Parallel Access to **NP**

Frank Heitmann
heitmann@informatik.uni-hamburg.de

Gastvortrag im Rahmen der Vorlesung
Komplexitätstheorie
von
Prof. Dr. Matthias Jantzen
16.06.2008

Eine einführende Frage

Beispiel

Was ist mit

$$\mathbf{P}^{\mathtt{SAT}}$$

gemeint? Was kann damit erreicht werden?

Eine einführende Frage

Beispiel

Was ist mit

$$\mathbf{P}^{\mathtt{SAT}}$$

gemeint? Was kann damit erreicht werden?

- SAT
- **NP**
- ... mehr als **NP** ?

Die polynomielle Hierarchie (Wdh.)

Was passiert, wenn man immer mächtigere (zumindest theoretisch) Orakel zulässt?

Die polynomielle Hierarchie (Wdh.)

Was passiert, wenn man immer mächtigere (zumindest theoretisch) Orakel zulässt?

- führt zur polynomiellen Hierarchie
- vermutete Struktur zwischen **NP** und **PSPACE**
- kann zur Klassifizierung von Problemen genutzt werden
- Ansatz zur Lösung der **P**-**NP**-Frage

Die polynomielle Hierarchie (Wdh.)

Definition (Polynomielle Hierarchie)

Die *polynomielle Hierarchie* wird induktiv definiert:

- $\Delta_0 = \Sigma_0 = \Pi_0 = \mathbf{P}$
- Für $i \geq 0$ sei

$$\Delta_{i+1} = \mathbf{P}^{\Sigma_i}, \Sigma_{i+1} = \mathbf{NP}^{\Sigma_i} \text{ und } \Pi_{i+1} = \mathbf{co}\Sigma_{i+1}$$

- $\mathbf{PH} = \bigcup_{k \geq 0} \Sigma_k$

Die polynomielle Hierarchie (Wdh.)

Definition (Polynomielle Hierarchie)

Die *polynomielle Hierarchie* wird induktiv definiert:

- $\Delta_0 = \Sigma_0 = \Pi_0 = \mathbf{P}$
- Für $i \geq 0$ sei

$$\Delta_{i+1} = \mathbf{P}^{\Sigma_i}, \Sigma_{i+1} = \mathbf{NP}^{\Sigma_i} \text{ und } \Pi_{i+1} = \mathbf{co}\Sigma_{i+1}$$

- $\mathbf{PH} = \bigcup_{k \geq 0} \Sigma_k$

Anmerkung

- $\Delta_1 = \mathbf{P}^{\Sigma_0} = \mathbf{P}^{\mathbf{P}} = \mathbf{P}$,
- $\Sigma_1 = \mathbf{NP}^{\Sigma_0} = \mathbf{NP}^{\mathbf{P}} = \mathbf{NP}$ und
- $\Pi_1 = \mathbf{co}\Sigma_1 = \mathbf{coNP}$.

Teilmengenbeziehungen (Wdh.)

Satz (Teilmengenbeziehungen)

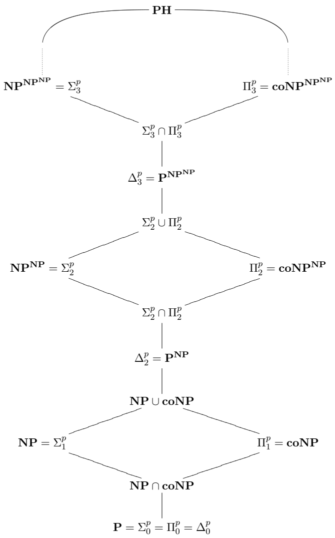
1. *Für jedes $i \geq 0$ gilt:*

$$\Sigma_i \cup \Pi_i \subseteq \Delta_{i+1} \subseteq \Sigma_{i+1} \cap \Pi_{i+1}$$

