6. Probabilism

6.1 Probabilistic Turing machines

Model of PTM:

- like nondeterministic Turing machine but only one comp. path is followed
- toss a fair coin for each nondeterministic branch
- $\text{prob}(r) =_{\text{def}} \left(\frac{1}{2}\right)^{\text{number of branches on } r}$

A probabilistic Turing machine M:

- accepts x with probability

$$\text{prob}_M(x) =_{\text{def}} \sum_{\substack{r \text{ is accept.} \\ \text{path of } M(x)}} \text{prob}(r)$$

- accepts language $L(M) =_{\text{def}} \{x \mid \text{prob}_M(x) > \frac{1}{2}\}$
- accepts $L(M)$ with bounded error-prob. iff

$$x \in L(M) \Rightarrow \text{prob}_M(x) \geq \frac{2}{3}$$

$$x \notin L(M) \Rightarrow \text{prob}_M(x) \leq \frac{1}{3}$$

- accepts $L(M)$ in time $t: \mathbb{N} \to \mathbb{N}$ iff all comp. paths of M on x have length $\leq t(|x|)$
- accepts $L(M)$ in space $s: \mathbb{N} \to \mathbb{N}$ iff all conf. on each comp. path of M on x have size $\leq s(|x|)$.

Complexity classes given type τ:

τ-PTIME(t) $=_{def}$ $\{ L(M) \mid M$ is τ-PTM accept. $L(M)$ in time $t \}$

τ-BPTIME(t) $=_{def}$ $\{ L(M) \mid M$ is τ-PTM accept. $L(M)$ w. bounded error-prob. in time $t \}$

τ-PSPACE(s) $=_{def}$ $\{ L(M) \mid M$ is τ-PTM accept. $L(M)$ in space $s \}$

τ-BPSPACE(s) $=_{def}$ $\{ L(M) \mid M$ is τ-PTM accept. $L(M)$ w. bounded error-prob. in space $s \}$

type-independent complexity classes:

PTIME$(Pol\, t)$, BPTIME$(Pol\, t)$, PSPACE(s), BPSPACE(s)

Special classes:

PP $=_{def}$ PTIME$(Pol\, n)$

BPP $=_{def}$ BPTIME$(Pol\, n)$

PL $=_{def}$ PSPACE$(\log n)$

BPL $=_{def}$ BPSPACE$(\log n)$

Proposition 1.

Let $t(n) \geq n$, $s(n) \geq 0$.

(1.) τ-DTIME$(t) \subseteq \tau$-BPTIME$(t) \subseteq \tau$-PTIME(t)

(2.) DTIME$(Pol\, t) \subseteq$ BPTIME$(Pol\, t) \subseteq$ PTIME$(Pol\, t)$

(3.) DSPACE$(s) \subseteq$ BPSPACE$(s) \subseteq$ PSPACE(s)

Corollary 2.

(1) $P \subseteq BPP \subseteq PP$

(2) $L \subseteq BPL \subseteq PL$

Theorem 3.

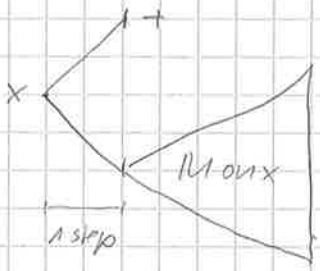
(1.) $\text{multiT-NTIME}(t) \subseteq \text{multiT-PTIME}(1+t)$ for $t(n) \geq n$

(2.) $NTIME(Pol\ t) \subseteq PTIME(Pol\ t)$ for $t(n) \geq n$.

(3.) $NSPACE(s) \subseteq PSPACE(s)$ for $s(n) \geq 0$.

Proof: (2) follows from (1).

