Diskrete Mathematik

Martin Avanzini Arne Dür Christoph Kollreider Georg Moser

Fakultät für Mathematik, Informatik und Physik @ UIBK
Sommersemester 2010

Zusammenfassung der letzten LV

Definition — NTM

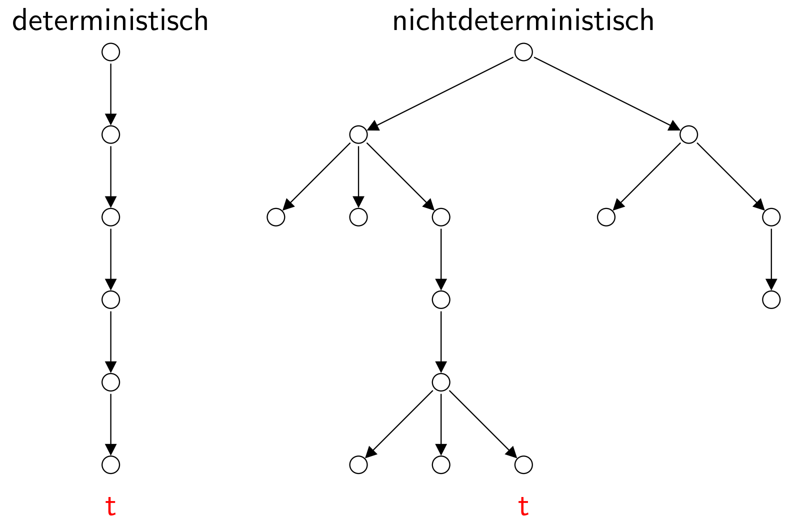
eine nichtdeterministische, k-bändige Turingmaschine N ist ein 9-Tupel

$$N = (Q, \Sigma, \Gamma, \vdash, \sqcup, \delta, s, t, r)$$

sodass

1. Q eine endliche Menge von Zuständen,
2. Σ eine endliche Menge von Eingabesymbolen,
3. Γ eine endliche Menge von Bandsymbolen, sodass $\Sigma \subseteq \Gamma$,
4. $\vdash \in \Gamma \setminus \Sigma$, der linke Endmarker,
5. $\sqcup \in \Gamma \setminus \Sigma$, das Blanksymbol,
6. $\delta \colon Q \times \Gamma^k \to \mathcal{P}(Q \times \Gamma^k \times \{\mathsf{L}, \mathsf{R}\}^k)$ die Übergangsfunktion,
7. $s \in Q$, der Startzustand,
8. $t \in Q$, der akzeptierende Zustand und
9. $r \in Q$, der verwerfende Zustand mit $t \neq r$.

Nichtdeterministischer Berechnungsbaum



Beachte

damit NTM N akzeptiert, genügt ein Weg, sodass N auf einen akzeptierenden Zustand trifft

Unentscheidbarkeit

Definition

definiere Halteproblem und Zugehörigkeitsproblem von TMs

$$\mathsf{HP} := \{M\sharp x \mid M \text{ hält bei Eingabe } x\}$$
$$\mathsf{MP} := \{M\sharp x \mid x \in \mathsf{L}(M)\}$$

Satz

HP und MP sind nicht rekursiv, aber rekursiv aufzählbar

Satz

es kann kein Testprogramm für "hello-world" Programme geben

Satz

die folgenden Probleme sind unentscheidbar:

1. das Postsche Korrespondenzproblem
2. ist eine beliebige Sprache regulär?

Übersicht

Automaten, reguläre Sprachen und Grammatiken, (nicht)-deterministische endliche Automaten, Teilmengenkonstruktion, Automaten mit ϵ-Übergängen, Umwandlung endlicher Automaten in reguläre Ausdrücke, Algebraische Gesetze für reguläre Ausdrücke, Pumpinglemma, Minimierung

Einführung in die Berechenbarkeitstheorie, Turing Maschinen, Entscheidungsprobleme, Äquivalente Formulierungen, Universelle Maschinen und Diagonalisierung,

Einführung in die Komplexitätstheorie, Laufzeitkomplexität, die Klassen P und NP, logarithmisch platzbeschränkte Reduktionen, Speicherplatzkomplexität

Einführung in die Komplexitätstheorie

Komplexitätstheorie analysiert Algorithmen und Probleme, zentrale Frage:

Welche Resourcen benötigt ein bestimmter Algorithmus oder ein Problem?

