Grammatik $G = (N, \Sigma, S, P)$?
- Problem $L(G)$

- Entscheidbarkeit von $L(G)$ entscheidbar
- Polynomielle Entscheidbarkeit von $L(G)$ in **P**
- CYK-Algorithmus $\mathcal{O}(|w|^3)$

Polynomielle Berechenbarkeit

Problem des Handelsreisenden

- Hat geg. Distanzmatrix $D \in \mathbb{N}^{n \times n}$ Rundreise der Länge höchstens k?
- Problem TSP $= \{\langle D, k \rangle \mid D$ hat Rundreise der Länge höchstens $k\}$

- Entscheidbarkeit von TSP entscheidbar
- Polynomielle Entscheidbarkeit von TSP unklar
- Nichtdet. polynomielle Entscheidbarkeit von TSP ja, in NP
- Zertifikat ist Rundreise der Länge höchstens k

Polynomielle Problemreduktion

§12.1 Definition (polynomielle Reduktion; *polynomial reduction*)

Problem $L \subseteq \Sigma^*$ **polynomiell reduzierbar** auf $L' \subseteq \Gamma^*$, kurz $L \preceq_P L'$, falls polyn. ber. totale Funktion $f : \Sigma^* \to \Gamma^*$ mit $L = f^{-1}(L')$ existiert

Konsequenzen

- Seien $L \subseteq \Sigma^*$ und $L' \subseteq \Gamma^*$ mit $L \preceq_P L'$
- L polynomiell entscheidbar falls L' polynomiell entscheidbar
  ($L \in \mathbf{P}$ falls $L' \in \mathbf{P}$)
- L nichtdet. polyn. entscheidbar
  falls L' nichtdet. polyn. entscheidbar
  ($L \in \mathbf{NP}$ falls $L' \in \mathbf{NP}$)

Polynomielle Problemreduktion

Problem

- Keine untere Schranke per Reduktion
- Wie erhalten wir untere Schranken?

Stephen Arthur Cook (* 1939)

- Amer.-kan. Mathematiker & Informatiker
- Polynomielle Reduktion & **NP**-Vollständigkeit
- Turing-Preisträger

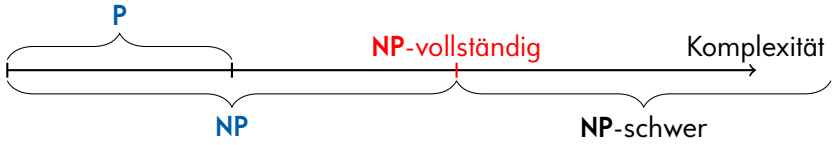
© Jiří Janíček

NP-Schwere & NP-Vollständigkeit

§12.2 Definition (NP-schwer, -vollständig; *NP-hard, -complete*)

Problem L

- **NP**-schwer falls $L' \preceq_P L$ für alle $L' \in \mathbf{NP}$
- **NP**-vollständig falls L **NP**-schwer und $L \in \mathbf{NP}$



Notizen

- **NP**-schwer = mind. so schwer wie alle Probleme in **NP**
  (untere Schranke)
- **NP**-vollständig = passende untere & obere Schranke **NP**

NP-Schwere & NP-Vollständigkeit

§12.3 Theorem

Sei L **NP**-vollständig. Dann $L \in \mathbf{P}$ gdw. $\mathbf{P} = \mathbf{NP}$

Beweis

Falls $\mathbf{P} = \mathbf{NP}$, dann $L \in \mathbf{P} = \mathbf{NP}$, da $L \in \mathbf{NP}$ (da **NP**-vollständig).

