Theoretische Informatik 2
Zusammenfassung

Jan Pöschko
auf Grundlage der Vorlesung von
Bettina Klinz

1. Dezember 2011

1 Probleme

Existenz eines perfekten Matchings $\in \mathbf{RP}$

2-SAT $\in \mathbf{RP}$

Primzahltest $\in \mathbf{RP} \cap \mathbf{co\text{-}RP}$

FSAT **FNP**-vollständig

SAT-UNSAT **DP**-vollständig

Entscheidungsproblem zu TSP **NP**-vollständig

EXACT-TSP **DP**-vollständig

TSP-COST bestimme Länge einer optimalen Tour
$\mathbf{FP}^{\mathbf{NP}}$-vollständig

TSP finde Tour
$\mathbf{FP}^{\mathbf{NP}}$-vollständig

UNIQUE-SAT Gibt es eine einzige erfüllende Wahrheitsbelegung?

CRITICAL-SAT Φ nicht erfüllbar, aber durch Streichen einer Klausel erfüllbar?
DP-vollständig (so wie alle *CRITICAL*-Probleme hier)

CRITICAL-HAMPATH G enthält keinen Hamiltonweg, aber nach Hinzufügen einer beliebigen Kante schon

CRITICAL-3-COLORABILITY

MAX-OUTPUT $\mathbf{FP}^{\mathbf{NP}}$-vollständig

MAX-WEIGHT-SAT (Klauseln) $\mathbf{FP}^{\mathbf{NP}}$-vollständig

MAX-W-SAT (Variablen) **MAX-NPO**-vollständig

CLIQUE-SIZE $\mathbf{FP}^{\mathbf{NP[log]}}$-vollständig

$QSAT_i$ $\exists X_1\ \forall X_2\ \exists X_3 \cdots QX_i : \Phi$
$\Sigma_i\mathbf{P}$-vollständig

#SAT Anzahl der erfüllenden Wahrheitsbelegungen
$\#\mathbf{P}$-vollständig

#HAMPATH $\#\mathbf{P}$-vollständig

#HAMCYCLE

#CLIQUE Anzahl der Cliquen mit $\geq k$ Knoten

#MATCHING, PERMANENT $\#\mathbf{P}$-vollständig

$\oplus$*SAT* $\oplus\mathbf{P}$-vollständig

$\oplus$*HAMPATH* $\oplus\mathbf{P}$-vollständig

$\oplus$*PERMANENT* $\in \mathbf{P}$ (berechne Determinante von A^G mod 2)

GI $GI \in \mathbf{IP}(1)$, da $GI \in \mathbf{NP}$
$\overline{GI} \in \mathbf{IP}(2)$: V schickt $(G_0, \pi_i(G_{b_i}))$; B sendet $\tilde{b}_i$; V aktzeptiert, wenn $b_i = \tilde{b}_i$
$GI \in \mathbf{IP}(1) \cap \mathbf{co\text{-}IP}(2)$
$GI \in \mathbf{PZK}$: B schickt $H = \pi(G_i)$; V sendet zufälliges j; B schickt Permutation $\tilde{\pi}$; V akzeptiert, wenn $H = \tilde{\pi}(G_j)$

HAMCYCLE $\in$ **CZK** (sofern one-way functions existieren): B schickt Bitfestlegung (versteckend + bindend) für π und $\pi(G)$; V schickt $i \in \{0,1\}$; falls $i = 0$: B deckt π und $\pi(G)$ auf, falls $i = 1$: B deckt n Kanten (Ham. Kreis, falls $\exists$) auf; V akzeptiert, falls konsistent bzw. tatsächlich Ham. Kreis

3-Knotenfärbbarkeit $\in$ **IP**: B schickt Bitfestlegung für $\pi(\Phi(i))$; V schickt zufällige Kante $e \in E$; Bob deckt Werte von Φ für adjazente Knoten auf; V akzeptiert, wenn konsistent und unterschiedliche Farben; wiederhole $t\,|E|$ mal für Fehlerwahrscheinlichkeit $\sim e^{-t}$

CLIQUE besitzt keinen Approximationsalgorithmus mit konstanter Güte ($\frac{n}{k}$ durch Betrachten k-elementiger Teilmengen möglich)

VERTEX COVER gesucht: Knotenmenge V' minimaler Kardinalität, sodass jede Kante überdeckt wird
$\in$ **APX**(2) (bestimmte greedy-artig max. Matching)

MAX-3SAT $\in$ **APX**($\frac{8}{7}$): Derandomisierung durch schrittweise Fixierung der Variablen gemäß Erwartungswert der Anzahl an erfüllter Klauseln
$\notin$ **PTAS**
MAX-3SAT $\leq_{\text{PTAS}}$ *CLIQUE*
APX-vollständig: **MAX-APX**-vollständig; für jedes Minimierungsproblem $A \in$ **APX** gibt es ein Maximierungsproblem $B \in$ **APX** mit $A \leq_{\text{PTAS}} B$

