Diskrete Mathematik

Arne Dür Kurt Girstmair Simon Legner
Georg Moser Harald Zankl

Fakultät für Mathematik, Informatik und Physik @ UIBK
Sommersemester 2011

Zusammenfassung der letzten LV

Definition

$$\mathrm{P} = \bigcup_{k \geqslant 1} \mathrm{DTIME}(n^k)$$

Definition

- ein Verifikator einer Sprache $L \subseteq \Sigma^*$, ist ein Algorithmus V sodass
$$L = \{x \in \Sigma^* \mid \exists\ c, \text{ sodass } V \text{ akzeptiert Eingabe } (x, c)\}$$
- ein polytime Verifikator ist Verifikator mit Laufzeit $\mathrm{O}(n^k)$ wobei $n = \ell(x)$
- Wort c wird Zertifikat genannt
- NP ist die Klasse der Sprachen, die einen polytime Verifikator haben

Übersicht

Endliche Automaten

Automaten, reguläre Sprachen und Grammatiken, (nicht)-deterministische endliche Automaten, Teilmengenkonstruktion, ϵ-NEAs, Umwandlung endlicher Automaten in reguläre Ausdrücke, Pumpinglemma, Minimierung

Berechenbarkeitstheorie

Einführung in die Berechenbarkeitstheorie, Turingmaschinen, Entscheidungsprobleme, Universelle Maschinen und Diagonalisierung

Komplexitätstheorie

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

Übersicht

Endliche Automaten

Automaten, reguläre Sprachen und Grammatiken, (nicht)-deterministische endliche Automaten, Teilmengenkonstruktion, ϵ-NEAs, Umwandlung endlicher Automaten in reguläre Ausdrücke, Pumpinglemma, Minimierung

Berechenbarkeitstheorie

Einführung in die Berechenbarkeitstheorie, Turingmaschinen, Entscheidungsprobleme, Universelle Maschinen und Diagonalisierung

Komplexitätstheorie

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

Speicherplatzkomplexität

Definition

sei M eine totale Mehrband-DTM

Speicherplatzkomplexität

Definition

sei M eine totale Mehrband-DTM

- die Speicherplatzkomplexität von M ist Funktion $S\colon \mathbb{N} \longrightarrow \mathbb{N}$, S misst die maximale Anzahl von Bandfeldern, die M liest auf allen Eingaben

Speicherplatzkomplexität

Definition

sei M eine totale Mehrband-DTM

- die Speicherplatzkomplexität von M ist Funktion $S \colon \mathbb{N} \to \mathbb{N}$, S misst die maximale Anzahl von Bandfeldern, die M liest auf allen Eingaben
- $S(n)$ ist der Speicherplatz von M, wenn n die Länge der Eingabe

Speicherplatzkomplexität

Definition

sei M eine totale Mehrband-DTM

- die Speicherplatzkomplexität von M ist Funktion $S\colon \mathbb{N} \to \mathbb{N}$,
  S misst die maximale Anzahl von Bandfeldern, die M liest
  auf allen Eingaben
- $S(n)$ ist der Speicherplatz von M, wenn n die Länge der Eingabe
- M heißt $S(n)$-Platz-Turingmaschine

Speicherplatzkomplexität

Definition

sei M eine totale Mehrband-DTM

- die Speicherplatzkomplexität von M ist Funktion $S\colon \mathbb{N} \to \mathbb{N}$, S misst die maximale Anzahl von Bandfeldern, die M liest auf allen Eingaben
- $S(n)$ ist der Speicherplatz von M, wenn n die Länge der Eingabe
- M heißt $S(n)$-Platz-Turingmaschine

Definition

sei M eine totale Mehrband-NTM

- die Speicherplatzkomplexität von M ist Funktion $S\colon \mathbb{N} \to \mathbb{N}$, S misst die maximale Anzahl von Bandfeldern die M liest auf allen Eingaben in jedem möglichen Berechnungspfad

Definition (vorläufig)

sei $S\colon\ \mathbb{N} \to \mathbb{N}$ eine numerische Funktion

DSPACE$(S(n)) = \{$L$(M) \mid M$ ist eine Mehrband-DTM mit Speicherplatz in O$(S(n))$ $\}$

NSPACE$(S(n)) = \{$L$(N) \mid N$ ist eine Mehrband-NTM mit Speicherplatz in O$(S(n))$ $\}$

