Probabilistische Turingmaschinen

Eike Müller

1. Juni 2010

Inhaltsverzeichnis

1 Motivation

Es gibt verschiedene Algorithmen, die Zufall verwenden um bestimmte Aufgabe zu lösen. Ein Beispiel ist dafür der Primzahltest nach Solovay und Strassen. Diese Algorithmen liefern zwar nicht immer das korrekte Ergebnis, aber durch Mehrfachanwendung werden diese Verfahren praxistauglich. Somit macht es Sinn, diese Probleme zu formalisieren.

2 Probabilistische Turingmaschinen

Definiton 1 (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.

Definiton 2 (Klasse **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 $\mathbf{BPP} = \bigcup_{c>0} \mathbf{BPTIME}\left(n^c\right)$

Eine probabilistische Turingmaschine, kann man sich auch als eine deterministische Turingmaschine vorstellen, welche die Abfolge der Entscheidungen zwischen den einzelnen Übergangsfunktionen, als Sequenz von Einsen und Nullen übergeben bekommt. Mit dieser Anschauung erhält man folgende analoge Definition der Klasse **BPP**.

Definiton 3 (Klasse **BPP**, *alternative Definition*)**.** *Eine Sprache $L \subseteq \{0,1\}^*$ liegt genau dann in* **BPP***, wenn eine polynomielle Turingmaschine M und ein Polynom $p : \mathbb{N} \to \mathbb{N}$ existiert, sodass für alle $x \in \{0,1\}^*$*

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

gilt.

Man kann sich leicht davon überzeugen, dass diese Definition nicht eine größere Klasse definiert, denn eine PTM kann am Anfang auch einfach einen zufälligen String $r \in \{0,1\}^{p(|x|)}$ erzeugen und sich dann wie eine deterministische TM verhalten.

Bis jetzt ist nur $\mathbf{P} \subseteq \mathbf{BPP} \subseteq \mathbf{EXP}$ bekannt, aber es wird vermutet dass $\mathbf{BPP} = \mathbf{P}$.

3 Einseitige Fehler und Nullseitige Fehler

3.1 Einseitige Fehler

Definiton 4 (Die Klassen **RP** und **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* $\mathbf{coRP} = \{L \subseteq \{0,1\}^* \mid \bar{L} \in \mathbf{RP}\}$

Es gilt $\mathbf{RP} \subseteq \mathbf{NP}$, denn jeder akzeptierender Zweig ist eine ein gültiges Zertifikat. Im Gegensatz dazu ist nicht bekannt ob $\mathbf{BPP} \subseteq \mathbf{NP}$ gilt.

3.2 Nullseitige Fehler

Für eine PTM M mit Eingabe $x \in \{0,1\}^*$ definieren wir die Zufallsvariable $T_{M,x}$ als die Laufzeit von M bei Eingabe x. Wir sagen nun M hat eine erwartete Laufzeit von $T(n)$ wenn

$$E[T_{M,x}] \leq T(|x|)$$

für alle $x \in \{0,1\}^*$ gilt.

Definiton 5 (Klasse **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 1. $\mathbf{ZPP} = \mathbf{RP} \cap \mathbf{coRP}$.

4 Robustheit

4.1 Fehlerreduktion

In der Definition von der Klasse **BPP** haben wir angenommen, das die Sprachen mit einer Wahrscheinlichkeit von $\frac{2}{3}$ korrekt erkannt werden müssen. Diese $\frac{2}{3}$ sind aber recht willkürlich gewählt. Mit Hilfe des nächsten Theorems zeigen wir das die Klasse **BPP** unabhängig von der Wahl der Wahrscheinlichkeit ist. Ausreichend für die Wahrscheinlichkeit ist eine Zahl $> \frac{1}{2}$ bzw. sogar $\frac{1}{2} + |x|^{-c}$ für alle $c > 0$ ist ausreichend.