2-Maschinen-Scheduling minimiere $\max\{\sum_{j\in J} p_j, \sum_{j\in\{1,\ldots,n\}\setminus J} p_j\}$
$\in$ **PTAS**: Aufteilung in große ($\geq \varepsilon T$) und kleine Jobs

Rucksackproblem $\in$ **FPTAS**: dynamische Programmierung $M[i{+}1, v] = \min\{M[i,v], M[i, v - v_{i+1}] + g_{i+1}\}$ und Skalieren der Werte

$$\tilde{v}_i = \left\lfloor \frac{v_i}{t} \right\rfloor \quad \text{mit } t = \frac{\varepsilon \max\{v_1, \ldots, v_n\}}{(1+\varepsilon)n}$$

GC gesucht: minimale Anzahl an Farben, mit denen Knoten gefärbt werden können
$\notin$ **APX**(c) mit $c < \frac{4}{3}$: $(3,4)$-Lückenproblem
es gibt keinen Approximationsalgorithmus für *GC* mit asymptotischer Approximationsgüte $< \frac{4}{3}$: „Aufblasargument“, Lücke $(3,4) \to (3k, 4k)$

BINPACKING $\notin$ **APX**(c) mit $c < \frac{3}{2}$
es gibt ein asymptotisches FPTAS für *BP*

MAX-CLIQUE $\notin$ **APX**

MAX-CUT $\in \mathbf{MAX\text{-}SNP}_0$
Formulierung als semidefinites Programm (statt quadratischer Terme) möglich

MAX-2-SAT $\in \mathbf{MAX\text{-}SNP}$

INDEPENDENT-SET mit max. Grad k $\in \mathbf{MAX\text{-}SNP}$

INDEPENDENT-SET $\notin \mathbf{MAX\text{-}SNP}$, falls $\mathbf{P} \neq \mathbf{NP}$

MIN-WEIGHT-VERTEX-COVER $\in \mathbf{APX}(2)$: Relaxation von $\min \sum_{i \in V} w_i x_i$ s.t. $x_i + x_j \geq 1$, $x_i \in \{0, 1\}$ (oder Dualisierung)

TSP mit Dreiecksungleichung $\in \mathbf{APX}(\frac{3}{2})$: Christofides-Heuristik (spannender Baum, perfektes Matching der Knoten mit ungeradem Grad, Eulerscher Weg + Abkürzungen)

2 Komplexitätsklassen

BPP $x \in L \Rightarrow \geq \frac{3}{4}$ Berechnungen enden mit „ja“
$x \notin L \Rightarrow \geq \frac{3}{4}$ Berechnungen enden mit „nein“
abgeschlossen bezüglich Komplementbildung
$= \delta$-**BPP** für $0 < \delta \leq \frac{1}{2}$

RP Monte-Carlo-Algorithmus: keine falsch positiven Antworten
$x \notin L \Rightarrow$ alle Berechnungen enden mit „nein“
$x \in L \Rightarrow$ mindestens die Hälfte der Berechnungen enden mit „ja“
$= \delta$-**RP** für $0 < \delta \leq \frac{1}{2}$
$\mathbf{RP} \subseteq \mathbf{NP}$

ZPP $= \mathbf{RP} \cap \mathbf{co\text{-}RP}$
Las-Vegas-Algorithmus
nach k Wiederholungen: Wahrscheinlichkeit für noch kein definitives Ergebnis $\leq 2^{-k}$

PP $x \in L \Leftrightarrow$ mind. die Hälfte der Berechnungen enden mit „ja“
MAJSAT ist **PP**-vollständig
$\mathbf{NP} \subseteq \mathbf{PP}$
$\mathbf{RP} \subseteq \mathbf{BPP} \subseteq \mathbf{PP}$

FNP Klasse von Funktionsproblemen, die mit Sprachen aus **NP** assoziiert sind (FL zu L mit „Beweisrelation“ R_L: finde String y sodass $R_L(x, y)$
$\mathbf{FNP} = \mathbf{FP} \Leftrightarrow \mathbf{NP} = \mathbf{P}$
bezüglich „**F**-Reduktionen“ abgeschlossen

FP Funktionsprobleme in **FNP**, die in polynomieller Zeit lösbar sind
bezüglich „**F**-Reduktionen“ abgeschlossen

TFNP Funktionsprobleme mit totalen Funktionen (es gibt stets zulässige Lösung)
enthält *Faktorisierung ganzer Zahlen*, *HAPPYNET*, *Bestimmung eines zweiten Hamilton-Kreises* (**TFNP**-vollständig), *Bestimme I, J mit* $\sum_{i\in I} a_i = \sum_{j\in J} a_j$