(1.), (3.): Let M be an NTM. Consider PTM M' that on input x works as follows:



$x \in L \Rightarrow M$ accepts x

$\Rightarrow prob_M(x) > 0$

$\Rightarrow prob_{M'}(x) = \frac{1}{2} + \frac{1}{2} prob_M(x) > 0$

$x \notin L \Rightarrow M$ rejects x

$\Rightarrow prob_M(x) = 0$

$\Rightarrow prob_{M'}(x) = \frac{1}{2}$ ∎

Corollary 4.

(1.) $NP \subseteq PP$.

(2.) $NL \subseteq PL$.

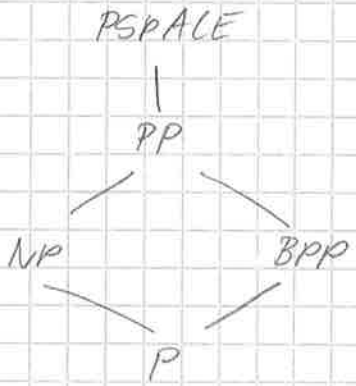
Theorem 5.

Let $s(n) \geq \log n$ be space-constructible.

(1.) $PSPACE(s) \subseteq DSPACE(s^2)$

(2.) $PSPACE(Pol\,s) = BPSPACE(Pol\,s) = DSPACE(Pol\,s)$.

Diagram:



6.2 The class BPP

Theorem 7. (Amplification)

For any language L, the following are equivalent:

(1.) $L \in BPP$.

(2) There ex. a PPTM M and $0 < \varepsilon < \frac{1}{2}$ s.t. for all $x \in \Sigma^*$.

$$x \in L \Rightarrow prob_M(x) \geq 1-\varepsilon$$

$$x \notin L \Rightarrow prob_M(x) \leq \varepsilon$$

(3.) For each polynomial p, there ex. a PPTM M s.t. for all $x \in \Sigma^*$.

$$x \in L \Rightarrow prob_M(x) \geq 1 - \frac{1}{2^{p(|x|)}}$$

$$x \notin L \Rightarrow prob_M(x) \leq \frac{1}{2^{p(|x|)}}$$

Proof: (3) $\Rightarrow$ (1) $\Rightarrow$ (2) is trivial.

(2) $\Rightarrow$ (3): Let M, ε be given as described in (2). Let p be a polynomial. Since $0 < \varepsilon < \frac{1}{2}$, we have $4\varepsilon(1-\varepsilon) < 1$. Choose k so that $(4\varepsilon(1-\varepsilon))^k \leq \frac{1}{2}$.

Define M' to be that PPTM that, on input x, sequentially simulates M on x exactly $2m$-times ($m =_{df} k \cdot p(|x|)$), and accepts x iff at least m simulations were accepting.

It holds that:

$$prob_{M'}(x) = \sum_{i=m}^{2m} prob(M \text{ accepts } x \text{ ex. } i\text{-times})$$

$$= \sum_{i=m}^{2m} \binom{2m}{i} prob(M \text{ accepts } x \text{ for ex. chosen simulations})$$

$$= \sum_{i=m}^{2m} \binom{2m}{i} \alpha^i (1-\alpha)^{2m-i}, \quad \alpha = prob_M(x).$$

We examine acc./rej. probabilities of M':

$$x \notin L \Rightarrow 0 \le \alpha \le \varepsilon < \frac{1}{2} < 1-\varepsilon \le 1-\alpha \le 1,$$

so:

$$prob_{M'}(x) = \sum_{i=m}^{2m} \binom{2m}{i} \alpha^i (1-\alpha)^{2m-i}$$

$$= \sum_{i=m}^{2m} \binom{2m}{i} (\alpha(1-\alpha))^m \underbrace{\alpha^{i-m} (1-\alpha)^{-(i-m)}}$$