2. *Für jedes $i \geq 0$ gilt:*

$$\Sigma_i \subseteq \Pi_{i+1} \textit{ und } \Pi_i \subseteq \Sigma_{i+1}$$

3. **PH** $\subseteq$ **PSPACE**


$\mathbf{PH}$
$\mathbf{NP}^{\mathbf{NP}^{\mathbf{NP}}} = \Sigma_3^p$
$\Pi_3^p = \mathbf{coNP}^{\mathbf{NP}^{\mathbf{NP}}}$
$\Sigma_3^p \cap \Pi_3^p$
$\Delta_3^p = \mathbf{P}^{\mathbf{NP}^{\mathbf{NP}}}$
$\Sigma_2^p \cup \Pi_2^p$
$\mathbf{NP}^{\mathbf{NP}} = \Sigma_2^p$
$\Pi_2^p = \mathbf{coNP}^{\mathbf{NP}}$
$\Sigma_2^p \cap \Pi_2^p$
$\Delta_2^p = \mathbf{P}^{\mathbf{NP}}$
$\mathbf{NP} \cup \mathbf{coNP}$
$\mathbf{NP} = \Sigma_1^p$
$\Pi_1^p = \mathbf{coNP}$
$\mathbf{NP} \cap \mathbf{coNP}$
$\mathbf{P} = \Sigma_0^p = \Pi_0^p = \Delta_0^p$

Reduktionen

Definition (Reduktionen)

- Die *Many-One-Reduktion* $\leq_m^p$ wird definiert durch $A \leq_m^p B$ genau dann, wenn $\exists f \in \mathbf{FP} : x \in A \Leftrightarrow f(x) \in B$.

Reduktionen

Definition (Reduktionen)

- Die *Many-One-Reduktion* $\leq_m^p$ wird definiert durch $A \leq_m^p B$ genau dann, wenn $\exists f \in \mathbf{FP} : x \in A \Leftrightarrow f(x) \in B$.
- Die *Polynomialzeit-Turing-Reduktion* $\leq_T^p$ wird definiert durch $A \leq_T^p B$ genau dann, wenn eine DPOTM M existiert mit $A = L(M^B)$.

Reduktionen

Definition (Reduktionen)

- Die *Many-One-Reduktion* $\leq_m^p$ wird definiert durch $A \leq_m^p B$ genau dann, wenn $\exists f \in \mathbf{FP} : x \in A \Leftrightarrow f(x) \in B$.
- Die *Polynomialzeit-Turing-Reduktion* $\leq_T^p$ wird definiert durch $A \leq_T^p B$ genau dann, wenn eine DPOTM M existiert mit $A = L(M^B)$.
- $\mathcal{C}$ ist $\leq_m^p$*-abgeschlossen* genau dann, wenn aus $A \leq_m^p B$ und $B \in \mathcal{C}$ stets $A \in \mathcal{C}$ folgt.

Reduktionen

Definition (Reduktionen)

- Die *Many-One-Reduktion* $\leq_m^p$ wird definiert durch $A \leq_m^p B$ genau dann, wenn $\exists f \in \mathbf{FP} : x \in A \Leftrightarrow f(x) \in B$.
- Die *Polynomialzeit-Turing-Reduktion* $\leq_T^p$ wird definiert durch $A \leq_T^p B$ genau dann, wenn eine DPOTM M existiert mit $A = L(M^B)$.
- $\mathcal{C}$ ist $\leq_m^p$*-abgeschlossen* genau dann, wenn aus $A \leq_m^p B$ und $B \in \mathcal{C}$ stets $A \in \mathcal{C}$ folgt.
- Entsprechend für $\leq_T^p$.

Einige Ergebnisse

Es folgen einige Ergebnisse...

