

Theoretische Informatik 3

Till Nierhoff

`nierhoff@informatik.hu-berlin.de`

Institut für Informatik

Humboldt-Universität zu Berlin

15. Juli 2003

Randomisierte Algorithmen

- können (faire) Münzen werfen
- und damit zB von allen Elementen einer Menge eines zufällig gleichverteilt auswählen

Beispiele:

- QuickSort
- MinCut

THEOREM

QuickSort benötigt im schlechtesten Fall (**Worst Case**) $\binom{n}{2} = \Theta(n^2)$ Vergleiche. Die erwartete Anzahl Vergleiche (**Average Case**) ist $2n \ln n$.

- Ausgabe **unabhängig** vom Zufall korrekt
- Laufzeit **abhängig** vom Zufall

→ „Las Vegas“-Algorithmus

DEFINITION

Ein **Multigraph** ist ein Graph, der Mehrfachkanten und Schleifen enthalten darf.

DEFINITION

Sei $G = (V, E)$ Multigraph. Seien U, W Knotenteilmengen mit $U, W \neq \emptyset$ und $V = U \dot{\cup} W$.

$$(U, W) := \{ \{u, w\} \mid \{u, w\} \in E, u \in U, w \in W \}$$

heißt **Cut**.

DEFINITION

Ein **Multigraph** ist ein Graph, der Mehrfachkanten und Schleifen enthalten darf.

DEFINITION

Sei $G = (V, E)$ Multigraph. Seien U, W Knotenteilmengen mit $U, W \neq \emptyset$ und $V = U \dot{\cup} W$.

$$(U, W) := \{ \{u, w\} \mid \{u, w\} \in E, u \in U, w \in W \}$$

heißt **Cut**.

DEFINITION

Das Problem **MINCUT** besteht darin, in einem gegebenen (Multi-)graphen einen Cut kleinstmöglicher Kardinalität zu finden.

Algorithmus KARGER

KARGER findet

- in einem gegebenen Multigraphen $G = (V, E)$
- einen Cut

Algorithmus KARGER

KARGER findet

- in einem gegebenen Multigraphen $G = (V, E)$
- einen Cut

- Eingabe: $G = (V, E)$
- Lösche Schleifen
- Falls $V = \{u, w\}$: Ausgabe E , stop
- Wähle $e \in E$ gleichverteilt
- Ausgabe $\text{KARGER}(G/e)$

THEOREM

KARGER gibt mit Wahrscheinlichkeit $\geq 2/n^2$ einen kleinstmöglichen Cut aus.

THEOREM

KARGER gibt mit Wahrscheinlichkeit $\geq 2/n^2$ einen kleinstmöglichen Cut aus.

- Ausgabe **abhängig** vom Zufall korrekt
- Laufzeit **unabhängig** vom Zufall

→ „Monte Carlo“-Algorithmus

Komplexitätsklassen

DEFINITION

Die Klasse ZPP besteht aus den Sprachen, für die es einen Las Vegas-Algorithmus mit polynomieller Laufzeit gibt.

DEFINITION

Die Klasse RP besteht aus den Sprachen L , für die es einen polynomiellen Monte Carlo-Algorithmus mit

$$\Pr[x \text{ akzeptiert}] \begin{cases} \geq 1/2 & x \in L \\ = 0 & \text{sonst.} \end{cases}$$