$$= \left(\frac{\alpha}{1-\alpha}\right)^{i-m} \le 1$$

$$\le \sum_{i=m}^{2m} \binom{2m}{i} (\alpha(1-\alpha))^m$$

$$\le (\alpha(1-\alpha))^m \sum_{i=0}^{2m} \binom{2m}{i}$$

$$\le (\alpha(1-\alpha))^m 2^{2m} = (4\alpha(1-\alpha))^m$$

$$\le (4\varepsilon(1-\varepsilon))^m = (4\varepsilon(1-\varepsilon))^{k \cdot p(|x|)}$$

$$\le \left(\frac{1}{2}\right)^{p(|x|)}$$

$x \in L \Rightarrow 0 \leq 1-\alpha \leq \varepsilon < \frac{1}{2} < 1-\varepsilon \leq \alpha \leq 1$

so:

$$1 - \text{prob}_m(x) = \sum_{i=0}^{2m} \binom{2m}{i} \alpha^i (1-\alpha)^{2m-i} - \sum_{i=m}^{2m} \binom{2m}{i} \alpha^i (1-\alpha)^{2m-i}$$

$$= \sum_{i=0}^{m-1} \binom{2m}{i} \alpha^i (1-\alpha)^{2m-i}$$

$$= \sum_{i=0}^{m-1} \binom{2m}{i} (\alpha(1-\alpha))^m \underbrace{\left(\frac{1-\alpha}{\alpha}\right)^{m-i}}_{\leq 1}$$

$$\leq \sum_{i=0}^{m-1} \binom{2m}{i} (\alpha(1-\alpha))^m$$

$$\leq (\alpha(1-\alpha))^m \sum_{i=0}^{2m} \binom{2m}{i}$$

$$= (4\alpha(1-\alpha))^m$$

$$\leq (4\varepsilon(1-\varepsilon))^m$$

$$\leq \frac{1}{2^{p(|x|)}}$$

Hence, $\text{prob}_m(x) \geq 1 - \frac{1}{2^{p(|x|)}}$ ∎

Let $B \subseteq \Sigma^* \times \{0,1\}^*$, p polynomial. Define

$$h_{B,p}(x) =_{def} \| \{ z \mid |z| = p(|x|) \wedge (x,z) \in B \} \|$$

It holds that $0 \leq h_{B,p}(x) \leq 2^{p(|x|)}$

Lemma 8.

(1.) For each PPTM M, there exist $B \in P$ and polynomial p such that for all $x \in \Sigma^*$,

$$h_{B,p}(x) = prob_M(x) \cdot 2^{p(|x|)}$$

(2.) For each $B \in P$, polynomial p, there is a PPTM M such that

$$prob_M(x) = \frac{h_{B,p}(x)}{2^{p(|x|)}}$$

Theorem 9.

For any language L, the following are equivalent:

(1) $L \in BPP$

(2.) There ex. $B \in P$, polynomial q, $0 < \varepsilon < \frac{1}{2}$ such that

$$x \in L \Rightarrow h_{B,q}(x) \geq (1-\varepsilon) 2^{q(|x|)}$$

$$x \notin L \Rightarrow h_{B,q}(x) \leq \varepsilon \cdot 2^{q(|x|)}$$

(3.) For each polynomial p, there exist $B \in P$, polynomial q such that

$$x \in L \Rightarrow h_{B,q}(x) \geq \left(1 - \frac{1}{2^{p(|x|)}}\right) 2^{q(|x|)}$$

$$x \notin L \Rightarrow h_{B,q}(x) \leq \frac{1}{2^{p(|x|)}} \cdot 2^{q(|x|)}$$

Theorem 10.

