7.2 Probabilistische Turingmaschinen und Komplexitätsklassen

Probabilistische Turingmaschine ≙
eine TM, die in jedem Schritt ihrer Berechnung eine Münze werfen kann.

Definition 7.5 (PTM)

(a) Eine probabilistische Turingmaschine (PTM) M mit zwei Transitionsfunktionen δ_0 und δ_1.
Bei Eingabe eines Worts $x \in \{0,1\}^*$ wird jeder einzelne Berechnungsschritt mit Wahrscheinlichkeit $1/2$ gemäß δ_0 und mit Wahrscheinlichkeit $1/2$ gemäß δ_1 durchgeführt.
M gibt am Ende ihrer Berechnung stets 1 (für "akzeptieren") oder 0 (für "verwerfen") aus.
Wir schreiben $M(x)$, um die Zufallsvariable (mit Werten aus $\{0,1\}$) zu bezeichnen, die der Ausgabe von M bei Eingabe x entspricht.

(b) Sei $T: \mathbb{N} \to \mathbb{N}$.
Eine PTM M ist $T(n)$-zeitbeschränkt, falls für jedes $x \in \{0,1\}^*$ gilt: Unabhängig von den zufälligen Entscheidungen, die M trifft, hält M bei Eingabe x nach höchstens $T(|x|)$ Schritten an.

Komplexitätsklassen mit einseitigem, beschränktem Fehler

Definition 7.6 (RTIME(T(n)), RP, coRP)

(a) Sei $T: \mathbb{N} \to \mathbb{N}$.

Die Klasse RTIME(T(n)) besteht aus allen Sprachen $L \subseteq \{0,1\}^*$, für die es eine T(n)-zeitbeschränkte PTM M gibt, so dass für alle Eingaben $x \in \{0,1\}^*$ gilt

- falls $x \in L$, so ist $\Pr[M(x) = 1] \geq 2/3$
- falls $x \notin L$, so ist $\Pr[M(x) = 0] = 1$

D.h.: Jedes $x \notin L$ wird von M stets verworfen; jedes $x \in L$ wird von M mit Wahrscheinlichkeit $\geq 2/3$ akzeptiert.

(b) $RP := \bigcup_{c \geq 1} RTIME(n^c)$ ist die Klasse aller randomisiert in Polynomialzeit lösbaren Probleme

(c) $coRP := \{ L \subseteq \{0,1\}^* : \overline{L} \in RP \}$.

D.h.: $L \in coRP \iff$ es gibt eine in Polynomialzeit laufende PTM M, so dass für alle Eingaben $x \in \{0,1\}^*$ gilt:

- falls $x \in L$, so ist $\Pr[M(x) = 1] = 1$
- falls $x \notin L$, so ist $\Pr[M(x) = 0] \geq 2/3$

D.h.: Jedes $x \in L$ wird von M stets akzeptiert, jedes $x \notin L$ wird von M mit Wahrscheinlichkeit $\geq 2/3$ verworfen.

Lemma 7.7 (Wahrscheinlichkeitsverstärkung für RP)

Für jedes $L \in RP$ und jedes Polynom $p: \mathbb{N} \to \mathbb{N}$ gibt es eine polynomiell zeitbeschränkte PTM M, s.d. f.a. $x \in \{0,1\}^*$ gilt:

- falls $x \in L$, so ist $Pr[M(x) = 1] \geq 1 - \frac{1}{2^{p(|x|)}}$
- falls $x \notin L$, so ist $Pr[M(x) = 0] = 1$

Beweis:

Wegen $L \in RP$ gibt es eine polynomiell zeitbeschränkte PTM M' s.d. f.a. $x \in \{0,1\}^*$ gilt

- falls $x \in L$, so $Pr[M'(x) = 1] \geq 2/3$
- falls $x \notin L$, so $Pr[M'(x) = 0] = 1$

Sei M die PTM, die bei Eingabe $x \in \{0,1\}^*$ folgendes tut:

1) Berechne $k := p(|x|)$
2) Starte unabhängig voneinander k Läufe von M' bei Eingabe x
3) Falls mindestens einer dieser k Läufe die Ausgabe 1 liefert, so gib 1 aus; ansonsten gib 0 aus

Offensichtlicherweise ist M polynomiell zeitbeschränkt.

Außerdem gilt:

- Falls $x \notin L$, so gibt jeder der k Läufe von M' bei Eingabe x den Wert 0 aus. M gibt dann auch 0 aus, und es gilt:

  $Pr[M(x) = 0] = 1$.