Definition (vorläufig)

sei $S\colon \mathbb{N} \to \mathbb{N}$ eine numerische Funktion

DSPACE$(S(n)) = \{$L$(M) \mid M$ ist eine Mehrband-DTM mit Speicherplatz in O$(S(n))\ \}$

NSPACE$(S(n)) = \{$L$(N) \mid N$ ist eine Mehrband-NTM mit Speicherplatz in O$(S(n))\ \}$

Definition (vorläufig)

$$\mathrm{PSPACE} = \bigcup_{k \geqslant 1} \mathrm{DSPACE}(n^k) \qquad \mathrm{NPSPACE} = \bigcup_{k \geqslant 1} \mathrm{NSPACE}(n^k)$$

Definition (vorläufig)

sei $S\colon \mathbb{N} \to \mathbb{N}$ eine numerische Funktion

$$\mathrm{DSPACE}(S(n)) = \{\mathrm{L}(M) \mid M \text{ ist eine Mehrband-DTM mit Speicherplatz in } \mathrm{O}(S(n))\ \}$$

$$\mathrm{NSPACE}(S(n)) = \{\mathrm{L}(N) \mid N \text{ ist eine Mehrband-NTM mit Speicherplatz in } \mathrm{O}(S(n))\ \}$$

Definition (vorläufig)

$$\mathrm{PSPACE} = \bigcup_{k \geqslant 1} \mathrm{DSPACE}(n^k) \qquad \mathrm{NPSPACE} = \bigcup_{k \geqslant 1} \mathrm{NSPACE}(n^k)$$

Beispiel

$\mathrm{GG} \in \mathrm{PSPACE}$

Definition (vorläufig)

sei $S\colon \mathbb{N} \to \mathbb{N}$ eine numerische Funktion

$$\text{DSPACE}(S(n)) = \{\text{L}(M) \mid M \text{ ist eine Mehrband-DTM mit Speicherplatz in } \text{O}(S(n))\ \}$$

$$\text{NSPACE}(S(n)) = \{\text{L}(N) \mid N \text{ ist eine Mehrband-NTM mit Speicherplatz in } \text{O}(S(n))\ \}$$

Definition (vorläufig)

$$\text{PSPACE} = \bigcup_{k\geqslant 1} \text{DSPACE}(n^k) \qquad \text{NPSPACE} = \bigcup_{k\geqslant 1} \text{NSPACE}(n^k)$$

Beispiel

GG $\in$ PSPACE

Satz

$$\text{P} \subseteq \text{NP} \subseteq \text{PSPACE} = \text{NPSPACE}$$

Definition (vorläufig)

sei $S\colon \mathbb{N} \to \mathbb{N}$ eine numerische Funktion

$$\mathrm{DSPACE}(S(n)) = \{\mathrm{L}(M) \mid M \text{ ist eine Mehrband-DTM mit Speicherplatz in } \mathrm{O}(S(n))\ \}$$

$$\mathrm{NSPACE}(S(n)) = \{\mathrm{L}(N) \mid N \text{ ist eine Mehrband-NTM mit Speicherplatz in } \mathrm{O}(S(n))\ \}$$

Definition (vorläufig)

$$\mathrm{PSPACE} = \bigcup_{k \geqslant 1} \mathrm{DSPACE}(n^k) \qquad \mathrm{NPSPACE} = \bigcup_{k \geqslant 1} \mathrm{NSPACE}(n^k)$$

Beispiel

$\mathrm{GG} \in \mathrm{PSPACE}$

Satz

$$\mathrm{P} \subseteq \mathrm{NP} \subseteq \mathrm{PSPACE} = \mathrm{NPSPACE}$$

Beispiel

betrache nichtdeterministischen Algorithmus A für MAZE

1. gegeben Graph G, Start- und Endknoten s und t
2. sei b der aktuell betrachtete Knoten; setze $b = s$
3. wähle nichtdeterministisch einen Nachfolgerknoten b' von b
4. wenn $b' = t$, akzeptiere
5. sonst setze $b = b'$ und gehe zu 3

Beispiel

betrache nichtdeterministischen Algorithmus A für MAZE

1. gegeben Graph G, Start- und Endknoten s und t
2. sei b der aktuell betrachtete Knoten; setze $b = s$
3. wähle nichtdeterministisch einen Nachfolgerknoten b' von b
4. wenn $b' = t$, akzeptiere
5. sonst setze $b = b'$ und gehe zu 3

Frage

Was ist die Platzkomplexität von A?