Theorem 2 (Error reduction for **BPP**). *Sei* $L \subseteq \{0,1\}^*$ *eine Sprache und angenommen es existiert eine polynomielle PTM* M*, sodass*

$$\Pr[M(x) = L(x)] \geq \frac{1}{2} + |x|^{-c} \text{ für alle } x \in \{0,1\}^* \text{ und ein } c > 0.$$

So existiert für jedes $d > 0$ eine polynomielle PTM M', so dass

$$\Pr\left[M'(x) = L(x)\right] \geq 1 - 2^{-|x|^d} \text{ für alle } x \in \{0,1\}^*.$$

Ein ähnliche Aussage existiert auch für die Klassen **RP** und **coRP**. Nur hier funktioniert es für alle Wahrscheinlichkeiten > 0.

4.2 worstcase Laufzeit vs. erwartete Laufzeit

Die Definitionen von **BPTIME** und **RTIME** verwenden, dass eine PTM M innerhalb von $T(n)$ Schritten anhält, wobei $T(n)$ ein Polynom ist. Im Gegensatz kann man in der Definition auch die erwartete Laufzeit verwenden, denn eine PTM M mit erwarteter Laufzeit $T(n)$ hält nach Markow's Ungleichung in 99% aller Fälle in $100T(n)$ Zeit an, was wiederum ein Polynom ist. Somit ändert sich die Wahrscheinlichkeit um maximal 1% und nach dem Fehlerreduktionstheorem ändert dies nicht die Komplexitätsklasse (**BPP**, **RP**).

4.3 p-Münzen

Lemma 1. *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 2. *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.*

5 Beispiele

Ein Beispiel ist wie bereits erwähnt der Primzahltest nach Solovay und Strassen.

5.1 Nullpolynomtest

Der Nullpolynomtest entscheidet für ein Polynom $p(x_1, \ldots, x_n)$, welches durch einen algebraischer Schaltkreis gegeben ist, ob p das Nullpolynom beschreibt ($p \in \mathsf{ZEROP}$).

6 Relation zur Polynomialzeithierarchie

Theorem 3 (Sipser-Gács Theorem)**.** $\mathbf{BPP} \subseteq \mathbf{\Sigma}_2^p \cap \mathbf{\Pi}_2^p$.

Da für $\mathbf{P} = \mathbf{NP}$ die Polynomialzeithierarchie zusammenfällt, gilt

$$\mathbf{P} = \mathbf{NP} \Rightarrow \mathbf{BPP} = \mathbf{P}.$$

7 Probabilistische Reduktionen

Definiton 6. *Eine Sprache $B \subseteq \{0,1\}^*$ lässt sich auf eine Sprache $C \subseteq \{0,1\}^*$ unter einer probabilistischen polynomiellen 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.

Die Komplexitätsklasse **NP** wurde als die folgende Menge definiert

$$\mathbf{NP} = \{L \mid L \leq_p \mathsf{3SAT}\}.$$

Ersetzt man die man die deterministische polynomielle Reduktion durch eine probabilisitische polynomielle Reduktion, so erhält man folgende Klasse

Definiton 7. $\mathbf{BP} \cdot \mathbf{NP} = \{L \mid L \leq_r \mathsf{3SAT}\}$.

8 Probabilistische Speicherplatzkomplexität

Definiton 8 (Klasse **BPL** und **RL**)**.** *Eine Sprache* $L \subseteq \{0,1\}^*$ *liegt in* **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* **RL**, *falls eine* $O(log(n))$*-platz probabilistische TM* M *existiert, sodass*

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

Für **BPL** und **RL** gilt auch das Fehlerreduktionstheorem, denn man muss nur die Anzahl der Ausführungen der PTM M und die Anzahl der Erfolge zählen. Da beide Zahlen maximal polynomiell wachsen können, liegt deren Darstellung in $O(\log(n))$ und somit lässt sich die Fehlerreduktion in $O(\log(n))$ Speicher durchführen.

Theorem 4. $\mathsf{UPATH} \in \mathbf{RL}$

9 Zusammenfassung

Wir haben folgende Relation

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