Umgekehrt sei $L \in \mathbf{P}$ und $L' \in \mathbf{NP}$ beliebig. Da L **NP**-vollständig und damit **NP**-schwer, gilt $L' \preceq_P L$. Zusammen mit $L \in \mathbf{P}$ folgt $L' \in \mathbf{P}$ und damit $\mathbf{NP} \subseteq \mathbf{P}$. Per Theorem §11.8 $\mathbf{P} \subseteq \mathbf{NP}$ und damit $\mathbf{P} = \mathbf{NP}$. □

NP-Schwere & NP-Vollständigkeit

Notizen

- Nachweis **NP**-Schwere schwierig
  (polynomielle Reduktion von jedem Problem aus **NP**)
- Mitgliedschaft in **NP** per nichtdet. polynomielle Entscheidbarkeit
  (Angabe geeigneter Zertifikatrelation)

NP-Schwere & NP-Vollständigkeit

§12.4 Theorem

Problem L **NP**-schwer, falls **NP**-schweres Problem L' mit $L' \preceq_P L$ existiert

Beweis

Sei L' **NP**-schwer und $L' \preceq_P L$. Dann $L'' \preceq_P L' \preceq_P L$ für alle $L'' \in \mathbf{NP}$.

Transitivität $\preceq_P$ liefert $L'' \preceq_P L$ für alle $L'' \in \mathbf{NP}$, womit L **NP**-schwer □

Schwierigkeit

- Bisher kein **NP**-schweres Problem

NP-Vollständigkeit

Erfüllbarkeit Aussagenlogik

- Geg. aussagenlogische Formel F
- F erfüllbar? (d.h. existiert Modell der Formel?)
- Problem SAT $= \{F \mid F$ erfüllbare Formel Aussagenlogik$\}$

- Entscheidbarkeit SAT entscheidbar
- Polynomielle Entscheidbarkeit SAT unklar
- Nichtdet. polynomielle Entscheidbarkeit SAT ja, in **NP**

NP-Vollständigkeit

Beispiele

- Erfüllbare Formel

  $F_1 = (x_2 \vee (x_1 \wedge \neg x_3) \vee x_4) \wedge x_1 \quad F_1^I = (1 \vee (1 \wedge \neg 0) \vee 0) \wedge 1 = 1$

  Modell $I = \{x_1, x_2\}$, kurz 1100 $\quad x_1 = 1; x_2 = 1; x_3 = 0; x_4 = 0$
- Unerfüllbare Formel

  $$F_2 = ((\neg x_1 \wedge \neg x_3) \vee x_2) \wedge x_1 \wedge \neg x_2$$
- Erfüllbare Formel

  $F_3 = (\neg x_1 \vee x_3 \vee x_2) \wedge x_1 \wedge \neg x_2 \quad F_3^I = (\neg 1 \vee 1 \vee 0) \wedge 1 \wedge \neg 0 = 1$

  Modell $I = \{x_1, x_3\}$, kurz: 101 $\quad x_1 = 1; x_2 = 0; x_3 = 1$

NP-Vollständigkeit

§12.5 Theorem

SAT $\in$ **NP**

Beweis

Sei F aussagenlogische Formel mit k Atomen $\{x_1, \ldots, x_k\}$. Wir setzen $R = \{(F, I) \mid I \models F\}$; Zertifikat ist Modell. Repräsentation R polynomiell entscheidbar, denn While-Programm kann F dekodieren, Atome gemäß Interpretation I auswerten und Wahrheitswert von $I \models F$ bestimmen. Zertifikat hat Länge $k \leq |F|$ (Interpretation = Teilmenge repräsentiert als $\{0,1\}^k$) und $F \in$ SAT gdw. $(F, I) \in R$ für $I \subseteq \{x_1, \ldots, x_k\}$, wobei $(F, I) \in R$ gdw. $I \models F$. □

NP-Vollständigkeit

§12.6 Theorem

Existiert Formel U polynomieller Größe in k mit Atomen $x_1, \ldots, x_k$ und $|I| = 1$ für jedes Modell $I \models U$ mit $I \subseteq \{x_1, \ldots, x_k\}$

Beweis

Sei

$$U = \Big(\bigvee_{i=1}^{k} x_i\Big) \wedge \Big(\bigwedge_{1 \leq m < \ell \leq k} \neg(x_m \wedge x_\ell)\Big)$$

Formel hat Größe in $\mathcal{O}(k^2)$ und Teil $\bigvee_{i=1}^{k} x_i$ erzwingt mind. 1 Atom in I. Verbleibender Teil genau dann falsch, wenn $|I| \geq 2$. Also $|I| = 1$ für alle Modelle $I \models F$ □