Beispiel

betrache nichtdeterministischen Algorithmus A für MAZE

1. gegeben Graph G, Start- und Endknoten s und t
2. sei b der aktuell betrachtete Knoten; setze $b = s$
3. wähle nichtdeterministisch einen Nachfolgerknoten b' von b
4. wenn $b' = t$, akzeptiere
5. sonst setze $b = b'$ und gehe zu 3

Frage

Was ist die Platzkomplexität von A?

Antwort

Speicherplatzkomplexität einer TM, die A implementiert ist $O(n)$, wobei n die Länge der Codierung der Eingabe!

Definition

eine TM mit Eingabeband und Arbeitsband

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

ist eine TM mit zwei Bändern, sodass

- das 1te Band ein Leseband — Eingabeband
- alle anderen Bänder sind les- und schreibbar — Arbeitsbänder

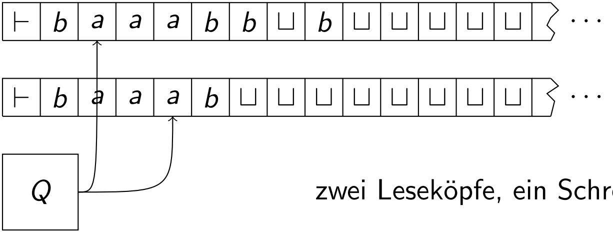
Definition

eine TM mit Eingabeband und Arbeitsband

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

ist eine TM mit zwei Bändern, sodass

- das 1te Band ein Leseband — Eingabeband
- alle anderen Bänder sind les- und schreibbar — Arbeitsbänder



zwei Leseköpfe, ein Schreibkopf

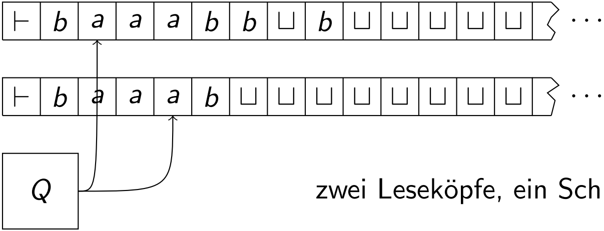
Definition

eine TM mit Eingabeband und Arbeitsband

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

ist eine TM mit zwei Bändern, sodass

- das 1te Band ein Leseband — Eingabeband
- alle anderen Bänder sind les- und schreibbar — Arbeitsbänder



zwei Leseköpfe, ein Schreibkopf

Bedingung für δ

$$\delta(p, a, b) = (q, a, c, D_1, D_2) \qquad \forall\ p, q \in Q,\ a, b, c \in \Gamma,\ D_1, D_2 \in \{\mathrm{L}, \mathrm{R}\}$$

Definition

sei $S\colon \mathbb{N} \to \mathbb{N}$ eine numerische Funktion

$\mathrm{DSPACE}(S(n)) = \{\mathrm{L}(M) \mid M$ ist eine Mehrband-DTM mit Speicherplatz auf den Arbeitsbändern in $\mathrm{O}(S(n))\}$

$\mathrm{NSPACE}(S(n)) = \{\mathrm{L}(N) \mid N$ ist eine Mehrband-NTM mit Speicherplatz auf den Arbeitsbändern in $\mathrm{O}(S(n))\}$

Definition

sei $S\colon \mathbb{N} \to \mathbb{N}$ eine numerische Funktion

$\mathrm{DSPACE}(S(n)) = \{\mathrm{L}(M) \mid M$ ist eine Mehrband-DTM mit Speicherplatz auf den Arbeitsbändern in $\mathrm{O}(S(n))\ \}$

$\mathrm{NSPACE}(S(n)) = \{\mathrm{L}(N) \mid N$ ist eine Mehrband-NTM mit Speicherplatz auf den Arbeitsbändern in $\mathrm{O}(S(n))\ \}$

Definition

sei $S\colon \mathbb{N} \to \mathbb{N}$ eine numerische Funktion

$\mathrm{DSPACE}(S(n)) = \{\mathrm{L}(M) \mid M$ ist eine Mehrband-DTM mit Speicherplatz auf den Arbeitsbändern in $\mathrm{O}(S(n))\}$

$\mathrm{NSPACE}(S(n)) = \{\mathrm{L}(N) \mid N$ ist eine Mehrband-NTM mit Speicherplatz auf den Arbeitsbändern in $\mathrm{O}(S(n))\}$