Resourcen

- Speicherplatz
- Rechenzeit

Problem & Algorithmus

- Problem: eine allgemeine, zu beantwortende Frage
- Algorithmus: Verfahren zur Beantwortung einer Frage

Komplexität

wir unterscheiden zwischen

- der Komplexität eines Algorithmus — `quicksort` hat $\mathrm{O}(n \cdot \log n)$
- der Komplexität eines Problems — MAZE ist in P

(n ist die Länge der zu sortierenden Liste)

Problem: MAZE

Problem — MAZE

gegeben

- gerichteten Graph G mit Eckenmenge E
- Knoten $s, t \in E$

$\exists$ Weg zwischen s und t?

Algorithmus

Nachfolgersuche — DM1

Komplexität

- Zeitkomplexität: $\mathrm{O}(n^2)$
- Platzbedarf: $\mathrm{O}(n)$

wobei n Anzahl der Knoten

Problem: Traveling Sales Person

Problem — TSP

gegeben

- n Städte
- Distanz $d_{ij} > 0$, sodass $d_{ij} = d_{ji}$

gesucht: Minimum der Kostensumme:

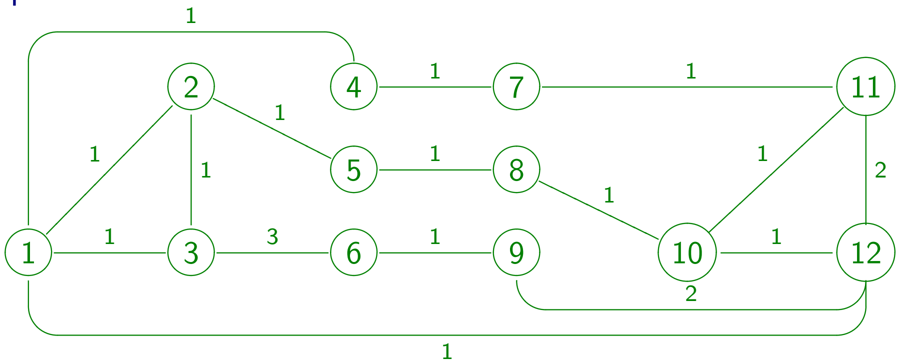
$$\sum_{i=1}^{n} d_{\pi(i),\pi(i+1)}$$

$\pi\colon \{1, \dots, n\} \to \{1, \dots, n\}$ Permutation mit $\pi(n+1) := \pi(1)$

Bemerkung

Tour kann in jeder beliebigen Stadt beginnen, muss aber wieder zum Ausgangspunkt zurück

Beispiel



- $\exists$ Tour die alle Städte verbindet? Ja
- $\exists$ Tour mit Budget $\leqslant 10$? Nein
- $\exists$ Tour mit Budget $\leqslant 20$? Ja
- minimale Tour:

  $(1, 4, 7, 11, 10, 8, 5, 2, 3, 6, 9, 12, 1)$ Budget $= 15$

man unterscheidet zwischen Optimierungsproblemen und Entscheidungsproblemen

Algorithmus

1. Aufzählen aller möglichen Lösungen
2. berechne die Kosten
3. wähle die Tour mit den geringsten Kosten

Komplexität

- Zeitkomplexität: $O(n!)$
- Zeitkomplexität kann auf $2^{O(n)}$ verbessert werden

hier bezeichnet n die Anzahl der Städte

Bemerkung

- wenn ein polynomieller Algorithmus existiert, dann gilt $P = NP$
- die Frage ob $P = NP$ ist eines der 7 Milleniumprobleme des Clay Institutes
- wenn ein polynomieller Algorithmus existiert, sind online Transaktionen unsicher

Problem: Generalised Geography

Problem — GG

das Spiel verallgemeinerte Länderkunde ist ein Zweipersonenspiel
Spieler heißen Anna und Otto, gegeben

- gerichteter Graph G und Startknoten s
- Anna beginnt im Land s sie wählt ein erreichbares (unmarkiertes) Land t, welches sie markiert
- Otto zieht von t weiter und markiert wieder
- derjenige Spieler, der nicht mehr ziehen kann verliert

$\exists$ Gewinnstrategie für Anna?

Beispiel

Länderkunde

Algorithmus A — Eingabe (G,b)

1. sei b der aktuelle Knoten und habe dieser Ausgangsgrad 0
   Spieler 1 verliert immer und A verwirft
2. eliminiere Knoten b und alle wegführenden Kanten
   bezeichne den neuen Graphen mit G'
3. $\forall$ unmittelbaren Nachfolger b' von b, rufe A rekursiv mit (G', b') auf
4. wenn alle Aufrufe akzeptieren, hat Spieler 2 eine Gewinnstrategie
5. wenn ein Aufruf nicht akzeptiert, hat Spieler 1 eine Gewinnstrategie
   also akzeptiert A

Komplexität

- Platzkomplexität: $O(n)$
- nur der Rekursionsstack braucht Platz, die Rekursionstiefe ist n

wobei n Größe des Graphen darstellt