NP-Vollständigkeit

§12.7 Theorem (Satz von Cook)

SAT **NP**-vollständig

Beweis (1/6)

SAT $\in$ **NP** bekannt; zu zeigen **NP**-Schwere
Sei $L \subseteq \Sigma^*$ Problem aus **NP**. Dann existieren Alphabet Γ, $k \geq 1$ und polynomiell entscheidbare Zertifikatrelation $R \subseteq \Sigma^* \times \Gamma^*$ mit

$$w \in L \text{ gdw. } (w, z) \in R \text{ und } |z| \leq |w|^k \text{ für ein } z \in \Gamma^*$$

Sei $M = (Q, \Sigma', \Gamma', \Delta, \square, q_0, q_+, q_-)$ det. TM, die R polynomiell berechnet und beschränkendes Polynom P. O.B.d.A.

- $Q = \{1, \ldots, k'\}$ und $\Gamma' = \{1, \ldots, k''\}$
- $(w, z) \in R$ impliziert $|z| = |w|^k$ (Zertifikate mit uniformer Länge)
- $t_{\max}(w) = P(1 + |w| + |w|^k)$ (ob. Schranke Laufzeit auf w)

NP-Vollständigkeit

Beweis (2/6)

Sei $w = \sigma_1 \cdots \sigma_\ell$. Konstruiere aussagenlogische Formel $F(w)$ mit folgenden Atomen für alle $0 \leq t \leq t_{\max}(w)$, $-t_{\max}(w) \leq i \leq t_{\max}(w)$, $q \in Q$ und $\gamma \in \Gamma'$

- $\mathrm{InState}_{t,q}$: Ist M bei Schritt t in Zustand q?
- $\mathrm{AtPos}_{t,i}$: Ist Kopf von M bei Schritt t an Bandposition i?
- $\mathrm{OnTape}_{t,i,\gamma}$: Steht Zeichen γ bei Schritt t an Bandposition i?

$$F(w) = A(w) \wedge I(w) \wedge T(w) \wedge E(w)$$

(wir geben offensichtliche Quantifikation nicht an)

Endbedingung $E(w) = \bigvee_t \mathrm{InState}_{t,q_+}$
(akzeptierender Zustand erreicht)

NP-Vollständigkeit

$F(w) = A(w) \wedge I(w) \wedge T(w) \wedge E(w)$
$Q = \{1, \ldots, k'\}$ und $\Gamma' = \{1, \ldots, k''\}$

Beweis (3/6)

Randbedingungen

$$A(w) = \bigwedge_{t} U(\mathsf{InState}_{t,1}, \ldots, \mathsf{InState}_{t,k'}) \wedge \bigwedge_{t} U(\mathsf{AtPos}_{t,-t_{\max}(w)}, \ldots, \mathsf{AtPos}_{t,t_{\max}(w)}) \wedge \bigwedge_{t,i} U(\mathsf{OnTape}_{t,i,1}, \ldots, \mathsf{OnTape}_{t,i,k''})$$

- Zu jedem Schritt in genau 1 Zustand
- Zu jedem Schritt an genau 1 Position
- Zu jedem Schritt steht genau 1 Zeichen an Position

NP-Vollständigkeit

$F(w) = A(w) \wedge I(w) \wedge T(w) \wedge E(w)$

Beweis (4/6)

Initialbedingungen

$$I(w) = \mathsf{InState}_{0,q_0} \wedge \mathsf{AtPos}_{0,0} \wedge \Big(\bigwedge_{m \notin \{0,\ldots,\ell^k+\ell\}} \mathsf{OnTape}_{0,m,\square} \Big) \wedge \Big(\bigwedge_{m=1}^{\ell} \mathsf{OnTape}_{0,m-1,\sigma_m} \Big) \wedge \mathsf{OnTape}_{0,\ell,\#} \wedge \Big(\bigwedge_{m=\ell+1}^{\ell^k+\ell} \neg \mathsf{OnTape}_{0,m,\square} \Big)$$

- Initial im Zustand q_0 und an Position 0
- Außerhalb Eingabe steht $\square$ auf Band
- Auf Band steht $w\#z$ für beliebiges $z \in \Gamma^{\ell^k}$

