

Testfragen zur Vorlesung

**Effiziente Algorithmen und Komplexitätstheorie
mit dem Schwerpunkt Komplexitätstheorie**

Wintersemester 2005/2006

Martin Sauerhoff

Hinweise:

- Testfragen zur Überprüfung des eigenen Wissens während des Durcharbeitens des Stoffes aus der Vorlesung für die Prüfungsvorbereitung.
- Prüfungsrelevant ist der Stoff der Vorlesung exklusive:
 - Kapitel 12.4 (MAX-3-SAT APX-vollständig);
 - Kapitel 17.
- Einige Tipps zum Gebrauch der Fragen in „Theoretische Informatik“, I. Wegener, Kapitel 9.2.

Einleitung – Wiederholung GTI

- 1.) Definiere die Komplexitätsklassen für deterministische und randomisierte Lösungen algorithmischer Probleme.
- 2.) Wann und wie lässt sich Probability-Amplification anwenden? Welcher Mehraufwand ist für welche Senkung der Versagens- und Fehlerwahrscheinlichkeit ausreichend?
- 3.) Was bedeutet es für die Anwendungen, dass ein Optimierungsproblem NP-äquivalent ist und was bedeutet es nicht?
- 4.) Beschreibe die Beweisidee des Satzes von Cook (auch für diese Vorlesung relevant, da diese Ideen in anderen Zusammenhängen (welchen?) wiederverwendet werden).

Kapitel 7

- 5.) Wann ist ein Problem stark NP-vollständig? Welche bekannten NP-vollständigen Probleme sind auch stark NP-vollständig und welche nicht (falls $P \neq NP$)?
- 6.) Erläutere den Zusammenhang zwischen starker NP-Vollständigkeit und der Existenz pseudopolynomieller Algorithmen.

Kapitel 8

- 7.) Erläutere die Begriffe Optimierungsproblem, Approximationsproblem, Worstcase-Approximationsgüte und asymptotische Approximationsgüte.
- 8.) Bei welchem Problem ist (falls $P \neq NP$) die in polynomieller Zeit erreichbare asymptotische Approximationsgüte echt kleiner als die in polynomieller Zeit erreichbare Worstcase-Approximationsgüte?
- 9.) Beschreibe einen effizienten Approximationsalgorithmus für MAX-3-SAT mit bestmöglicher Worstcase-Approximationsgüte (falls $P \neq NP$).

- 10.) Beschreibe ein PTAS für das Lastverteilungsproblem und ein FPTAS für das Rucksackproblem.
- 11.) Erläutere die Lückentechnik und wende sie auf Beispielprobleme an.
- 12.) Was sind PTAS-Reduktionen und welche Eigenschaften haben sie?
- 13.) Warum lässt sich aus der bekannten polynomiellen Reduktion $3\text{-SAT} \leq_p \text{CLIQUE}$ eine PTAS-Reduktion für die Maximierungsvarianten ableiten, nicht aber für $\text{SAT} \leq_p 3\text{-SAT}$?

- 14.) Definiere die Komplexitätsklassen FPTAS, PTAS, APX und NPO.
- 15.) Welches Problem ist NPO-vollständig und wie führt man den Vollständigkeitsbeweis?

Kapitel 10

- 16.) Was ist NPI? Was folgt aus $\text{NPI} = \emptyset$? Welches „natürliche“ Problem ist Kandidat für eine Mitgliedschaft in NPI?
- 17.) Was folgt, wenn ein NP-vollständiges Problem in co-NP enthalten ist?
- 18.) Definiere die polynomielle Hierarchie. Warum ist ihre Betrachtung interessant, wenn doch schon die NP-vollständigen Probleme schwierig sind?

- 19.) Wo ist das zur Schaltkreisminimierung gehörende Entscheidungsproblem (*Minimum Equivalent Circuit*) in der polynomiellen Hierarchie einzuordnen?
- 20.) Welche Komplexitätsklassen der polynomiellen Hierarchie lassen sich wie logikorientiert beschreiben?
- 21.) Was folgt aus $\Sigma_k = \Sigma_{k+1}$ bzw. aus $\Sigma_k = \Pi_k$?
- 22.) Nenne ein Σ_k -vollständiges Problem.