$$BPP^{BPP} = BPP.$$

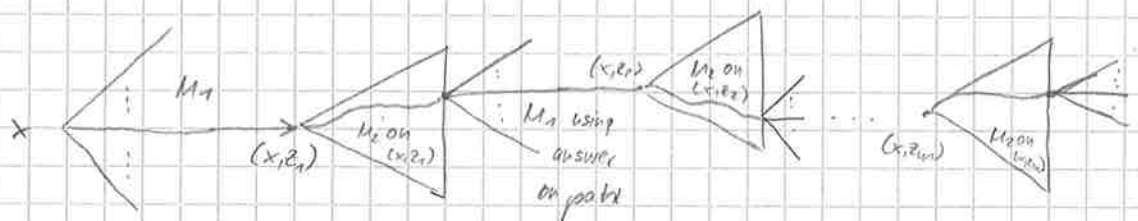
Proof: Let $A \in BPP^B$, $B \in BPP$, $A \subseteq \Sigma^*$, $B' =_{def} \Sigma^* \times B$, i.e., $B' \in BPP$. So, A can be accepted by a PPTM M_1 in time p (polynomial) such that, on input x, only queries "$(x,z) \in B'$?" are asked and it holds that

$$\text{prob}_{r_1}\left[M_1 \text{ acc. } x \text{ w. oracle } B' \Leftrightarrow x \in A\right] \geq \frac{2}{3}$$

Let M_2 be a PPTM such that

$$\text{prob}\left[M_2 \text{ acc. } (x,z) \Leftrightarrow (x,z) \in B'\right] \geq 1 - \frac{1}{2^{|x|}}$$

Define M_3 to be that PPTM that, on input x, works as follows:



We obtain:

$$\begin{aligned}
&\text{prob}\left[M_3 \text{ acc. } x \Leftrightarrow x \in A\right] \\
&\geq \text{prob}\left[M_1 \text{ acc. } x \text{ w. oracle } B' \Leftrightarrow x \in A\right] \\
&\qquad \cdot \text{prob}\left[(\forall\, 1 \leq i \leq m)\left[M_2 \text{ acc. } (x,z_i) \Leftrightarrow (x,z_i) \in B'\right]\right] \\
&\geq \frac{2}{3} \prod_{i=1}^{m} \text{prob}\left[M_2 \text{ acc. } (x,z_i) \Leftrightarrow (x,z_i) \in B'\right] \\
&\geq \frac{2}{3}\left(1 - \frac{1}{2^{|x|}}\right)^m \\
&\geq \frac{2}{3}\left(1 - \frac{m}{2^{|x|}}\right) \qquad \text{(Bernoulli-inequality: } (1+x)^m \geq 1+mx,\ x \geq -1\text{)} \\
&\geq \frac{2}{3}\left(1 - \frac{p(|x|)}{2^{|x|}}\right) \qquad (m \leq p(|x|)) \\
&\geq \frac{3}{5} \qquad \text{for suff. long } x.
\end{aligned}$$

Amplification shows $A \in BPP$.

Corollary 11.

BPP is closed under $\cap, \cup, {}^{-}, \leq_m^p, \leq_T^p$.

Theorem 12. (Lautemann, Sipser 1983)

$$BPP \subseteq \Sigma_2^p \cap \Pi_2^p.$$

Proof: It suffices to show $BPP \subseteq \Sigma_2^p$. Let $L \in BPP$, i.e., there exist $B \in P$, polynomial q such that

(i) $x \in L \Rightarrow n_{B,q}(x) \geq \left(1 - \frac{1}{2^{|x|}}\right) 2^{q(|x|)}$

(ii) $x \notin L \Rightarrow n_{B,q}(x) \leq 2^{q(|x|)} - |x|$

For $z = z_1 z_2 \ldots z_m$, $u = u_1 u_2 \ldots u_m \in \{0,1\}^*$, define

$$z \oplus u =_{df} (z_1 \oplus u_1)(z_2 \oplus u_2) \cdot \ldots \cdot (z_m \oplus u_m)$$

Claim. $x \in L \Leftrightarrow (\exists u^1, \ldots, u^{q(|x|)}) \Big[|u^i| = q(|x|) \wedge (\forall z) \big[|z| = q(|x|) \rightarrow (\exists i \leq q(|x|)) [(x, z \oplus u^i) \in B] \big] \Big]$

(Note: if claim is correct then $L \in \Sigma_2^p$)

Let $m = q(|x|)$

$\Leftarrow$ Suppose there are $u^1, \ldots, u^m$ s.t. $|u^i| = m$ and for all z s.t. $|z| = m$ there is an $i \leq m$ s.t. $(x, z \oplus u^i) \in B$.