DP enthält Sprachen der Form $L = L_1 \cap L_2$ mit $L_1 \in \mathbf{NP}$, $L_2 \in \mathbf{co\text{-}NP}$
„natürliche“ Klasse für *EXACT-COST*-Probleme

FP$^{\mathbf{NP}}$ $\mathbf{FP}^{\mathbf{NP}}$-vollständig: *MAX-OUTPUT*, *MAX-WEIGHT-SAT*, *TSP-COST*; Optimierungsvarianten von *RUCKSACK*, gewichtete Version von *MAX-CUT* und *BISECTION-WIDTH*

$\mathbf{P}_{\parallel}^{\mathbf{NP}}$ $=\mathbf{P}^{\mathbf{NP[log]}}$
nicht adaptive bzw. $\mathcal{O}(\log|x|)$ viele Orakelaufrufe

PH

$$\Delta_0\mathbf{P} = \Sigma_0\mathbf{P} = \Pi_0\mathbf{P} = \mathbf{P}$$
$$\Delta_{i+1}\mathbf{P} = \mathbf{P}^{\Sigma_i\mathbf{P}}$$
$$\Sigma_{i+1}\mathbf{P} = \mathbf{NP}^{\Sigma_i\mathbf{P}}$$
$$\Pi_{i+1}\mathbf{P} = \mathbf{co\text{-}NP}^{\Sigma_i\mathbf{P}}$$

$\mathbf{PH} = \bigcup_{i\geq 0} \Sigma_i\mathbf{P}$

$$L \in \Sigma_i\mathbf{P} \Leftrightarrow \exists R : \{x; y : (x,y) \in R\} \in \Pi_{i-1}\mathbf{P}, L = \{x : \exists y : (x,y) \in R\}$$
$$L \in \Pi_i\mathbf{P} \Leftrightarrow \exists R : \{x; y : (x,y) \in R\} \in \Sigma_{i-1}\mathbf{P}, L = \{x : \forall y : (x,y) \in R\}$$

Falls $\Sigma_i\mathbf{P} = \Pi_i\mathbf{P}$, folgt $\Sigma_i\mathbf{P} = \Pi_j\mathbf{P} = \Delta_j\mathbf{P} = \Sigma_j\mathbf{P}$ für alle $j > i$.
Ebenso, wenn ein **PH**-vollständiges Problem existiert.
$\mathbf{PH} \subseteq \mathbf{PSPACE}$
$\mathbf{BPP} \subseteq \Sigma_2\mathbf{P} \cap \Pi_2\mathbf{P}$
$\mathbf{PH} \subseteq \mathbf{P}^{\mathbf{PP}}$

#P Wie viele y gibt es mit $(x,y) \in Q$ bei gegebener polynomiell balancierter in polynomieller Zeit entscheidbarer binärer Relation Q?

$\oplus$P $x \in L \Leftrightarrow$ Anzahl der akzeptierenden Berechnungen ist ungerade
abgeschlossen bezüglich Komplement
$\mathbf{NP} \subseteq \mathbf{RP}^{\oplus\mathbf{P}}$

IP Falls $x \in L$, dann ist die Wahrscheinlichkeit, dass x von (B, V) akzeptiert wird, $\geq \frac{3}{4}$.
Falls $x \notin L$, dann ist die Wahrscheinlichkeit, dass x von (B', V), akzeptiert wird, $\leq \frac{1}{4}$.
$\mathbf{IP}(l)$: l Runden reichen aus
$\mathbf{NP} \subseteq \mathbf{IP}(1)$
$\mathbf{BPP} \subseteq \mathbf{IP}$
$\mathbf{IP} = \mathbf{PSPACE}$

PZK Es gibt einen randomisierten Simulationsalgorithmus für jeden randomisierten Algorithmus V'
$\mathbf{BPP} \subseteq \mathbf{PZK}$
$\mathbf{PZK} \subseteq \mathbf{IP}(2) \cap \mathbf{co\text{-}IP}(2)$
Aus $\mathbf{co\text{-}IP} \subseteq \mathbf{IP}(2)$ würde $\Sigma_2\mathbf{P} = \Pi_2\mathbf{P}$ folgen.