- 23.) Wie steht BPP zur polynomiellen Hierarchie? Gib die kleinste bekannte Oberklasse und die größte bekannte Unterklasse an.
- 24.) Skizziere den Beweis des Satzes von Lautemann ($BPP \subseteq \Sigma_2$):
- a) Grundidee des Beweises?
 - b) Wie ist der „Rechenwegtest“ definiert?
 - c) Wie verhält sich der Test in den Fällen $x \in L$ und $x \notin L$?
- 25.) Welche formalen Argumente kannst du für die Vermutung anführen, dass NP-vollständige Probleme keine BPP-Algorithmen haben?
- 26.) Was ist universelles Hashing?

Kapitel 11

27.) Definiere und motiviere interaktive Beweissysteme.

28.) Warum ist NP eine Teilmenge von IP(1)?

29.) Zeige $\overline{GI} \in IP(2)$. Warum ist es wert, dies zu beweisen?

30.) Was ist ein Artus-Merlin-Protokoll?

- 31.) Was sind Quantorenklassen und was haben sie mit Artus-Merlin-Protokollen zu tun?
- 32.) Gib das stärkste dir bekannte Argument an, warum GI wohl nicht NP-vollständig ist. Beweisideen?
- 33.) Beschreibe das Simulationsparadigma und die Definition der perfekten Zero-Knowledge-Eigenschaft.
- 34.) Warum vermutet man, dass es für NP-vollständige Probleme keine interaktiven Beweissysteme mit perfekter Zero-Knowledge-Eigenschaft gibt?

35.) Wie ist die allgemeine Zero-Knowledge-Eigenschaft definiert?

36.) Was ist ein Bitfestlegungsverfahren?

37.) Beschreibe interaktive Beweissysteme mit allgemeiner Zero-Knowledge-Eigenschaft für GI und für HC.

Kapitel 12

- 38.) Beschreibe die PCP-Klassen und gib an, welche bekannten Komplexitätsklassen man wie auf einfache Weise wiederfindet.
- 39.) Zeige $NP = PCP(\log n, \text{poly})$.
- 40.) Formuliere das PCP-Theorem.

41.) Gib die Kernideen des Beweises von $NP \subseteq PCP(n^3, 1)$ an.
Insbesondere:

- a) Wie funktioniert die Verifikation von wohlgeformten Beweisen und welche Ressourcen werden benötigt?
- b) Welche weiteren Module werden benutzt, um nicht wohlgeformte Beweise zu entlarven und welche Rolle spielen sie im Einzelnen? Ressourcenverbrauch jeweils?
- c) Wie werden nicht wohlgeformte Beweise behandelt, deren Teile „fast lineare“ Funktionen darstellen? Warum schließt man diese nicht von vornherein aus?

- 42.) Wieso kann die Lückentechnik durch das PCP-Theorem verstärkt werden?
- 43.) Zeige, dass MAX-3-SAT \notin PTAS, falls $P \neq NP$.
- 44.) Zeige, dass MAX-CLIQUE \notin APX, falls $P \neq NP$.

Kapitel 13

- 45.) Wieviel Zeit benötigt eine $s(n)$ -platzbeschränkte, deterministische TM maximal? Was gilt im nichtdeterministischen Fall?
- 46.) Was besagt der Satz von Savitch? Beweisidee?
- 47.) Skizziere eine randomisierte TM, die fast sicher hält, aber nicht absolut.

- 48.) Wie kann man die Rechenzeit von platzbeschränkten randomisierten TMs nach oben abschätzen?
- 49.) Was weißt du über die Beziehungen der Komplexitätsklassen für deterministische, nichtdeterministische und randomisierte TMs mit logarithmischer Platzschranke?
- 50.) Zeige, dass das Problem DSTCON NL-vollständig bezüglich logarithmischer Reduktionen ist.

Kapitel 14

- 51.) Was ist der Unterschied zwischen uniformen und nichtuniformen Berechnungsmodellen?
- 52.) Was ist eine nichtuniforme TM und wie ist der Speicherplatz für nichtuniforme TMs definiert?
- 53.) Wie hängen Schaltkreisgröße und die Rechenzeit für nichtuniforme TMs zusammen? Schaltkreistiefe und Speicherplatz für nichtuniforme TMs?
- 54.) Wie hängen Branchingprogrammgröße und Speicherplatzbedarf von Turingmaschinen zusammen?