We obtain

$$\begin{aligned} 2^m &= \| \{ z \mid |z| = m \} \| \\ &\leq \| \{ (z, u^i) \mid |z| = m \wedge i \in \{1, \ldots, m\} \wedge (x, z \oplus u^i) \in B \} \| \\ &= \sum_{i=1}^{m} \| \{ z \mid |z| = m \wedge (x, z \oplus u^i) \in B \} \| \\ &= \sum_{i=1}^{m} \| \{ z \mid |z| = m \wedge (x, z) \in B \} \| \\ &= q(|x|) \cdot n_{B,q}(x) \end{aligned}$$

Thus, $n_{B,q}(x) \geq \frac{2^{q(|x|)}}{q(|x|)} > \frac{1}{2^{|x|}} 2^{q(|x|)}$

Hence, $x \in L$ (ii)

$\Rightarrow$ (contraposition) Suppose for each $u^1, \dots, u^m$ s.t. $|u^i| = m$, there ex. z s.t. $|z| = m$ and $(x, z \oplus u^i) \notin B$ for all $i \in \{1, \dots, m\}$.

We obtain:

$$
\begin{aligned}
2^{m^2} &= \| \{ (u^1, \dots, u^m) \mid |u^i| = m \} \| \\
&\le \| \{ (u^1, \dots, u^m, z) \mid |u^i| = |z| = m \wedge \bigwedge_{i=1}^{m} [(x, z \oplus u^i) \notin B] \} \| \\
&= \sum_{|z|=m} \| \{ (u^1, \dots, u^m) \mid |u^i| = m \wedge \bigwedge_{i=1}^{m} [(x, z \oplus u^i) \notin B] \} \| \\
&= \sum_{|z|=m} \prod_{j=1}^{m} \| \{ u^j \mid |u^j| = m \wedge (x, z \oplus u^j) \notin B \} \| \\
&= \sum_{|z|=m} \| \{ u \mid |u| = m \wedge (x, z \oplus u) \notin B \} \|^m \\
&= \sum_{|z|=m} \| \{ z \mid |z| = m \wedge (x, z) \notin B \} \|^m \\
&= 2^m \left(2^m - h_{B,q}(x) \right)^m
\end{aligned}
$$

Thus, $2^{q(|x|)^2} \le 2^{q(|x|)} \left(2^{q(|x|)} - h_{B,q}(x) \right)^{q(|x|)}$, i.e.

$2^{q(|x|)} \le 2 \left(2^{q(|x|)} - h_{B,q}(x) \right)$

Thus, $h_{B,q}(x) \le \frac{1}{2} 2^{q(|x|)}$

Hence, $x \notin L$ (i).

Let $\mathcal{C}$ be a class of languages and $\mathcal{F}$ be a class of functions $\mathbb{N} \mapsto \Sigma^*$. Define the class $\mathcal{C}/\mathcal{F}$ as follows:

$A \in \mathcal{C}/\mathcal{F} \Leftrightarrow_{def}$ there ex. $B \in \mathcal{C}$, $h \in \mathcal{F}$ such that
$A = \{ x \mid (x, h(|x|)) \in B \}$

Example: $\mathcal{C} = P$, $\mathcal{F} = poly$: $P/poly$ is the class of languages possessing polynomial-size circuits.