SZK vernachlässigbarer ($< \frac{1}{p(n)}$ für alle Polynome p für n groß genug) Abstand zur Verteilung im realen Protokoll
$\mathbf{SZK} \subseteq \mathbf{IP}(2) \cap \mathbf{co\text{-}IP}(2)$

CZK Verteilung nur mit vernachlässigbarer Wahrscheinlichkeit zu erkennen
$\mathbf{NPC} \subseteq \mathbf{CZK}$

UP höchstens eine akzeptierende Berechnung
$\mathbf{P} \subseteq \mathbf{UP} \subseteq \mathbf{NP}$
$\mathbf{UP} = \mathbf{P} \Leftrightarrow$ es gibt keine one-way functions

PCP(r, q) V hat r Zufallsbits und $\mathcal{O}(q)$ Positionen im Beweis
$\forall x \in L\ \exists B : P_z(V(x, z, B) = 1) = 1$
$\forall x \notin L\ \forall B' : P_z(V(x, z, B') = 1) \leq 1$
$\mathbf{P} = \mathbf{PCP}(0, 0)$
$\mathbf{NP} = \mathbf{PCP}(0, \text{polyn.})$
$\mathbf{co\text{-}RP} = \mathbf{PCP}(\text{polyn.}, 0)$
$\mathbf{NP} = \mathbf{PCP}(\log n, 1)$ (wir haben gezeigt: $3SAT \in \mathbf{PCP}(n^3, 1)$)

APX(r) Approximationsprobleme mit maximaler Approximationsgüte $r_A(n) \leq r(n)$

$$r(x, S) := \frac{v(x, S)}{v_{\text{opt}}(x)} \qquad \text{für Minimierungsprobleme}$$

$$r(x, S) := \frac{v_{\text{opt}}(x)}{v(x, S)} \qquad \text{für Maximierungsprobleme}$$

$$r_A(x) := r(x, S_A(x))$$

$$r_A(n) := \max\{r_A(x) \mid |x| \leq n\}$$

$\mathbf{APX} = \bigcup_{c \geq 1} \mathbf{APX}(c)$
$\mathbf{APX^*} = \bigcap_{c > 1} \mathbf{APX}(c)$

PTAS in polynomieller Zeit in $|x|$ eine $(1+\varepsilon)$-optimale Lösung

FPTAS in polynomieller Zeit in $|x|$ und $\frac{1}{\varepsilon}$ eine $(1+\varepsilon)$-optimale Lösung
$\mathbf{P} \subseteq \mathbf{FPTAS} \subseteq \mathbf{PTAS} \subseteq \mathbf{APX}$

NPO $v(x,S)$ ganzzahlig, Test $s \in S(x)$ in polynomieller Zeit, $v(x,S)$ in polynomieller Zeit berechenbar
NPO-vollständig: $B \leq_{\text{PTAS}} A$ für alle $B \in \mathbf{NPO}$

MAX-SNP Eigenschaften, die als $\exists S\ \forall x_1, x_2, \ldots, x_k : \Phi(S, G, x_1, \ldots, x_k)$ ausdrückbar sind (Einschränkung von **NP** auf Allquantoren)
$\mathbf{MAX\text{-}SNP}_0$: $\max_S \left|\{(x_1, \ldots, x_k) \in V^k \mid \Phi(G_1, \ldots, G_m, S, x_1, \ldots, x_k)\}\right|$
MAX-SNP: Klasse aller Optimierungsprobleme, die **L**-reduzierbar auf ein Problem in $\mathbf{MAX\text{-}SNP}_0$ sind
Abschluss von **MAX-SNP** unter PTAS-Reduktion ist **APX**
Jedes Problem in **MAX-SNP** besitzt Approximationsalgorithmus mit konstanter Güte

3 Nichtapproximierbarkeitsresultate

MAX-SAT	1.2987-approximierbar und **APX**-vollständig
MAX-k-SAT	$\frac{1}{1-2^{-k}}$-approximierbar für $k \geq 3$, aber nicht $\left(\frac{1}{1-2^{-k-\varepsilon}}\right)$-approximierbar
MAX-3-SAT	1.249-approximierbar
MAX-2-SAT	1.0741-approximierbar, aber nicht 1.0746-approximierbar
MIN-VG	$\left(2 - \frac{\log\log n}{2\log n}\right)$-approximierbar, aber nicht $\left(\frac{7}{6} - \varepsilon\right)$
MIN-CG	$\mathcal{O}\left(n\frac{(\log\log n)^2}{\log^3 n}\right)$-approximierbar, aber nicht $n^{\frac{1}{7}} - \varepsilon$, falls $\mathbf{NP} \neq \mathbf{ZPP}$
MAX-CLIQUE	$\mathcal{O}\left(\frac{n}{\log^2 n}\right)$-approximierbar, aber nicht $n^{\frac{1}{2}-\varepsilon}$; sogar nicht $n^{1-\varepsilon}$ falls $\mathbf{NP} \neq \mathbf{ZPP}$
(MIN-) TSP	**NPO**-vollständig; symmetrisch + $\triangle$-Ungleichung: $\frac{3}{2}$-approximierbar, **APX**-vollst.
(MIN-) BP	$\frac{3}{2}$-approximierbar, aber nicht $\left(\frac{3}{2} - \varepsilon\right)$

4 Weiterführende Informationen

`http://qwiki.stanford.edu/index.php/Complexity_Zoo`
`http://www.nada.kth.se/~viggo/problemlist/`