Abschlusseigenschaften

Satz

Für $i \geq 0$ *sind*

- Δ_i, Σ_i *und* Π_i $\leq_m^p$*-abgeschlossen;*
- Δ_i *ist sogar* $\leq_T^p$*-abgeschlossen;*
- **PH** *ist* $\leq_m^p$*-abgeschlossen.*

Alternative Darstellung (1/3)

Satz

Für eine Sprache $L \subseteq \Sigma^*$ gilt $L \in \mathbf{NP}$ genau dann, wenn ein $L' \in \mathbf{P}$ und ein Polynom p existiert derart, dass für alle $x \in \Sigma^*$ gilt:

$$x \in L \Leftrightarrow \textit{es gibt ein } w \in \Sigma^* \textit{ mit } |w| \leq p(|x|) \textit{ und } \langle x, w \rangle \in L'$$

Alternative Darstellung (1/3)

Satz

Für eine Sprache $L \subseteq \Sigma^*$ gilt $L \in \mathbf{NP}$ genau dann, wenn ein $L' \in \mathbf{P}$ und ein Polynom p existiert derart, dass für alle $x \in \Sigma^*$ gilt:

$$x \in L \Leftrightarrow \textit{es gibt ein } w \in \Sigma^* \textit{ mit } |w| \leq p(|x|) \textit{ und } \langle x, w\rangle \in L'$$

Definition (Längenbeschränkte Quantoren)

Für jedes Prädikat B, jedes Polynom p und jede Zeichenkette x sei

$$\begin{aligned} \exists^p y B(x,y) &\quad :\Longleftrightarrow \quad \exists y[|y| \leq p(|x|) \wedge B(x,y)] \\ \forall^p y B(x,y) &\quad :\Longleftrightarrow \quad \forall y[|y| \leq p(|x|) \Rightarrow B(x,y)] \end{aligned}$$

Alternative Darstellung (2/3)

Satz

Sei $i \geq 0$. Es gilt

- *$A \in \Sigma_i$ genau dann, wenn ein $B \in \mathbf{P}$ und ein Polynom p existiert derart, dass für alle $x \in \Sigma^*$ gilt*

  $$x \in A \Leftrightarrow \exists^p w_1 \forall^p w_2 \dots \mathcal{Q}^p w_i [\langle x, w_1, w_2, \dots, w_i \rangle \in B]$$

  wobei $\mathcal{Q}^p = \exists^p$, wenn i ungerade ist und $\mathcal{Q}^p = \forall^p$, wenn i gerade ist.

Alternative Darstellung (3/3)

Satz

Sei $i \geq 0$. Es gilt

- *$A \in \Pi_i$ genau dann, wenn ein $B \in \mathbf{P}$ und ein Polynom p existiert derart, dass für alle $x \in \Sigma^*$ gilt*

$$x \in A \Leftrightarrow \forall^p w_1 \exists^p w_2 \dots \mathcal{Q}^p w_i [\langle x, w_1, w_2, \dots, w_i \rangle \in B]$$

wobei $\mathcal{Q}^p = \forall^p$, wenn i ungerade ist und $\mathcal{Q}^p = \exists^p$, wenn i gerade ist.

Zusammenbruch

Satz (Zusammenbruch der polynomiellen Hierarchie)

1. *Gilt* $\Sigma_i = \Sigma_{i+1}$ *für ein* $i \geq 0$*, so folgt* $\Sigma_i = \Pi_i = \Delta_{i+1} = \Sigma_{i+1} = \Pi_{i+1} = \ldots = \mathbf{PH}$.
2. *Gilt* $\Sigma_i = \Pi_i$ *für ein* $i \geq 1$*, so folgt* $\Sigma_i = \Pi_i = \Delta_{i+1} = \Sigma_{i+1} = \Pi_{i+1} = \ldots = \mathbf{PH}$.

Eine neue Klasse...

Wir haben mit $\mathbf{P}^{\mathtt{SAT}}$ begonnen...

- Wieviele Fragen an das Orakel kann man dabei stellen?

Eine neue Klasse...

Wir haben mit $\mathbf{P}^{\mathtt{SAT}}$ begonnen...

- Wieviele Fragen an das Orakel kann man dabei stellen?
- Was passiert wenn man dies einschränkt?

Eine neue Klasse...

Wir haben mit $\mathbf{P}^{\mathtt{SAT}}$ begonnen...

- Wieviele Fragen an das Orakel kann man dabei stellen?
- Was passiert wenn man dies einschränkt?
- Dies führt zu Klassen der Art $\mathbf{P}^{\mathtt{SAT}[\mathcal{O}(\log)]}$ ...
- ... und um die soll es jetzt gehen!