NP-Vollständigkeit

$F(w) = A(w) \wedge I(w) \wedge T(w) \wedge E(w)$

Beweis (5/6)

Übergangsbedingungen mit $\diamond = 0$, $\triangleleft = -1$ und $\triangleright = 1$

$$T(w) = \bigwedge_{\substack{t,i,\gamma \\ t \neq t_{\max}(w)}} \Big((\neg \mathsf{AtPos}_{t,i} \wedge \mathsf{OnTape}_{t,i,\gamma}) \rightarrow \mathsf{OnTape}_{t+1,i,\gamma} \Big) \wedge \bigwedge_{\substack{t,q,i,\gamma \\ t \neq t_{\max}(w), q \notin \{q_+,q_-\}}} \Big((\mathsf{InState}_{t,q} \wedge \mathsf{AtPos}_{t,i} \wedge \mathsf{OnTape}_{t,i,\gamma}) \rightarrow \bigvee_{((q,\gamma)\rightarrow(q',\gamma',d)) \in \Delta'} (\mathsf{InState}_{t+1,q'} \wedge \mathsf{AtPos}_{t+1,i+d} \wedge \mathsf{OnTape}_{t+1,i,\gamma'}) \Big)$$

- Band außerhalb aktueller Position erhalten
- Prüfe Vorbedingungen Übergang
- Für jeden Schritt führe passenden Übergang aus

NP-Vollständigkeit

$F(w) = A(w) \wedge I(w) \wedge T(w) \wedge E(w)$

Beweis (6/6)

Teilformeln polynomieller Länge in $|w|$ und $F(w)$ polynomiell berechenbar. Sei $w \in L$ mit Zertifikat $z \in \Gamma^{\ell^k}$. Dann $F(w)$ für Band $w\#z$ erfüllbar, da Berechnung von M simuliert und M akzeptiert. Umgekehrt sei $F(w)$ erfüllbar. Dann liefert Modell Zertifikat z und akzeptierende Berechnung det. TM M. Folglich $w \in L$. Also $w \in L$ gdw. $F(w)$ erfüllbar gdw. $F(w) \in \mathrm{SAT}$. Damit $L \preceq_{\mathrm{P}} \mathrm{SAT}$, womit SAT **NP**-schwer und **NP**-vollständig. $\square$

NP-vollständige Probleme

§12.8 Definition (konjunktive Normalform mit 3 Literalen)

Aussagenlogische Formel F in **konjunktiver Normalform mit 3 Literalen** (3KNF) falls $F = F_1 \wedge \cdots \wedge F_k$ für Formeln $F_1, \ldots, F_k$ mit $F_i = L_{i1} \vee L_{i2} \vee L_{i3}$ für alle $1 \leq i \leq k$ und Literale L_{i1}, L_{i2}, L_{i3}
(Literal = Atom oder negiertes Atom)

Beispiele

- $x_1 \vee x_2 \vee x_3$ in 3KNF
- $(x_1 \wedge x_2) \vee x_4$ nicht in 3KNF
- $x_1 \wedge (x_2 \vee x_1 \vee \neg x_3)$ nicht in 3KNF
- $(x_1 \vee x_1 \vee x_1) \wedge (x_2 \vee \neg x_1 \vee \neg x_3)$ in 3KNF
  (erlauben auch ≤ 3 Literale; dann 3. Beispiel in 3KNF)

NP-vollständige Probleme

Erfüllbarkeit 3KNF-Formel

- Geg. aussagenlogische Formel F in 3KNF
- Ist F erfüllbar? (Existiert Modell?)
- Problem 3-SAT $= \{F \mid F$ erfüllbare Formel in 3KNF$\}$

- Entscheidbarkeit 3-SAT entscheidbar
- Polynomielle Entscheidbarkeit 3-SAT unklar
- Nichtdet. polynomielle Entscheidbarkeit 3-SAT ja, in **NP**
  (denn 3-SAT $\preceq_{\mathsf{P}}$ SAT vermittels Identität; also 3-SAT $\in$ **NP**)

NP-vollständige Probleme

§12.9 Theorem

3-SAT **NP**-vollständig

Beweis (1/2)

Da 3-SAT $\in$ **NP** nur **NP**-Schwere per SAT $\preceq_{\mathsf{P}}$ 3-SAT zu zeigen. Sei F aussagenlogische Formel. Transformiere F in Negationsnormalform (Negationen nur vor Atomen). Sei T Syntaxbaum der erhaltenen Formel F' und für jeden Knoten w dieses Baumes sei

- $v(w) = T(w)$ falls Knotenbeschriftung $T(w)$ Literal
- sonst $v(w) = y$ für neues Atom y.