- Falls $x \in L$, so gilt für jeden einzelnen der k Läufe von M' bei Eingabe x: $\Pr[M'(x)=1] \geq 2/3$,

  also $\Pr[M'(x)=0] \leq \frac{1}{3} < \frac{1}{2}$.

  M gibt nur dann 0 aus, wenn jeder der k Läufe 0 von M' ausgibt. D.h.:

  $\Pr[M(x)=0] < \left(\frac{1}{2}\right)^k$, und $\Pr[M(x)=1] > 1-\left(\frac{1}{2}\right)^k = 1-\frac{1}{2^{p(|x|)}}$!

Beispiel 7.8

Aus Theorem 7.1 und der Wk-Verstärkungsmethode aus dem Beweis von Lemma 7.7 erhalten wir für das Primzahlproblem $\text{PRIMES} := \{\langle n \rangle : n \text{ ist eine Primzahl}\}$:

$\text{PRIMES} \in \text{co}RP$.

Bemerkung 7.9

(i) $RP \subseteq NP$, denn aus Theorem 2.7 folgt f.a. $L \subseteq \{0,1\}^*$:

$L \in NP \Leftrightarrow$ es gibt eine polynomiell zeitbeschränkte PTM M, s.d. f.a. Eingaben $x \in \{0,1\}^*$ gilt:

- falls $x \in L$, so $\Pr[M(x)=1] > 0$
- falls $x \notin L$, so $\Pr[M(x)=0] = 1$.

(ii) $P \subseteq RP$ (klar.)

Probabilistische Komplexitätsklassen ohne Fehler

Ist M eine PTM und x eine Eingabe für M, so schreiben wir $T_{M,x}$, um die Zufallsvariable zu bezeichnen, die die Laufzeit von M bei Eingabe x angibt.

D.h: Für $t \in \mathbb{N}$ und $0 \leq p \leq 1$ gilt

$\Pr[T_{M,x} \leq t] = p$ genau dann, wenn p die Wahrscheinlichkeit dafür ist, dass M bei Eingabe x nach höchstens t Schritten anhält.

Sei $T: \mathbb{N} \to \mathbb{N}$. Wir sagen:

M hat <u>erwartete Laufzeit $\leq T(n)$</u>, falls für jedes $x \in \{0,1\}^*$ gilt: $E[T_{M,x}] \leq T(|x|)$, d.h:

Der Erwartungswert der Zufallsvariable $T_{M,x}$ ist $\leq T(|x|)$

<u>Definition 7.10</u> (ZTIME(T(n)), ZPP)

(a) Sei $T: \mathbb{N} \to \mathbb{N}$.

Die Klasse ZTIME(T(n)) besteht aus allen Sprachen $L \subseteq \{0,1\}^*$, für die es eine PTM M mit den folgenden Eigenschaften gibt:

(1) M hat erwartete Laufzeit $O(T(n))$ und

(2) für jedes $x \in \{0,1\}^*$ gilt:

- falls $x \in L$, so gibt M bei Eingabe x bei jedem terminierenden Lauf den Wert 1 aus

- falls $x \notin L$, so gibt M bei Eingabe x bei jedem terminierenden Lauf den Wert 0 aus.

Bemerkung: Der Buchstabe "Z" in $ZTIME(T(n))$ steht für "zero-sided error" d.h. "ohne Fehler".

(b) $ZPP := \bigcup_{c \geq 1} ZTIME(n^c)$

("zero-error probabilistic polynomial time")

Klar: $P \subseteq ZPP$

Theorem 7.11

$ZPP = RP \cap coRP$

Beweis:

"$\subseteq$": Sei $L \in ZPP$ und sei M eine PTM mit erwarteter Laufzeit $\leq n^c$, s.d. für jedes $x \in \{0,1\}^*$ gilt:

- falls $x \in L$, so gibt M bei Eingabe x bei jedem terminierenden Lauf den Wert 1 aus
- falls $x \notin L$, so gibt M bei Eingabe x bei jedem terminierenden Lauf den Wert 0 aus.