Definition

$$\mathrm{LOGSPACE} = \mathrm{DSPACE}(\log n) \qquad \mathrm{NLOGSPACE} = \mathrm{NSPACE}(\log n)$$

$$\mathrm{PSPACE} = \bigcup_{k \geqslant 1} \mathrm{DSPACE}(n^k) \qquad \mathrm{NPSPACE} = \bigcup_{k \geqslant 1} \mathrm{NSPACE}(n^k)$$

Definition

sei $S\colon \mathbb{N} \to \mathbb{N}$ eine numerische Funktion

$\text{DSPACE}(S(n)) = \{\mathrm{L}(M) \mid M$ ist eine Mehrband-DTM mit Speicherplatz auf den Arbeitsbändern in $\mathrm{O}(S(n))\ \}$

$\text{NSPACE}(S(n)) = \{\mathrm{L}(N) \mid N$ ist eine Mehrband-NTM mit Speicherplatz auf den Arbeitsbändern in $\mathrm{O}(S(n))\ \}$

Definition

$$\text{LOGSPACE} = \text{DSPACE}(\log n) \qquad \text{NLOGSPACE} = \text{NSPACE}(\log n)$$

$$\text{PSPACE} = \bigcup_{k \geqslant 1} \text{DSPACE}(n^k) \qquad \text{NPSPACE} = \bigcup_{k \geqslant 1} \text{NSPACE}(n^k)$$

Beispiele

MAZE $\in$ NLOGSPACE und GG $\in$ PSPACE

Logarithmisch Platzbeschränkte Reduktionen

Frage

Ist MAZE NLOGSPACE-vollständig?

Logarithmisch Platzbeschränkte Reduktionen

Frage

Ist MAZE NLOGSPACE-vollständig?

Antwort

die Frage ist nicht wohldefiniert

Logarithmisch Platzbeschränkte Reduktionen

Frage

Ist MAZE NLOGSPACE-vollständig?

Antwort

die Frage ist nicht wohldefiniert

Definition

ein logarithmischer Umwandler

$$T = (Q, \Sigma, \Gamma, \Delta, \vdash, \sqcup, \delta, s, t)$$

ist eine totale DTM mit 3 Bändern, sodass

- das 1te Band ist Leseband — Eingabeband
- vom 2te Band mit $O(\log n)$ Zeichen, Eingabelänge n — Arbeitsband
- das 3te Band ist Schreibeband — Ausgabeband

Logarithmisch Platzbeschränkte Reduktionen

Frage

Ist MAZE NLOGSPACE-vollständig?

Antwort

die Frage ist nicht wohldefiniert

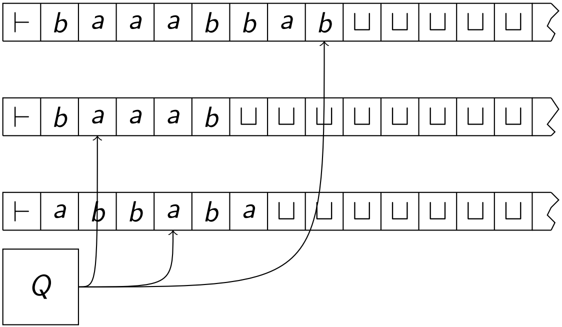
Definition

ein logarithmischer Umwandler

$$T = (Q, \Sigma, \Gamma, \Delta, \vdash, \sqcup, \delta, s, t)$$

ist eine totale DTM mit 3 Bändern, sodass

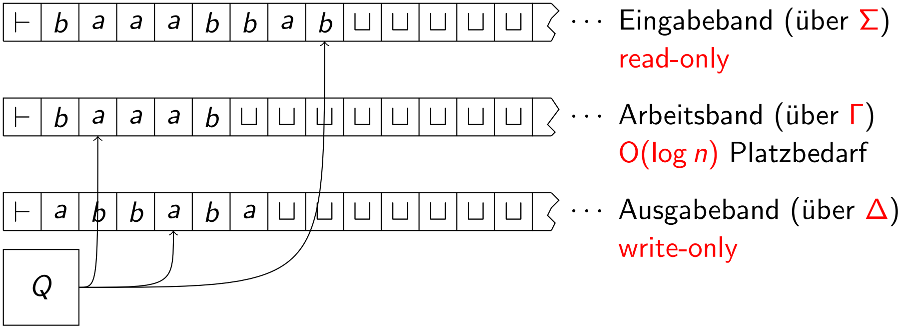
- das 1te Band ist Leseband — Eingabeband
- vom 2te Band mit $\mathrm{O}(\log n)$ Zeichen, Eingabelänge n — Arbeitsband
- das 3te Band ist Schreibeband — Ausgabeband



