Theorem 7.21 (Satz von Sipser und Gacs, 1983)

$$BPP \subseteq \Sigma_2^P \cap \Pi_2^P$$

Beweis: (Lautemann-Methode)

Wegen $BPP = co\,BPP$ (gemäß der Definition von BPP) genügt es zu zeigen, dass $BPP \subseteq \Sigma_2^P$ ist.

Sei $L \in BPP$.

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

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

D.h.: F.a. $n \in \mathbb{N}$ und f.a. $x \in \{0,1\}^n$ gilt:

- Falls $x \in L$, so $\dfrac{|\{r \in \{0,1\}^{p(n)} : M(x,r) = 1\}|}{2^{p(n)}} \geq 1 - \frac{1}{2^n}$
- Falls $x \notin L$, so $\dfrac{|\{r \in \{0,1\}^{p(n)} : M(x,r) = 1\}|}{2^{p(n)}} \leq \frac{1}{2^n}$.

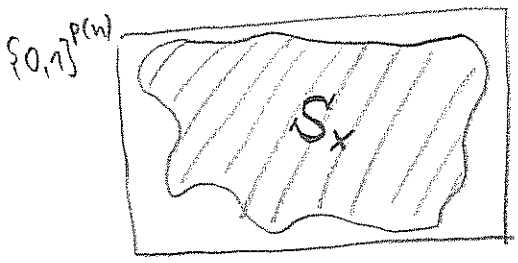
Sei $S_x := \{r \in \{0,1\}^{p(n)} : M(x,r) = 1\}$. Somit gilt:

- Falls $x \in L$, so $|S_x| \geq (1 - \frac{1}{2^n}) \cdot 2^{p(n)}$
- Falls $x \notin L$, so $|S_x| \leq \frac{1}{2^n} \cdot 2^{p(n)}$

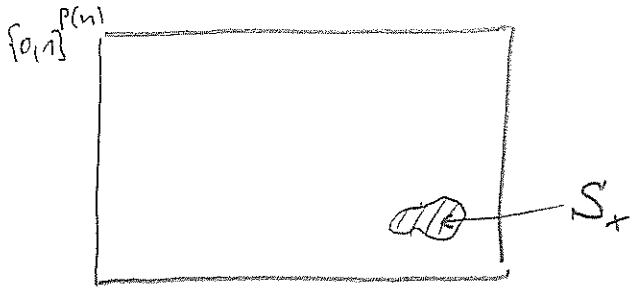
} (*)

Skizze:

$x \in L \Rightarrow$



$x \notin L \Rightarrow$



Notation:

Für $u, v \in \{0,1\}^{p(n)}$ sei

$u+v := (u_1+v_1 \bmod 2,\ u_2+v_2 \bmod 2,\ \dots,\ u_{p(n)}+v_{p(n)} \bmod 2)$

Für $u \in \{0,1\}^{p(n)}$ und $S \subseteq \{0,1\}^{p(n)}$ sei

$S+u := \{ v+u : v \in S \}$ die "Verschiebung" von S um u.

Beachte: $u+v = u-v$ und $S+u = S-u$.

Sei $k(n) := \left\lceil \frac{p(n)}{n} + 1 \right\rceil$

Behauptung 1: F.a. hinreichend großen $n \in \mathbb{N}$ gilt:

Für jedes $S \subseteq \{0,1\}^{p(n)}$ mit $|S| \leq \frac{2^{p(n)}}{2^n}$ und

für alle $u^{(1)}, \dots, u^{(k(n))} \in \{0,1\}^{p(n)}$ gilt:

$$\bigcup_{i=1}^{k(n)} (S+u^{(i)}) \neq \{0,1\}^{p(n)}$$

Beweis:

$$\left| \bigcup_{i=1}^{k(n)} (S+u^{(i)}) \right| \leq \sum_{i=1}^{k(n)} |S+u^{(i)}| = k(n) \cdot |S| \leq \left\lceil \frac{p(n)}{n} + 1 \right\rceil \cdot \frac{2^{p(n)}}{2^n}$$

$$< 2^{p(n)} = |\{0,1\}^{p(n)}|.$$

↑ für hinreichend großes n.