Für $i \in \{0,1\}$ sei M_i die $4 \cdot n^c$-zeitbeschränkte PTM, die folgendes tut: M_i simuliert die ersten $4 \cdot n^c$ Schritte von M. Falls M in dieser Zeit anhält, so gibt M_i die Ausgabe von M aus. Ansonsten gibt M die Ausgabe i aus.

man leicht nachweisen, dass folgendes f.a. $x \in \{0,1\}^*$ gilt:
(Details: Übung):

- Falls $x \in L$, so $\Pr[M_0(x) = 1] \geq 2/3$ und $\Pr[M_1(x) = 1] = 1$
- Falls $x \notin L$, so $\Pr[M_0(x) = 0] = 1$ und $\Pr[M_1(x) = 0] \geq 2/3$

Zur Erinnerung: Die Markov-Ungleichung besagt, dass für alle Zufallsvariablen X mit Werten ≥ 0 und für alle Zahlen $a > 0$ gilt: $\Pr[X > a] \leq \frac{E[X]}{a}$.

Somit bezeugt M_0, dass $L \in RP$ ist.
M_1 bezeugt, dass $L \in coRP$ ist.
Also ist $ZPP \subseteq RP \cap coRP$.

"$\supseteq$": Sei $L \in RP \cap coRP$, und seien M_1 und M_2 zwei PTMen, die dies bezeugen. Sei $c \in \mathbb{N}$ s.d. M_1 und M_2 n^c-zeitbeschränkt sind.
Sei M eine PTM, die bei Eingabe $x \in \{0,1\}^*$ folgendes tut

> Für $r = 1, 2, 3, \ldots$ tue folgendes:
>
> 1) simuliere n^c Schritte von M_1 bei Eingabe x;
> sei $a_1 \in \{0,1\}$ die entsprechende Ausgabe
> 2) simuliere n^c Schritte von M_2 bei Eingabe x;
> sei $a_2 \in \{0,1\}$ die entsprechende Ausgabe
> 3) Falls $a_1 = 1$, so STOPP mit Ausgabe 1
> Falls $a_2 = 0$, so STOPP mit Ausgabe 0

Wir wissen, dass f.a. $x \in \{0,1\}^*$ gilt:

- Falls $x \in L$, so $\Pr[M_1(x)=1] \geq 2/3$ und $\Pr[M_2(x)=1] = 1$
- Falls $x \notin L$, so $\Pr[M_1(x)=0] = 1$ und $\Pr[M_2(x)=0] \geq 2/3$

Somit gilt für jeden terminierenden Lauf von M bei Eingabe x:

- M gibt 1 aus $\Leftrightarrow$ M_1 gibt 1 aus $\Leftrightarrow$ $x \in L$
- M gibt 0 aus $\Leftrightarrow$ M_2 gibt 0 aus $\Leftrightarrow$ $x \notin L$

D.h.: M erfüllt die Bedingung (2) von Definition 7.10.

Laufzeitanalyse:

Für jede einzelne Runde r von M gilt:

$$p := \Pr[a_1 = 1 \text{ oder } a_2 = 0] \geq 2/3$$

In jeder einzelnen Runde r werden $\leq 2n^c + 2$ Schritte durchgeführt.

Somit ist die erwartete Laufzeit von M bei Eingabe $x \leq$

$$\sum_{r=1}^{\infty} \underbrace{r \cdot (2n^c+2)}_{\text{Laufzeit bei Stopp nach genau } r \text{ Runden}} \cdot \underbrace{(1-p)^{r-1} \cdot p}_{\text{Wk dafür, dass kein Stopp nach Runden } 1,\dots,r-1, \text{ aber Stopp nach } r \text{ Runden}}$$

$$\leq (2n^c+2) \cdot p \cdot \sum_{r=1}^{\infty} r \cdot (1-p)^{r-1} = (2n^c+2) \cdot \frac{p}{(1-p)} \cdot \underbrace{\sum_{r=1}^{\infty} r \cdot (1-p)^r}_{= \frac{(1-p)}{p^2}} = (2n^2+2) \cdot \dots$$

Denn: Für $0 < c < 1$ gilt:

$$\sum_{r=1}^{\infty} r \cdot c^r = \frac{c}{(1-c)^2}$$

(Nachrechnen: Übung!)

Somit hat M erwartete polynomielle Laufzeit und bezeugt daher, dass $L \in ZPP$ ist.

Somit ist $RP \cap coRP \subseteq ZPP$. □

Komplexitätsklassen mit zweiseitigem, beschränktem Fehler

Notation 7.12

Für eine Sprache $L \subseteq \{0,1\}^*$ ist der Wert $L(x) \in \{0,1\}$ f.a. $x \in \{0,1\}^*$ wie folgt definiert:

$$L(x) := \begin{cases} 0 & \text{falls } x \notin L \\ 1 & \text{falls } x \in L. \end{cases}$$

Definition 7.13 (BPTIME(T(n)), BPP)

(a) Sei $T: \mathbb{N} \to \mathbb{N}$ und sei $L \subseteq \{0,1\}^*$.