$\cdots$ Eingabeband (über Σ)
read-only

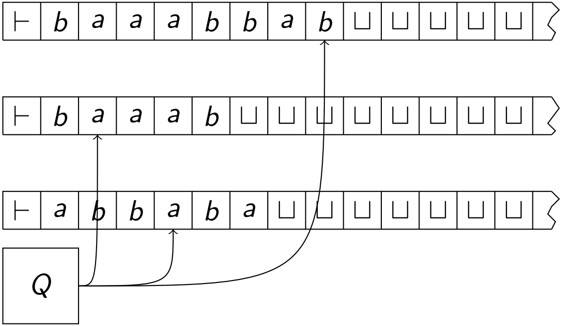
$\cdots$ Arbeitsband (über Γ)
$O(\log n)$ Platzbedarf

$\cdots$ Ausgabeband (über Δ)
write-only



Definition

1. $\exists$ logarithmischer Umwandler T mit Eingabealphabet Σ und Ausgabealphabet Δ



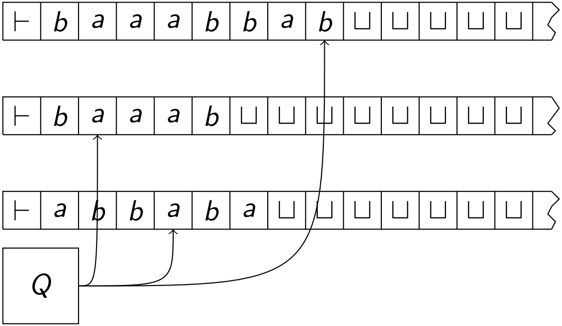
$\cdots$ Eingabeband (über Σ)
read-only

$\cdots$ Arbeitsband (über Γ)
$O(\log n)$ Platzbedarf

$\cdots$ Ausgabeband (über Δ)
write-only

Definition

1. $\exists$ logarithmischer Umwandler T mit Eingabealphabet Σ und Ausgabealphabet Δ
2. bei Eingabe $x \in \Sigma^*$, schreibt T $f(x)$ auf Ausgabeband



$\cdots$ Eingabeband (über Σ)
read-only

$\cdots$ Arbeitsband (über Γ)
$O(\log n)$ Platzbedarf

$\cdots$ Ausgabeband (über Δ)
write-only

Definition

1. $\exists$ logarithmischer Umwandler T mit Eingabealphabet Σ und Ausgabealphabet Δ
2. bei Eingabe $x \in \Sigma^*$, schreibt T $f(x)$ auf Ausgabeband

dann heißt $f : \Sigma^* \to \Delta^*$ berechenbar mit logarithmischem Platz

Reduktion mit logarithmischen Platz

Definition

1. $\exists\ R\colon \Sigma^* \to \Delta^*$
2. R berechenbar mit logarithmischem Platz
3. für $L \subseteq \Sigma^*$, $M \subseteq \Delta^*$ gilt $x \in L \iff R(x) \in M$

Reduktion mit logarithmischen Platz

Definition

1. $\exists\ R\colon \Sigma^* \to \Delta^*$
2. R berechenbar mit logarithmischem Platz
3. für $L \subseteq \Sigma^*$, $M \subseteq \Delta^*$ gilt $x \in L \iff R(x) \in M$

dann ist L auf M reduzierbar mit logarithmischem Platz ; kurz $L \leqslant_m^{\log} M$

Reduktion mit logarithmischen Platz

Definition

1. $\exists\ R\colon \Sigma^* \to \Delta^*$
2. R berechenbar mit logarithmischem Platz
3. für $L \subseteq \Sigma^*$, $M \subseteq \Delta^*$ gilt $x \in L \iff R(x) \in M$

dann ist L auf M reduzierbar mit logarithmischem Platz ; kurz $L \leqslant_m^{\text{log}} M$

Satz

seien L und M Sprachen; wenn $L \leqslant_m^{log} M$, dann gilt auch $L \leqslant_m^{p} M$

