Probabilistische Turingmaschinen

Eike Müller

1. Juni 2010

Inhalt

Motivation

Primzahltest nach Soloway und Strassen

Probabilistische Turingmaschinen

Definition (Probabilistische Turingmaschine)

Eine probabilistische Turingmaschine (PTM) ist eine Turingmaschine mit zwei Übergangsfunktionen δ_0, δ_1.
Bei der Ausführung der PTM M bei Eingabe von einem $x \in \{0,1\}^*$ wird im jedem Schritt δ_0 mit Wahrscheinlichkeit $\frac{1}{2}$ verwendet und sonst δ_1.
Eine PTM läuft in $T : \mathbb{N} \to \mathbb{N}$ Zeit, wenn sie für jedes $x \in \{0,1\}^*$ in $T(|x|)$ Schritten unabhängig von der Wahl der Übergangsfunktionen anhält.

Probabilistische Turingmaschinen

Definition (Klasse $\mathbf{BPP}$)

Für $T : \mathbb{N} \to \mathbb{N}$ definieren wir die Klasse $\mathbf{BPTIME}(T(n))$ als die Menge der Sprachen $L \subseteq \{0,1\}^*$ zu denen eine PTM M existiert, sodass für alle $x \in \{0,1\}^*$

$$\Pr\left[M(x) = L(x)\right] \geq \frac{2}{3}$$

und M hält nach $O(T(|x|))$ Schritten an.
Definiere nun $\mathbf{BPP} = \bigcup_{c>0} \mathbf{BPTIME}\left(n^c\right)$

Probabilistische Turingmaschinen

Definition (Klasse $\mathbf{BPP}$, *alternative Definition*)

Eine Sprache $L \subseteq \{0,1\}^*$ liegt genau dann in $\mathbf{BPP}$, wenn eine polynomielle Turingmaschine M und ein Polynom $p : \mathbb{N} \to \mathbb{N}$ existiert, sodass für alle $x \in \{0,1\}^*$

$$\Pr_{r \in_R \{0,1\}^{p(|x|)}} [M(r,x) = L(x)] \geq \frac{2}{3}$$

gilt.

Einseitige Fehler

Definition (Die Klassen $\mathbf{RP}$ und $\mathbf{coRP}$)

Die Klasse $\mathbf{RTIME}(T(n))$ enthält alle Sprachen $L \subseteq \{0,1\}^*$, für die eine probabilistische TM M mit einer Laufzeit $O(T(n))$ existiert, sodass

$$x \in L \Rightarrow \Pr[M(x) = 1] \geq \frac{2}{3}$$
$$x \notin L \Rightarrow \Pr[M(x) = 0] = 1$$

für alle $x \in \{0,1\}^*$ gilt.
Definiere nun $\mathbf{RP} = \cup_{c>0}\mathbf{RTIME}(n^c)$ und $\mathbf{coRP} = \{L \subseteq \{0,1\}^* \mid \bar{L} \in \mathbf{RP}\}$

Nullseitige Fehler

Definition (Klasse $\mathbf{ZPP}$)

Die Klasse $\mathbf{ZTIME}(T(n))$ enthält alle Sprachen $L \subseteq \{0,1\}^*$, für die eine probabilistische TM M mit einer erwarteten Laufzeit $O(T(n))$ existiert, sodass

$$\Pr[M(x) = L(x)] = 1$$

für alle $x \in \{0,1\}^*$ gilt.
Definiere nun $\mathbf{ZPP} = \cup_{c>0}\mathbf{ZTIME}(n^c)$.

Theorem

$\mathbf{ZPP} = \mathbf{RP} \cap \mathbf{coRP}$.

Fehlerreduktion

Theorem (Error reduction for $\mathbf{BPP}$)

Sei $L \subseteq \{0,1\}^*$ eine Sprache und angenommen es existiert eine polynomielle PTM M, sodass

$$\Pr\left[M(x) = L(x)\right] \geq \frac{1}{2} + |x|^{-c}$$

für alle $x \in \{0,1\}^*$ und ein $c > 0$. So existiert für jedes $d > 0$ eine polynomielle PTM M', so dass

$$\Pr\left[M'(x) = L(x)\right] \geq 1 - 2^{-|x|^d}$$

für alle $x \in \{0,1\}^*$.

erwartete Laufzeit

$\mathbf{BPTIME}$ und $\mathbf{RTIME}$ lassen sich auch durch die erwartete Laufzeit definieren.

p-Münzen

Lemma

Eine Münze mit $\Pr[\text{Kopf}] = p$, $p \in (0,1)$ lässt sich von einer PTM in $O(1)$ erwarteter Laufzeit simulieren, wenn das i-te Bit von p in $\text{poly}(i)$ berechnet werden kann.

Lemma

Eine Münze mit $\Pr[\text{Kopf}] = \frac{1}{2}$ lässt sich von einer PTM in $O(\frac{1}{p(1-p)})$ erwarteter Laufzeit simulieren, wenn die PTM nur Zugriff auf p-Münzen besitzt.

Beispiel

- Primzahltest
- Nullpolynomtest

Relation zur Polynomialzeithierarchie

Theorem (Sipser-Gács Theorem)

$\mathbf{BPP} \subseteq \mathbf{\Sigma}_2^p \cap \mathbf{\Pi}_2^p$.

Probabilistische Reduktionen

Definition

Eine Sprache $B \subseteq \{0,1\}^*$ lässt sich auf eine Sprache $C \subseteq \{0,1\}^*$ unter einer probabilistischen polynomialzeit Reduktion reduzieren ($B \leq_r C$), falls eine polynomielle PTM M existiert, sodass für alle $x \in \{0,1\}^*$

$$\Pr[B(M(x)) = C(x)] \geq \frac{2}{3}$$

gilt.

Definition

$\mathbf{BP} \cdot \mathbf{NP} = \{L \mid L \leq_r \text{3SAT}\}$.

Probabilistische Speicherplatzkomplexität

Definition (Klasse $\mathbf{BPL}$ und $\mathbf{RL}$)

Eine Sprache $L \subseteq \{0,1\}^*$ liegt in $\mathbf{BPL}$, falls eine $O(log(n))$-platz probabilistische TM M existiert, sodass

$$\Pr[M(x) = L(x)] \geq \frac{2}{3}.$$

Eine Sprache $L \subseteq \{0,1\}^*$ liegt in $\mathbf{RL}$, falls eine $O(log(n))$-platz probabilistische TM M existiert, sodass

$$x \in L \Rightarrow \Pr[M(x) = 1] \geq \frac{2}{3}$$
$$x \notin L \Rightarrow \Pr[M(x) = 0] = 1$$

Probabilistische Speicherplatzkomplexität

Beispiel

UPATH $\in \mathbf{RL}$

Zusammenfassung

- $\mathbf{P} \subseteq \mathbf{BPP} \subseteq \mathbf{EXP}$,
- es wird vermutet, dass $\mathbf{P} = \mathbf{BPP}$,
- $\mathbf{RP}, \mathbf{coRP}, \mathbf{ZPP} \subseteq \mathbf{BPP}$,
- $\mathbf{BPP} \subseteq \mathbf{PH}$ und
- $\mathbf{P} = \mathbf{NP} \Rightarrow \mathbf{P} = \mathbf{BPP}$.

Ende