Eine PTM M entscheidet L in Zeit T(n), falls M T(n)-zeitbeschränkt ist und f.a. $x \in \{0,1\}^*$ gilt:

$$Pr[M(x) = L(x)] \geq 2/3.$$

D.h.: Falls $x \in L$, so ist $Pr[M(x)=1] \geq 2/3$;
Falls $x \notin L$, so ist $Pr[M(x)=0] \geq 2/3$.

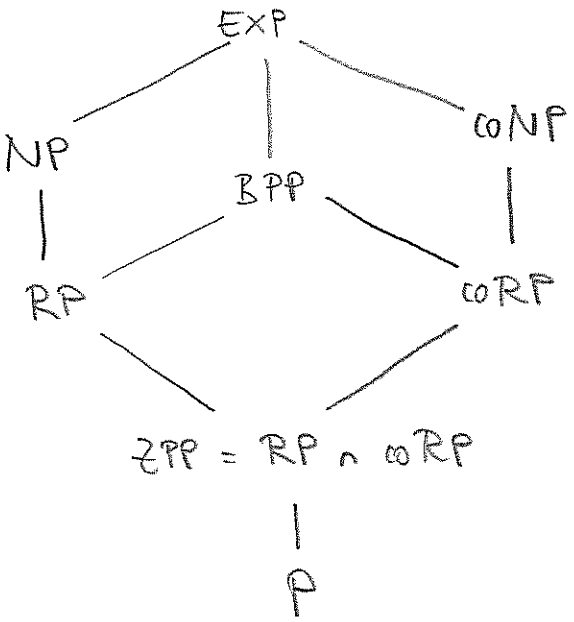
(b) Sei $T: \mathbb{N} \to \mathbb{N}$.
Die Klasse $BPTIME(T(n))$ besteht aus allen Sprachen $L \subseteq \{0,1\}^*$, die von einer $O(T(n))$-zeitbeschränkten PTM entschieden werden.

(c) $$BPP := \bigcup_{c \geq 1} BPTIME(n^c)$$

("bounded-error probabilistic polynomial time")

Bemerkung 7.14

Aus den Definitionen der Komplexitätsklassen sowie Theorem 7.11 und Bem 7.16 ergibt sich folgende Inklusionsstruktur der einzelnen Klassen:



Offene Forschungsfrage: Ist $BPP = P$?

Vermutung: Ja (!) ... und es gibt Resultate, die diese Vermutung sehr plausibel erscheinen lassen; siehe Kapitel 19 und 20 in [AB].

Ähnlich wie NP lässt sich BPP auch durch deterministische TMen mit "Zusatzeingabe" charakterisieren

Satz 7.15

Sei $L \subseteq \{0,1\}^*$. Es gilt:

$L \in BPP \iff$ Es gibt eine polynomiell zeitbeschränkte deterministische TM M und ein Polynom $p: \mathbb{N} \to \mathbb{N}$, s.d. f.a. $x \in \{0,1\}^*$ gilt:

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

Dabei ist für $i \in \{0,1\}$

$$\Pr_{r \in \{0,1\}^{p(|x|)}} \left[M(x,r) = i \right] := \frac{|\{ r \in \{0,1\}^{p(|x|)} : M(x,r) = i \}|}{2^{p(|x|)}} .$$

Beweis: Übung!

Bemerkung 7.16

Aus Satz 7.15 folgt direkt, dass $BPP \subseteq EXP$ ist.

Lemma 7.17 (Wahrscheinlichkeitsverstärkung für BPP)

Sei $L \subseteq \{0,1\}^*$, sei p ein Polynom > 1 und sei M eine polynomiell zeitbeschränkte PTM, s.d. f.a. $x \in \{0,1\}^*$ gilt

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

Dann gibt es für jedes Polynom q eine polynomiell zeitbeschränkte PTM M', s.d. f.a. $x \in \{0,1\}^*$ gilt:

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

Beweis:

Bei Eingabe $x \in \{0,1\}^*$ geht M' wie folgt vor:

1) Berechne $k := 2 \cdot \ln 2 \cdot q(|x|) \cdot p(|x|)^2$
2) Starte unabhängig voneinander k Läufe von M bei Eingabe x;
   seien $y_1, \ldots, y_k \in \{0,1\}$ die Ausgaben dieser k Läufe
3) Falls die Mehrheit der $y_1, \ldots, y_k$ gleich 1 ist, gib 1 aus; ansonsten gib 0 aus.