Probleme aus der Graphentheorie I

Definition (Independent Set (IS) und Vertex Cover (VC))

Sei G ein ungerichteter Graph.

- Ein *independent set* von G ist eine Teilmenge $I \subseteq V(G)$ derart, dass für $x, y \in I$ stets $\{x, y\} \notin E(G)$ gilt. $\alpha(G)$ bezeichne die Grösse eines maximalen independent sets.
- Eine *vertex cover* von G ist eine Teilmenge $C \subseteq V(G)$ derart, dass $\{x, y\} \cap C \neq \emptyset$ für jede Kante $\{x, y\} \in E(G)$ gilt. $\iota(G)$ bezeichne die Grösse einer minimalen vertex cover.

Probleme aus der Graphentheorie I

Definition (Independent Set (IS) und Vertex Cover (VC))

Sei G ein ungerichteter Graph.

- Ein *independent set* von G ist eine Teilmenge $I \subseteq V(G)$ derart, dass für $x, y \in I$ stets $\{x, y\} \notin E(G)$ gilt. $\alpha(G)$ bezeichne die Grösse eines maximalen independent sets.
- Eine *vertex cover* von G ist eine Teilmenge $C \subseteq V(G)$ derart, dass $\{x, y\} \cap C \neq \emptyset$ für jede Kante $\{x, y\} \in E(G)$ gilt. $\iota(G)$ bezeichne die Grösse einer minimalen vertex cover.

Damit werden nun das *independent set problem* und das *vertex cover problem* definiert durch:

- $\texttt{IS} = \{(G, k) \mid G \text{ ist ein Graph mit } \alpha(G) \geq k\}$
- $\texttt{VC} = \{(G, k) \mid G \text{ ist ein Graph mit } \iota(G) \leq k\}$

Probleme aus der Graphentheorie II

Die Probleme `IS` und `VC` sind bekanntlich (?) **NP**-vollständig.
Wir benötigen nachher aber sogar eine spezielle Reduktion:

Probleme aus der Graphentheorie II

Die Probleme IS und VC sind bekanntlich (?) **NP**-vollständig.
Wir benötigen nachher aber sogar eine spezielle Reduktion:

Satz (3SAT $\leq_m^p$ IS)

Es existiert eine Reduktion g, die 3SAT in Polynomialzeit auf IS reduziert und folgende Eigenschaft besitzt: Für jede Boolesche Formel ϕ ist $g(\phi) = (G, m)$, wobei G ein Graph ist und m eine natürliche Zahl (genauer: die Anzahl der Klauseln von ϕ), und es gilt:

$$\phi \in \mathit{3SAT} \implies \alpha(G) = m \quad (1)$$
$$\phi \notin \mathit{3SAT} \implies \alpha(G) = m - 1 \quad (2)$$

IN-Odd, IN-Equ und IN-Geq

Definition (IN-Odd, IN-Equ und IN-Geq)

Sei G ein ungerichteter Graph und $\alpha(G)$ die Grösse eines maximalen independent sets. Wir definieren:

$$\begin{aligned}
\texttt{IN-Odd} &= \{G \mid \alpha(G) \text{ ist ungerade}\} \\
\texttt{IN-Equ} &= \{(G, H) \mid \alpha(G) = \alpha(H)\} \\
\texttt{IN-Geq} &= \{(G, H) \mid \alpha(G) \geq \alpha(H)\}
\end{aligned}$$

$\texttt{IN-Odd} \in \mathbf{\Theta}_2$

Definition

1. Es sei $\mathbf{P}^{\mathbf{NP}[\mathcal{O}(\log)]}$ die Klasse jener Probleme A, die von einer DPOTM M mit Orakel $B \in \mathbf{NP}$ gelöst werden können, d.h. $L(M^B) = A$, derart, dass M bei einer Eingabe der Länge n nicht mehr als $\mathcal{O}(\log n)$ (sequentielle) Fragen an das Orakel B stellt.
2. Es sei $\mathbf{\Theta}_2 = \mathbf{P}^{\mathbf{NP}[\mathcal{O}(\log)]}$. (Verallgemeinerbar!)