Kapitel 15

- 55.) Definiere Kommunikationsprotokolle und die zugehörigen Komplexitätsmaße (deterministisch, nichtdeterministisch, randomisiert).
- 56.) Beschreibe die Anwendungsgebiete der Theorie der Kommunikationskomplexität.
- 57.) Warum sind untere Schranken in dieser Theorie wichtiger als obere Schranken?

- 58.) Beschreibe die allgemeine Variante der Rechteckmaßmethode für den Nachweis von unteren Schranken. Für welche Modelle ist sie anwendbar? Beispiele?
- 59.) Wie funktioniert die Methode der Unterscheidungsmengen? Was hat sie mit der Rechteckmaßmethode zu tun? Für welche Modelle erhält man damit wie untere Schranken? Beispiele?
- 60.) Beschreibe die Rangmethode. Für welche Modelle ist sie wie anwendbar? Beispiele?

- 61.) Beschreibe die Diskrepanzmethode. In welchen Modellen ist sie wie anwendbar? Beispiele?
- 62.) Wie lässt sich die Kommunikationskomplexität des mittleren Bits der Multiplikation abschätzen?
- 63.) Wozu dient die Methode der „Maskenvarianten“ von Funktionen? Nenne Beispiele für Anwendungen der dafür erzielten Ergebnisse später in der Vorlesung.

- 64.) Wie lässt sich die nichtdeterministische Kommunikationskomplexität kombinatorisch charakterisieren?
- 65.) Was ist fehlerfreier Nichtdeterminismus? Welche Beziehung gilt zwischen der Komplexität deterministischer und fehlerfreier nichtdeterministischer Protokolle und wie beweist man diese?
- 66.) Erläutere die Fingerprinting-Methode am Beispiel von \overline{EQ}_n (für privaten und öffentlichen Zufall).
- 67.) Wie lassen sich Protokolle mit öffentlichem Zufall durch solche mit privatem Zufall simulieren (Satz von Newman)?

- 68.) Was besagt Yaos-Minimax-Prinzip für Kommunikationsprotokolle mit öffentlichem Zufall? Beweisskizze?
- 69.) Wie erhält man bei VLSI-Schaltkreisen untere Schranken für AT^2 mit Hilfe der Kommunikationskomplexität?
- 70.) Warum ist ein quadratischer Blow-up bei der Simulation von 2-Band-TM durch 1-Band-TM unvermeidbar?

Kapitel 16

- 71.) Wie funktioniert die Methode der Bausteineliminierung? Fasse die wesentlichen Beweisideen für die Anwendung auf $T_{\geq 2, n}$ zusammen.
- 72.) Beschreibe die Methode von Nechiporuk zum Nachweis von unteren Schranken für die Formelgröße und für die Größe von Branchingprogrammen. Wende diese auf eine geeignete Beispielfunktion an.

- 73.) Wie sieht der Zusammenhang zwischen Kommunikationskomplexität und Tiefe von Schaltkreisen aus? Zum Beweis:
- a) Wie können Alice und Bob einen Weg im Schaltkreis zu einem geeigneten Eingang berechnen?
 - b) Wie übersetzen wir umgekehrt Teile eines Protokolls in die zugehörige Bestandteile einer Formel?
- 74.) Wie sieht die Spezialisierung der Methode von Karchmer-Wigderson auf den Fall monotoner Schaltkreise aus und welche Beispiele für eine Anwendung der Methode in diesem Fall kennst du?

75.) Was besagt das Austauschlemma?

76.) Was kann über die Tiefe von Schaltkreisen polynomieller Größe bei unbeschränktem Eingangsgrad, die die Paritätsfunktionen berechnen, gesagt werden? Beweisidee?

77.) Beschreibe den Zusammenhang zwischen Kommunikationskomplexität und der Größe von Thresholdschaltkreisen sehr kleiner Tiefe.

- 78.) Beschreibe den Zusammenhang zwischen Kommunikationskomplexität und der Größe von k -OBDDs.
- 79.) Skizziere, wie man Kommunikationskomplexität auch für den allgemeineren Fall stereotyper BPs mit Längenschranke anwenden kann.
- 80.) Für welche Funktionen erhalten wir wie untere Schranken für die Größe von k -OBDDs bzw. längenbeschränkten, stereotypen BPs?