Offensichtlicherweise ist M' eine polynomiell zeitbeschränkte PTM.

Sei $n := |x|$. Um $(*)$ nachzuweisen, reicht es, zu zeigen, dass gilt:

$$Pr[M'(x) \neq L(x)] \leq 2^{-q(n)} = e^{-\ln 2 \cdot q(n)} \quad (**)$$

Dazu sei f.a. $i \in \{1,\dots,k\}$ X_i eine Zufallsvariable mit

$s := Pr[X_i = 1] = Pr[M(x) = L(x)] \geq \frac{1}{2} + \frac{1}{p(n)}$ und

$1 - s = Pr[X_i = 0]$.

Sei $X := \sum_{i=1}^{k} X_i$. D.h.: X gibt an, wie viele der k Aufrufe von M bei Eingabe x das korrekte Ergebnis liefern.

Außerdem gilt:

$M'(x) \neq L(x) \Leftrightarrow$ M' gibt bei Eingabe x das falsch Ergebnis aus

$\Leftrightarrow$ weniger als $k/2$ der Aufrufe von M bei Eingabe x liefern das korrekte Ergebnis

$\Leftrightarrow X < k/2$

Um $Pr[M'(x) \neq L(x)] = Pr[X < k/2]$ abzuschätzen, nützen wir das folgende aus der Stochastik bekannte Lemma:

<u>Lemma 7.18</u> (Chernoff-Schranke)

Sei $k > 0$, seien $X_1, \dots, X_k$ unabhängige Zufallsvariablen, sei s mit $0 < s < 1$ s.d. f.a. $i \in \{1,\dots,k\}$ gilt: $Pr[X_i = 1] = s$ und $Pr[X_i = 0] = 1 - s$.

Sei $X := \sum_{i=1}^{k} X_i$. Dann gilt:

(a) $E[X] = k \cdot s$ und

(b) F.a. δ mit $0 < \delta \leq 1$ ist

$$Pr[X < (1-\delta) \cdot E[X]] < e^{-\frac{\delta^2}{2} \cdot E[X]}$$

(Hier ohne Beweis)

Um die Chernoff-Schranke anzuwenden, wählen wir δ so, dass $(1-\delta)\cdot E[X] = \frac{k}{2}$ ist

Dh: $\frac{k}{2} = (1-\delta)\cdot k\cdot s$

$\Leftrightarrow \quad \frac{1}{2} = (1-\delta)\cdot s = s - \delta s$

$\Leftrightarrow \quad \delta s = s - \frac{1}{2}$

$\Leftrightarrow \quad \delta = 1 - \frac{1}{2s}$.

Beachte: Wegen $s>0$ ist $\delta<1$; wegen $s>\frac{1}{2}$ ist $\delta>0$

Daher können wir die Chernoff-Schranke anwenden und erhalten:

$$\Pr\left[X < \frac{k}{2}\right] = \Pr\left[X < (1-\delta)\cdot E[X]\right]$$

$$< e^{-\frac{\delta^2}{2}\cdot E[X]} = e^{-\delta^2/2 \cdot k\cdot s}$$

Um (**) nachzuweisen, müssen wir zeigen, dass

$$-\frac{\delta^2}{2}\cdot k\cdot s \leq -\ln 2 \cdot q(n).$$

D.h. es bleibt zu zeigen, dass

$$k \geq 2\cdot \ln 2 \cdot q(n)\cdot \frac{1}{s\cdot\delta^2} \quad \text{ist}$$

Wegen $k = 2\ln 2 \cdot q(n)\cdot p(n)^2$ müssen wir also nur noch zeigen, dass $p(n)^2 \geq \frac{1}{s\cdot\delta^2}$ ist

Somit bleibt zu zeigen: $s\cdot\delta^2 \geq \left(\frac{1}{p(n)}\right)^2$

Dazu sei ε s.d. $s = \frac{1}{2} + \varepsilon$.

Wegen $\frac{1}{2} + \frac{1}{p(n)} \leq s \leq 1$ gilt: $\frac{1}{p(n)} \leq \varepsilon \leq \frac{1}{2}$.