$\texttt{IN-Odd} \in \mathbf{\Theta}_2$

Definition

1. Es sei $\mathbf{P}^{\mathbf{NP}[\mathcal{O}(\log)]}$ die Klasse jener Probleme A, die von einer DPOTM M mit Orakel $B \in \mathbf{NP}$ gelöst werden können, d.h. $L(M^B) = A$, derart, dass M bei einer Eingabe der Länge n nicht mehr als $\mathcal{O}(\log n)$ (sequentielle) Fragen an das Orakel B stellt.
2. Es sei $\mathbf{\Theta}_2 = \mathbf{P}^{\mathbf{NP}[\mathcal{O}(\log)]}$. (Verallgemeinerbar!)

Satz

Es gilt $\texttt{IN-Odd}, \texttt{IN-Equ}, \texttt{IN-Geq} \in \mathbf{\Theta}_2$

$\texttt{IN-Odd} \in \mathbf{\Theta}_2$

Definition

1. Es sei $\mathbf{P}^{\mathbf{NP}[\mathcal{O}(\log)]}$ die Klasse jener Probleme A, die von einer DPOTM M mit Orakel $B \in \mathbf{NP}$ gelöst werden können, d.h. $L(M^B) = A$, derart, dass M bei einer Eingabe der Länge n nicht mehr als $\mathcal{O}(\log n)$ (sequentielle) Fragen an das Orakel B stellt.
2. Es sei $\mathbf{\Theta}_2 = \mathbf{P}^{\mathbf{NP}[\mathcal{O}(\log)]}$. (Verallgemeinerbar!)

Satz

Es gilt $\texttt{IN-Odd}, \texttt{IN-Equ}, \texttt{IN-Geq} \in \mathbf{\Theta}_2$

Beweis.

... hat jemand eine Idee? □

Ein wichtiges Lemma

Satz (Wagner)

Sei A eine **NP***-vollständige Menge und B eine beliebige Menge. Existiert eine in Polynomialzeit berechenbare Funktion f derart, dass für alle $k \geq 1$ und alle $x_1, x_2, \ldots, x_{2k} \in \Sigma^*$ mit $\chi_A(x_1) \geq \chi_A(x_2) \geq \ldots \geq \chi_A(x_{2k})$*

$$||\{i \mid x_i \in A\}|| \text{ ist ungerade} \Leftrightarrow f((x_1, \ldots, x_{2k})) \in B$$

erfüllt ist, so ist B $\mathbf{\Theta}_2$-schwierig.

Ein wichtiges Lemma

Satz (Wagner)

Sei A eine **NP***-vollständige Menge und B eine beliebige Menge. Existiert eine in Polynomialzeit berechenbare Funktion f derart, dass für alle $k \geq 1$ und alle $x_1, x_2, \ldots, x_{2k} \in \Sigma^*$ mit $\chi_A(x_1) \geq \chi_A(x_2) \geq \ldots \geq \chi_A(x_{2k})$*

$$||\{i \mid x_i \in A\}|| \text{ ist ungerade} \Leftrightarrow f((x_1, \ldots, x_{2k})) \in B$$

erfüllt ist, so ist B $\mathbf{\Theta}_2$-schwierig.

Beweis.

Entfällt hier... bei Interesse gibt es einen ähnlichen im Zuge der Booleschen Hierarchie... □

Der Satz

Satz

`IN-Odd`, `IN-Equ` *und* `IN-Geq` *sind* $\mathbf{\Theta}_2$*-vollständig.*

Der Beweis: Vorarbeiten

Anmerkung

- $\mathtt{IN\text{-}Odd}, \mathtt{IN\text{-}Equ}, \mathtt{IN\text{-}Geq} \in \mathbf{\Theta}_2$ hatten wir schon.

Der Beweis: Vorarbeiten

Anmerkung

- IN-Odd, IN-Equ, IN-Geq $\in \mathbf{\Theta}_2$ hatten wir schon.
- Wir betrachten nur den Fall IN-Equ.