NLOGSPACE-Vollständigkeit von MAZE

Definition

sei M eine Sprache, $\mathcal{C}$ eine beliebige Komplexitätsklasse,

NLOGSPACE-Vollständigkeit von MAZE

Definition

sei M eine Sprache, $\mathcal{C}$ eine beliebige Komplexitätsklasse,

1. wenn $\forall$ Sprachen $L \in \mathcal{C}$ gilt: $L \leqslant_m^{\log} M$
   dann ist M $\leqslant_m^{\log}$-hart für $\mathcal{C}$

NLOGSPACE-Vollständigkeit von MAZE

Definition

sei M eine Sprache, $\mathcal{C}$ eine beliebige Komplexitätsklasse,

1. wenn $\forall$ Sprachen $L \in \mathcal{C}$ gilt: $L \leqslant_m^{\log} M$
   dann ist M $\leqslant_m^{\log}$-hart für $\mathcal{C}$
2. wenn M $\leqslant_m^{\log}$-hart für $\mathcal{C}$ und $M \in \mathcal{C}$
   dann ist M $\leqslant_m^{\log}$-vollständig für $\mathcal{C}$ oder (kurz) $\mathcal{C}$-vollständig

NLOGSPACE-Vollständigkeit von MAZE

Definition

sei M eine Sprache, $\mathcal{C}$ eine beliebige Komplexitätsklasse,

1. wenn $\forall$ Sprachen $L \in \mathcal{C}$ gilt: $L \leqslant_m^{\log} M$
   dann ist M $\leqslant_m^{\log}$-hart für $\mathcal{C}$
2. wenn M $\leqslant_m^{\log}$-hart für $\mathcal{C}$ und $M \in \mathcal{C}$
   dann ist M $\leqslant_m^{\log}$-vollständig für $\mathcal{C}$ oder (kurz) $\mathcal{C}$-vollständig

Beispiele

- GG ist $\leqslant_m^{\log}$-vollständig für PSPACE
- TSP ist $\leqslant_m^{\log}$-vollständig für NP
- MAZE ist $\leqslant_m^{\log}$-vollständig für NLOGSPACE

NLOGSPACE-Vollständigkeit von MAZE

Definition

sei M eine Sprache, $\mathcal{C}$ eine beliebige Komplexitätsklasse,

1. wenn $\forall$ Sprachen $L \in \mathcal{C}$ gilt: $L \leqslant_m^{\log} M$
   dann ist M $\leqslant_m^{\log}$-hart für $\mathcal{C}$
2. wenn M $\leqslant_m^{\log}$-hart für $\mathcal{C}$ und $M \in \mathcal{C}$
   dann ist M $\leqslant_m^{\log}$-vollständig für $\mathcal{C}$ oder (kurz) $\mathcal{C}$-vollständig

Beispiele

- GG ist $\leqslant_m^{\log}$-vollständig für PSPACE
- TSP ist $\leqslant_m^{\log}$-vollständig für NP
- MAZE ist $\leqslant_m^{\log}$-vollständig für NLOGSPACE

Satz

$$\text{LOGSPACE} \subseteq \text{NLOGSPACE} \subseteq \text{P} \subseteq \text{NP} \subseteq \text{PSPACE} = \text{NPSPACE}$$

NLOGSPACE-Vollständigkeit von MAZE

Definition

sei M eine Sprache, $\mathcal{C}$ eine beliebige Komplexitätsklasse,

1. wenn $\forall$ Sprachen $L \in \mathcal{C}$ gilt: $L \leqslant_m^{\log} M$
   dann ist M $\leqslant_m^{\log}$-hart für $\mathcal{C}$
2. wenn M $\leqslant_m^{\log}$-hart für $\mathcal{C}$ und $M \in \mathcal{C}$
   dann ist M $\leqslant_m^{\log}$-vollständig für $\mathcal{C}$ oder (kurz) $\mathcal{C}$-vollständig

Beispiele

- GG ist $\leqslant_m^{\log}$-vollständig für PSPACE
- TSP ist $\leqslant_m^{\log}$-vollständig für NP
- MAZE ist $\leqslant_m^{\log}$-vollständig für NLOGSPACE

Satz

$$\text{LOGSPACE} \subseteq \text{NLOGSPACE} \subseteq \text{P} \subseteq \text{NP} \subseteq \text{PSPACE} = \text{NPSPACE}$$

Vielen Dank für Ihre Aufmerksamkeit!