Wegen $\delta = 1 - \frac{1}{2s}$ gilt:

$$s \cdot \delta^2 = s\left(1 - \frac{1}{2s}\right)^2 = s \cdot \left(1 - \frac{1}{s} + \frac{1}{4s^2}\right) = s - 1 + \frac{1}{4s}$$

$$= \frac{1}{2} + \varepsilon - 1 + \frac{1}{4(\frac{1}{2} + \varepsilon)} = \varepsilon - \frac{1}{2} + \frac{1}{2 + 4\varepsilon}$$

$$= \frac{2\varepsilon + 4\varepsilon^2 - 1 - 2\varepsilon + 1}{2 + 4\varepsilon} = \frac{4\varepsilon^2}{2 + 4\varepsilon}$$

$$\geq \frac{4\varepsilon^2}{4} = \varepsilon^2 \geq \left(\frac{1}{p(n)}\right)^2.$$

$\uparrow$ $2 + 4\varepsilon \leq 4$, da $\varepsilon \leq \frac{1}{2}$

Insgesamt haben wir damit gezeigt, dass

$$Pr[M'(x) \neq L(x)] = Pr\left[X < \frac{k}{2}\right] < e^{-\ln 2 \cdot q(n)} = \frac{1}{2^{q(n)}}.$$

Daher gilt

$$Pr[M'(x) = L(x)] \geq 1 - \frac{1}{2^{q(n)}}. \qquad \square$$

7.3 Derandomisierung: BPP vs P/poly und PH

Theorem 7.19 (Adelman, 1978)

$BPP \subseteq P/poly$

Beweis:

Sei $L \in BPP$.

Gemäß Satz 7.15 und dem Wahrscheinlichkeitsverstärkungs-Lemma 7.17 gibt es eine det. TM M und ein Polynom p, s.d. f.a. $x \in \{0,1\}^*$ gilt:

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

Also:

$$\Pr_{r \in \{0,1\}^{p(|x|)}} \left[M(x,r) \neq L(x) \right] \leq \frac{1}{2^{|x|+1}} \quad (*)$$

Wir nennen eine Zusatzeingabe $r \in \{0,1\}^{p(|x|)}$ schlecht für x, falls $M(x,r) \neq L(x)$ gilt; ansonsten heißt r gut für x.

Wegen (*) gibt es für jedes $n \in \mathbb{N}$ und $x \in \{0,1\}^n$ höchstens $\frac{2^{p(n)}}{2^{n+1}}$ Zusatzeingaben, die schlecht für x sind.

Daher gibt es höchstens

$$\sum_{x \in \{0,1\}^n} \frac{2^{p(n)}}{2^{n+1}} = 2^n \cdot \frac{2^{p(n)}}{2^{n+1}} = \frac{2^{p(n)}}{2}$$

Zusatzeingaben, die für mindestens ein $x \in \{0,1\}^n$ schlecht sind.

Da es insgesamt $2^{p(n)} > \frac{2^{p(n)}}{2}$ Zusatzeingaben gibt, muss es mindestens eine Zusatzeingabe $r_n \in \{0,1\}^{p(n)}$ geben, die für <u>jedes</u> $x \in \{0,1\}^n$ gut ist.

D.h.: F.a. $x \in \{0,1\}^n$ ist $M(x, r_n) = L(x)$.

Gemäß Theorem 6.20 $\left(P/poly = \bigcup_{c,d \geq 1} DTIME(n^c)/n^d\right)$

folgt somit: $L \in P/poly$.

□

<u>Bemerkung 7.20</u>

Wegen $BPP \subseteq P/poly$ und

Theorem 6.16 (Falls $NP \subseteq P/poly$, so kollabiert die PH)

ist vermutlich $BPP \neq NP$.

Außerdem gilt: Falls $SAT \in BPP$, so kollabiert die PH

Exkurs Begriffe aus der Wahrscheinlichkeitsrechnung

Sei U eine endliche Menge.

(a) Eine Wahrscheinlichkeitsverteilung über U ist eine Funktion $\pi : U \to [0,1]$, so dass gilt:

$$\sum_{u \in U} \pi(u) = 1.$$

(b) Die Elemente von U heißen Elementarereignisse.
Teilmengen von U heißen Ereignisse.
Die Wahrscheinlichkeit eines Ereignisses $V \subseteq U$ ist

$$\Pr[V] := \sum_{u \in V} \pi(u)$$

(c) Eine Zufallsvariable über U ist eine Funktion

$X : U \to \mathbb{R}$.

Der Erwartungswert von X ist

$$E[X] := \sum_{u \in U} \pi(u) \cdot X(u).$$

Die Variant von X ist

$$\mathrm{Var}[X] := E\left[X^2 - E[X]^2 \right]$$