Der Beweis: Vorarbeiten

Anmerkung

- `IN-Odd`, `IN-Equ`, `IN-Geq` $\in \mathbf{\Theta}_2$ hatten wir schon.
- Wir betrachten nur den Fall `IN-Equ`.
- Wir werden Wagners Lemma benutzen.

Der Beweis: Vorarbeiten

Anmerkung

- `IN-Odd`, `IN-Equ`, `IN-Geq` $\in \mathbf{\Theta}_2$ hatten wir schon.
- Wir betrachten nur den Fall `IN-Equ`.
- Wir werden Wagners Lemma benutzen.
- Als **NP**-vollständige Menge A wählen wir `3SAT`.

Der Beweis: Vorarbeiten

Anmerkung

- $\texttt{IN-Odd}, \texttt{IN-Equ}, \texttt{IN-Geq} \in \mathbf{\Theta}_2$ hatten wir schon.
- Wir betrachten nur den Fall $\texttt{IN-Equ}$.
- Wir werden Wagners Lemma benutzen.
- Als **NP**-vollständige Menge A wählen wir $\texttt{3SAT}$.
- Wir benutzen die oben angesprochene Reduktion $g(\phi) = (G, m)$ mit:

$$\begin{aligned}
\phi \in \texttt{3SAT} &\implies \alpha(G) = m \\
\phi \notin \texttt{3SAT} &\implies \alpha(G) = m - 1
\end{aligned}$$

Der Beweis: Das Ziel

Das Ziel

Mit obigen geben wir eine in Polynomialzeit berechenbare Funktion f an mit

$$||\{i \mid \phi_i \in \mathtt{3SAT}\}|| \text{ ist gerade} \Leftrightarrow f((\phi_1, \dots, \phi_{2k})) \in \mathtt{IN\text{-}Equ}$$

für alle $k \geq 1$ und Formeln $\phi_1, \dots, \phi_{2k}$ mit

$$\phi_{i+1} \in \mathtt{3SAT} \Rightarrow \phi_i \in \mathtt{3SAT}$$

für alle i mit $1 \leq i \leq 2k$.

Der Beweis

Sei nachfolgend $k \geq 1$ und seien $\phi_1, \ldots, \phi_{2k}$ Boolesche Formeln mit

$$\phi_{i+1} \in \mathtt{3SAT} \Rightarrow \phi_i \in \mathtt{3SAT}$$

für alle $i < 2k$. Sei ferner für jedes i mit $1 \leq i \leq 2k$

$$g(\phi_i) = (G_i, m_i)$$

Der Beweis

Sei nachfolgend $k \geq 1$ und seien $\phi_1, \ldots, \phi_{2k}$ Boolesche Formeln mit

$$\phi_{i+1} \in \mathtt{3SAT} \Rightarrow \phi_i \in \mathtt{3SAT}$$

für alle $i < 2k$. Sei ferner für jedes i mit $1 \leq i \leq 2k$

$$g(\phi_i) = (G_i, m_i)$$

Anmerkung

Man beachte:

$$\begin{aligned} ||\{i \mid \phi_i \in \mathtt{3SAT}\}|| = n \\ \Leftrightarrow \quad \phi_1, \ldots, \phi_n \in \mathtt{3SAT} \wedge \\ \phi_{n+1}, \ldots, \phi_{2k} \notin \mathtt{3SAT} \end{aligned}$$

Der Beweis

Zwei Fälle: Ist $||\{i \mid \phi_i \in \mathtt{3SAT}\}||$ *gerade*, so gilt für jedes $i \in \{1, \ldots, k\}$:

$$\phi_{2i-1} \in \mathtt{3SAT} \Leftrightarrow \phi_{2i} \in \mathtt{3SAT}$$

Der Beweis

Zwei Fälle: Ist $||\{i \mid \phi_i \in \texttt{3SAT}\}||$ *gerade*, so gilt für jedes $i \in \{1, \ldots, k\}$:

$$\phi_{2i-1} \in \texttt{3SAT} \Leftrightarrow \phi_{2i} \in \texttt{3SAT}$$

Daraus folgt für jedes $i \in \{1, \ldots, k\}$:

$$\alpha(G_{2i-1}) + m_{2i} = \alpha(G_{2i}) + m_{2i-1}$$

Der Beweis

Ist $||\{i \mid \phi_i \in \mathtt{3SAT}\}||$ *ungerade*, so *gibt es ein* $i \in \{1, \ldots, k\}$ mit:

$$\begin{array}{ccc} \phi_{2i-1} \in \mathtt{3SAT} & \text{und} & \phi_{2i} \notin \mathtt{3SAT} \text{ und} \\ \phi_{2j-1} \in \mathtt{3SAT} & \Leftrightarrow & \phi_{2j} \in \mathtt{3SAT} \end{array}$$

für alle $j \in \{1, \ldots, k\}$ mit $j \neq i$.

Der Beweis

Ist $||\{i \mid \phi_i \in \mathtt{3SAT}\}||$ *ungerade*, so *gibt es ein* $i \in \{1, \ldots, k\}$ mit:

$$\begin{array}{ccc} \phi_{2i-1} \in \mathtt{3SAT} & \text{und} & \phi_{2i} \notin \mathtt{3SAT} \text{ und} \\ \phi_{2j-1} \in \mathtt{3SAT} & \Leftrightarrow & \phi_{2j} \in \mathtt{3SAT} \end{array}$$

für alle $j \in \{1, \ldots, k\}$ mit $j \neq i$.
Damit gilt für dieses i und diese j:

$$\begin{array}{rcl} \alpha(G_{2i-1}) + m_{2i} - 1 & = & \alpha(G_{2i}) + m_{2i-1} \\ \alpha(G_{2j-1}) + m_{2j} & = & \alpha(G_{2j}) + m_{2j-1} \end{array}$$

Der Beweis

Sei nun:

$$
\begin{aligned}
m_{odd} &= \sum_{1 \le i \le k} m_{2i-1} \\
m_{even} &= \sum_{1 \le i \le k} m_{2i} \\
G_{odd} &= \cup_{1 \le i \le k} G_{2i-1} \\
G_{even} &= \cup_{1 \le i \le k} G_{2i}
\end{aligned}
$$

H_n sei der Graph, der aus n isolierten Knoten besteht.

Anmerkung

$G \cup H$ ist die disjunkte Vereinigung zweier Graphen. Man beachte, dass $\alpha(G \cup H) = \alpha(G) + \alpha(H)$ gilt. $G_1, \ldots, G_{2k}$ sind als disjunkt angenommen. Man beachte ferner, dass $\alpha(H_n) = n$ gilt.

Der Beweis

Die Reduktion f wird nun definiert durch:

Der Beweis

Die Reduktion f wird nun definiert durch:

$$f((\phi_1, \dots, \phi_{2k})) = (G_{odd} \cup H_{m_{even}}, G_{even} \cup H_{m_{odd}})$$

f ist in Polynomialzeit berechenbar und es bleibt zu zeigen:

$$||\{i \mid \phi_i \in \texttt{3SAT}\}|| \text{ ist gerade} \Leftrightarrow \alpha(G_{odd} \cup H_{m_{even}}) = \alpha(G_{even} \cup H_{m_{odd}})$$

Der Beweis

$$
\begin{aligned}
&||\{i \mid \phi_i \in \mathtt{3SAT}\}|| \text{ ist gerade}\\
&\quad \Rightarrow \forall i \in [k]\ \alpha(G_{2i-1}) + m_{2i} = \alpha(G_{2i}) + m_{2i-1}\\
&\quad \Rightarrow \sum_{1 \leq i \leq k} (\alpha(G_{2i-1}) + m_{2i}) = \sum_{1 \leq i \leq k} (\alpha(G_{2i}) + m_{2i-1})\\
&\quad \Rightarrow \alpha(G_{odd}) + m_{even} = \alpha(G_{even}) + m_{odd}\\
&\quad \Rightarrow \alpha(G_{odd} \cup H_{m_{even}}) = \alpha(G_{even} \cup H_{m_{odd}})
\end{aligned}
$$

Der Beweis

$$
\begin{aligned}
&||\{i \mid \phi_i \in \mathtt{3SAT}\}|| \text{ ist ungerade} \\
&\qquad \Rightarrow \ldots \\
&\qquad \Rightarrow \alpha(G_{odd} \cup H_{m_{even}}) \neq \alpha(G_{even} \cup H_{m_{odd}})
\end{aligned}
$$

Der Beweis

Mit dem Lemma von Wagner folgt damit der zu zeigende Satz!