□ Beh 1.

Behauptung 2: Für jedes $n \geq 1$ gilt:

Für jedes $S \subseteq \{0,1\}^{p(n)}$ mit $|S| \geq \left(1 - \frac{1}{2^n}\right) \cdot 2^{p(n)}$

gibt es $u^{(1)}, \ldots, u^{(k(n))} \in \{0,1\}^{p(n)}$, so dass

$$\bigcup_{i=1}^{k(n)} \left(S + u^{(i)}\right) = \{0,1\}^{p(n)}$$

Bevor wir Behauptung 2 beweisen, zeigen wir zunächst, wie man aus $\circledast$, Beh 1 und Beh 2 erhält, dass $L \in \Sigma_2^P$ ist:

Für jedes hinreichend große n und jedes $x \in \{0,1\}^n$ gilt gemäß $\circledast$, Beh 1 und Beh 2:

$$x \in L$$

$$\Leftrightarrow \exists u^{(1)}, \ldots, u^{(k(n))} \in \{0,1\}^{p(n)} : \forall r \in \{0,1\}^{p(n)} : r \in \bigcup_{i=1}^{k(n)} \left(S_x + u^{(i)}\right)$$

$$\Leftrightarrow \bigvee_{i=1}^{k(n)} \left(r + u^{(i)} \in S_x\right)$$

$$\Leftrightarrow \exists u^{(1)}, \ldots, u^{(k(n))} \in \{0,1\}^{p(n)} : \forall r \in \{0,1\}^{p(n)} : \bigvee_{i=1}^{k(n)} M(\langle x, r + u^{(i)} \rangle) = 1$$

Wegen $k(n) = \text{poly}(n)$ kann dies bei gegebenem $x, u^{(1)}, \ldots, u^{(k(n))}$ von einer det. Polynomialzeit-TM überprüft werden.

Insgesamt erhalten wir, dass $L \in \Sigma_2^P$ ist.

Zum Abschluss des Beweises von Theorem 7.21 genügt es also, Behauptung 2 zu beweisen.

Beweis von Behauptung 2:

Wir nutzen die sog. probabilistische Methode:

Wähle $u^{(1)}, \dots, u^{k(n)}$ zufällig und unabhängig voneinander aus $\{0,1\}^{p(n)}$.

Für $i \in \{1, \dots, k(n)\}$ und $r \in \{0,1\}^{p(n)}$ sei

- $B_{i,r}$ das Ereignis, dass $r \notin S + u^{(i)}$ (dh: $r + u^{(i)} \notin S$)
- B_r das Ereignis, dass $r \notin \bigcup_{i=1}^{k(n)} (S + u^{(i)})$

D.h.: - $B_r \iff B_{1,r}$ und $B_{2,r}$ und ... und $B_{k(n),r}$ und
- $\bigcup_{i=1}^{k(n)} (S + u^{(i)}) \neq \{0,1\}^{p(n)} \iff$ ex $r \in \{0,1\}^{p(n)}$ s.d. das Ereignis B_r eintritt

Da die $u^{(i)}$ unabhängig voneinander gewählt werden, gilt

$$\Pr[B_r] = \prod_{i=1}^{k(n)} \Pr[B_{i,r}]$$

Ereignis $B_{i,r}$ tritt genau dann ein, wenn $r + u^{(i)} \notin S$.
Da $u^{(i)}$ zufällig gewählt wird gilt:

$$\Pr[B_{i,r}] = \frac{|\{0,1\}^{p(n)} \setminus S|}{|\{0,1\}^{p(n)}|}$$

Wegen $|S| \geq (1 - \frac{1}{2^n}) \cdot 2^{p(n)}$ ist $|\{0,1\}^{p(n)} \setminus S| \leq \frac{1}{2^n} \cdot 2^{p(n)}$.