Konstruiere Formel $f(F) = v(\varepsilon) \wedge \bigwedge_{w \text{ innere Position in } T} F'_w$, in der für jedes w Formel F'_w durch Formel $v(w) \leftrightarrow (v(w_1)\ T(w)\ v(w_2))$ in 3KNF gegeben ist, wobei $T(w)$ Symbol ($\vee$ oder $\wedge$) an Position w und w_1/w_2 erste/zweite Kindposition von w (Tseitin-Transformation)

NP-vollständige Probleme

Beweis (2/2)

3KNF Teilformel F'_w gegeben durch

$(L_1 \leftrightarrow (L_2 \vee L_3))$ äq. zu $(L_1 \vee \neg L_2) \wedge (\neg L_1 \vee L_2 \vee L_3) \wedge (L_1 \vee \neg L_3)$

$(L_1 \leftrightarrow (L_2 \wedge L_3))$ äq. zu $(\neg L_1 \vee L_2) \wedge (L_1 \vee \neg L_2 \vee \neg L_3) \wedge (\neg L_1 \vee L_3)$

Offenbar $f(F)$ in 3KNF und

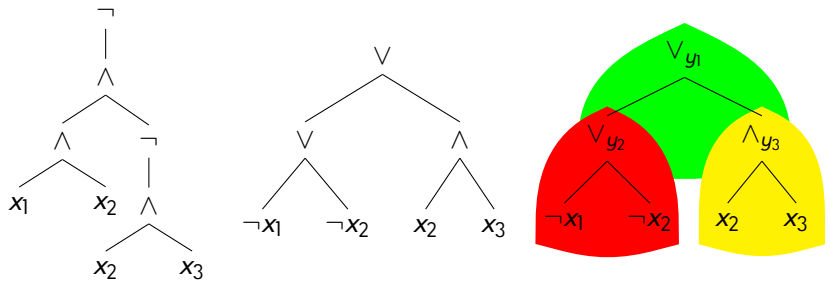
F erfüllbar gdw. $f(F)$ erfüllbar

Damit SAT $\preceq_{\mathsf{P}}$ 3-SAT, womit 3-SAT **NP**-vollständig. $\square$

NP-vollständige Probleme

Beispiel $F = \neg((x_1 \wedge x_2) \wedge \neg(x_2 \wedge x_3))$

Syntaxbaum von F | Syntaxbaum NNF F' | Zuweisung



Konstruierte Formel $f(F)$

$$y_1 \wedge (y_1 \leftrightarrow (y_2 \vee y_3)) \wedge (y_2 \leftrightarrow (\neg x_1 \vee \neg x_2)) \wedge (y_3 \leftrightarrow (x_2 \wedge x_3))$$

NP-vollständige Probleme

Konjunktive Normalform mit 2 Literalen

- Geg. aussagenlogische Formel F in 2KNF (max. 2 Literale)
- Ist F erfüllbar? (Existiert Modell?)
- Problem 2-SAT $= \{F \mid F$ erfüllbare Formel in 2KNF$\}$

- Entscheidbarkeit 2-SAT entscheidbar
- Polynomielle Entscheidbarkeit 2-SAT ja, in **P**
- Nichtdet. polynomielle Entscheidbarkeit 2-SAT ja, in **NP**

NP-vollständige Probleme

Algorithmus für polynomielle Entscheidbarkeit

- Resolution für Unerfüllbarkeit (Resolution korrekt & vollständig)
- Resolventen haben höchstens 2 Literale
- Höchstens $(2|F|)^2$ Resolventen bildbar