Fazit

- Damit haben wir für $\mathbf{\Theta}_2$ vollständige Probleme gefunden...

Fazit

- Damit haben wir für $\mathbf{\Theta}_2$ vollständige Probleme gefunden...
- ... die allerdings etwas künstlich wirken...

Es gibt aber sehr natürliche Probleme, die vollsändig für $\mathbf{\Theta}_2$ sind.

$\Rightarrow$ computational politics

$\Rightarrow$ social choice theory

Ausblick: Warum eigentlich *parallel access* ??

Warum eigentlich *parallel access* ??

Ausblick: Warum eigentlich *parallel access* ??

Warum eigentlich *parallel access* ??

- Man kann Orakelmaschinen definieren, die nicht wie bisher in sequentieller Weise Fragen beantworten.
- Stattdessen sammelt man alle Fragen und stellt diese auf einmal.
- Man kann zeigen, dass polynomiell viele Fragen dieser Art gerade logarithmisch viel sequentiellen entsprechen!

Ausblick: Warum eigentlich *parallel access* ??

Warum eigentlich *parallel access* ??

- Man kann Orakelmaschinen definieren, die nicht wie bisher in sequentieller Weise Fragen beantworten.
- Stattdessen sammelt man alle Fragen und stellt diese auf einmal.
- Man kann zeigen, dass polynomiell viele Fragen dieser Art gerade logarithmisch viel sequentiellen entsprechen!
- Darauf kommen wir (über-)nächstes Mal zu sprechen...

Ausblick I

Nächstes Mal (23.6):

- Wir werden die Boolesche Hierarchie definieren...
- ... und vollständige Probleme in ihr betrachten (Wagners Lemma II).
- Wir werden noch ein wenig mehr über die polynomielle Hierarchie reden...
- ... und Zusammenhänge zur Booleschen Hierarchie betrachten.

Ausblick II

Übernächstes Mal (30.6):

- Wir werden die Query Hierarchie und die parallele Query Hierarchie definieren...
- ... und Zusammenhänge zwischen allen bisher betrachteten Hierarchien herstellen!

Ausblick II

Übernächstes Mal (30.6):

- Wir werden die Query Hierarchie und die parallele Query Hierarchie definieren...
- ... und Zusammenhänge zwischen allen bisher betrachteten Hierarchien herstellen!

Überübernächstes Mal (7.7):

- Wir werden die polynomielle Hierarchie nutzen, um mehr über die Struktur *in* **NP** zu erfahren!

Ausblick III

Überüberübernächstes Mal (14.7): Wenn da noch jemand kommt...

- ... gibt's einen bunten Mix aus dem, was war, und dem, was es noch so gibt...

Hausaufgaben

- Findet eine Reduktion g, die 3SAT auf IS in Polynomialzeit reduziert, wobei $g(\phi) = (G, m)$ ist, und

$$\phi \in \mathtt{3SAT} \implies \alpha(G) = m \quad (3)$$
$$\phi \notin \mathtt{3SAT} \implies \alpha(G) = m - 1 \quad (4)$$

  erfüllt.
- Zeigt, dass IN-Odd und IN-Geq $\mathbf{\Theta}_2$-vollständig sind.

Kurz vor Schluss...

Wenn Frank jetzt noch Zeit hat, erzählt er noch was zu Steinerbäumen...

Kurz vor Schluss...

Wenn Frank jetzt noch Zeit hat, erzählt er noch was zu Steinerbäumen... ... sonst klickt er sich zur nächsten Folie und sagt...

Ende...

Danke für die Aufmerksamkeit
!