Somit ist $\Pr[B_{i,r}] \leq \frac{\frac{1}{2^n} \cdot 2^{p(n)}}{2^{p(n)}} = \frac{1}{2^n}$

und $\Pr[B_r] = \prod_{i=1}^{k(n)} \Pr[B_{i,r}] \leq \left(\frac{1}{2^n}\right)^{k(n)} = \frac{1}{2^{n \cdot k(n)}}$

Wegen $k(n) = \left\lceil \frac{p(n)}{n} + 1 \right\rceil$ ist $n \cdot k(n) \geq p(n) + n > p(n)$

Somit ist $\Pr[B_r] < \frac{1}{2^{p(n)}}$ und

$$\Pr\left[\begin{array}{l}\text{ex. } r \in \{0,1\}^{p(n)} \text{ s.d.} \\ \text{das Ereignis } B_r \text{ eintritt}\end{array}\right] \leq \sum_{r \in \{0,1\}^{p(n)}} \Pr[B_r] < 2^{p(n)} \cdot \frac{1}{2^{p(n)}} = 1$$

$$\Pr\left[\bigcup_{i=1}^{k(n)} (S + u^{(i)}) \neq \{0,1\}^{p(n)}\right]$$

Wir haben also folgendes gezeigt:
Wenn wir $u^{(1)}, \ldots, u^{(k(n))}$ zufällig aus $\{0,1\}^{p(n)}$ wählen,
so ist die Wahrscheinlichkeit, dass $\bigcup_{i=1}^{k(n)} (S + u^{(i)}) \neq \{0,1\}^{p(n)}$
ist, <u>echt</u> kleiner als 1.

Somit muss es eine Möglichkeit geben, $u^{(1)}, \ldots, u^{(k(n))}$
zu wählen, so dass $\bigcup_{i=1}^{k(n)} (S + u^{(i)}) = \{0,1\}^{p(n)}$ ist

□ Beh 2

Dies schließt den Beweis von Theorem 7.21 ab.

□

Wegen $BPP \subseteq \Sigma_2^P$ folgt insbesondere:
Falls $P = NP$ ist, so ist $PH = P$ und $BPP = P$.

7.4 Vollständige Probleme bzw Hierarchiesätze für BPP?

Es sind keine vollständigen Probleme für BPP bekannt.

Ein naheliegender Versuch, ein vollständiges Problem zu definieren ist, die Sprache

$$L' := \{ \langle M, x, 1^t \rangle : M \text{ ist eine PTM, die bei Eingabe } x \text{ nach } t \text{ Berechnungsschritten mit Wahrscheinlichkeit} \geq 2/3 \text{ den Wert } 1 \text{ ausgibt} \}$$

Man sieht leicht, dass L' BPP-hart ist bzgl. Polynomialzeitreduktionen – dh f.a. $L \in BPP$ ist $L \leq_p L'$.

Aber es ist unklar, ob $L' \in BPP$ ist. Denn: Für $\langle M, x, 1^t \rangle \notin L'$ könnte es z.B. sein, dass $Pr[M(x) = 0] = \frac{1}{2} < \frac{2}{3}$ ist – und somit wäre M keine im Sinne von BPP geeignete PTM.

In der Tat liegt L' vermutlich nicht in BPP, da bekannt ist, dass L' vollständig ist für eine Komplexitätsklasse, die vermutlich deutlich größer als BPP ist.

Andererseits: Falls die Vermutung "BPP = P" tatsächlich wahr ist, so besitzt BPP natürlich vollständige Probleme.

Es sind keine Zeithierarchiesätze für BPP bekannt. So ist z.B. unklar, ob

- $BPTIME(n) \neq BPTIME(n^2)$ oder ob
- $BPTIME(n) \neq BPTIME(n^{((\log n)^{10})})$

ist.

Die in Kapitel 3 betrachteten Diagonalisierungsmethoden funktionieren hier nicht, da wir für eine gegebene PTM M nicht entscheiden können, ob f.a. Eingaben $x \in \{0,1\}^*$ gilt:

entweder $Pr[M(x)=1] \geq 2/3$ oder $Pr[M(x)=1] \leq 1/3$.

7.5 Randomisierte Platzbeschränkte Berechnungen

Ähnlich wie BPP und RP randomisierte Varianten von P sind, können wir randomisierte Varianten der Klasse L aller auf logarithmischem Platz berechenbaren Probleme definieren:

Definition 7.22 (BPL und RL)

(a) Die Klasse BPL besteht aus allen Sprachen $L \subseteq \{0,1\}^*$, für die es eine $O(\log n)$-platzbeschränkte PTM M gibt, s.d. f.a. $x \in \{0,1\}^*$ gilt:

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

(b) Die Klasse RL besteht aus allen Sprachen $L \subseteq \{0,1\}^*$, für die es eine $O(\log n)$-platzbeschränkte PTM M gibt, s.d. f.a. $x \in \{0,1\}^*$ gilt:

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

Bemerkung 7.23

(a) Die Wahrscheinlichkeitsverstärkungs-Lemmata 7.7 und 7.17 gelten analog auch für RL und BPL:

Man kann sich leicht davon überzeugen, dass die im Beweis von Lemma 7.7 und 7.17 konstruierten PTMen M' nur logarithmisch mehr Platz benutzen als die gegebenen PTMen M

(b) Offensichtlich gilt: $L \subseteq RL \subseteq NL \subseteq P$

(c) Man kann zeigen, dass $BPL \subseteq P$ gilt (Übung!)

Theorem 7.24

$UPATH \in RL$, wobei

$UPATH := \{ \langle G, s, t \rangle :$ G ist ein endlicher ungerichteter Graph, in dem es einen Weg von Knoten s zu Knoten t gibt $\}$

Beweisidee:

Konstruiere eine PTM M, die bei Eingabe von $\langle G, s, t \rangle$ folgenden randomisierten Algorithmus ausführt:

Random Walk on $\langle G, s, t \rangle$

$n := |V(G)|$

$i := 0$

$u := s$

while $u \neq t$ and $i < 100 \cdot n^4$ do

sei v ein zufällig gewählter Nachbarknoten von u (d.h. $\{u, v\} \in E(G)$).

$i := i + 1$

$u := v$

Falls $u = t$, so STOPP mit Ausgabe "1"
Sonst STOPP mit Ausgabe "0".

Dieser Algorithmus lässt sich leicht durch eine $O(\log n)$-platzbeschränkte PTM M realisieren.

Falls t von s aus nicht erreichbar ist, so gilt offensichtlicherweise $Pr[M(\langle G, s, t \rangle) = 0] = 1$.

Unter Verwendung der Theorie der Markov-ketten kann man folgendes beweisen (hier ohne Beweis):

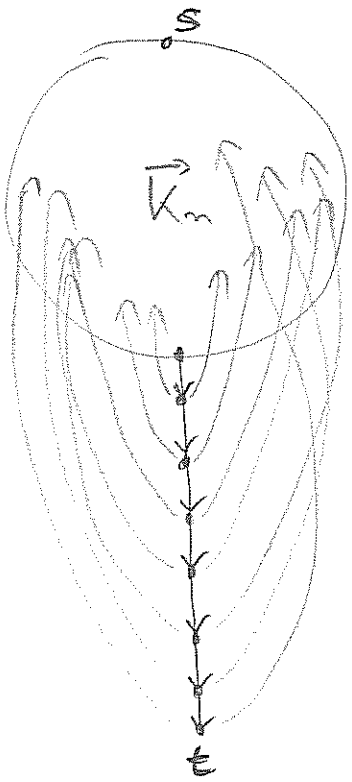
Falls t von s aus erreichbar ist, so ist die erwartete Anzahl von Schritten im "random walk"

bis Knoten t erreicht ist $\leq 10n^4$, und daher ist die Wahrscheinlichkeit, dass t innerhalb von $100 \cdot n^4$ Schritten erreicht wird, $\geq 2/3$.

□

Bemerkung 7.25

Auf gerichteten Graphen funktioniert die Random-Walk-Methode nicht so gut. Betrachtet man z.B. einen Graphen der Form,



($\vec{K}_n$: gerichteter vollständiger Graph auf n Knoten mit Kantenmenge $V \times V$)

so kann man nachweisen, dass ein in s startender Random Walk Erwartungswert deutlich mehr als $10n^4$ Schritte braucht, um Knoten t zu erreichen.