Theorem 13.
$BPP \subseteq P/poly$

Proof: Let $A \in BPP$, i.e., there ex. PPTM M, polynomial p such that for each x,

$$prob[x \in A \Leftrightarrow M \text{ acc. } x] \geq 1 - 2^{-2n},$$

i.e., there are at most $2^{p(|x|)} \cdot 2^{-2n}$ contrad. paths.
Consider all strings x of length n. There are 2^n such strings, i.e., there are at most $\underbrace{2^n \cdot 2^{p(|x|)-2n}}_{= 2^{p(|x|)-n}}$ contr. paths of M in total.
Since $2^{p(|x|)} - 2^{p(|x|)-|x|} > 0$, there ex. a path y, $|y| = p(|x|)$ such that for all x, $|x| = n$:

$x \in A \Leftrightarrow M$ accepts x on path y.

Define $h : n \mapsto y$. Thus,

$x \in A \Leftrightarrow (x, h(x)) \in B$

where $B =_{def} \{ (x, y) \mid M \text{ accepts } x \text{ on path } y \} \in P$.
Hence, $A \in P/poly$. ∎

Remark:
(1.) $NP \subseteq P/poly \Rightarrow \Sigma_2^p = \Pi_2^p$ (Karp-Lipton 82)
(2.) $NP \subseteq BPP \Rightarrow \Sigma_2^p = \Pi_2^p$

6.3 The classes #P and GapP

Define $h_{B,p}(x) =_{df} \|\{z \mid |z| = p(|x|) \wedge (x,z) \in B\}\|$

Let M be an NPTM. Define

$acc_M(x) =_{df}$ number of all accepting paths of M on x

$rej_M(x) =_{df}$ number of all rejecting paths of M on x

Complexity classes of functions:

$$\#P =_{df} \{ acc_M \mid M \text{ is an NPTM} \}$$

$$GapP =_{df} \{ acc_M - rej_M \mid M \text{ is an NPTM} \}$$

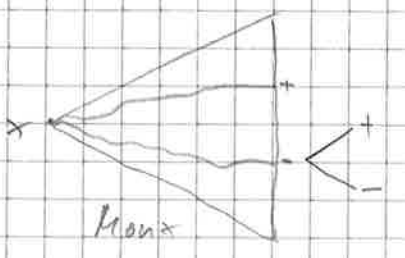
Proposition 14

$$FP \subseteq \#P \subseteq GapP \subseteq FPSPACE.$$

Proof: We show inclusions:

- $FP \subseteq \#P$: Let $f \in FP$, i.e., there ex. polynomial p s.t. $|f(x)| \leq p(|x|)$ or $f(x) \leq 2^{p(|x|)}$ resp. Define M to be that NPTM that on input x,
  (i) branches exactly $p(|x|)$ times on each comp. path, i.e., there are $2^{p(|x|)}$ paths $1, 2, \ldots, 2^{p(|x|)}$,
  (ii) accepts along path τ iff $\tau \in f(x)$

  Clearly, $f \in \#P$.
- $\#P \subseteq GapP$: Let $f \in \#P$ via NPTM M, i.e., $f(x) = acc_M(x)$. Define M' to be that NPTM M' that on input x:



We have:

$$acc_{M'}(x) - rej_{M'}(x)$$
$$= acc_M(x) + rej_M(x) - rej_M(x)$$
$$= f(x)$$

- GapP $\subseteq$ FPSPACE: Let $f \in$ GapP, i.e., there ex. NPTM M s.t. $f(x) = acc_M(x) - rej_M(x)$. A PSPACE TM simulates all paths of M and counts accepting and rejecting paths.

Define operators on functions f, g:

$$(f \circ g)(x) =_{def} f(g(x))$$

$$(f+g)(x) =_{def} f(x) + g(x)$$

$$(f-g)(x) =_{def} f(x) - g(x) \qquad \left((f-g)(x) =_{def} \max\{0, (f-g)(x)\}\right)$$

$$(f \cdot g)(x) =_{def} f(x) \cdot g(x)$$

$$\binom{f}{g}(x) =_{def} \binom{f(x)}{g(x)}$$

$$\left(\sum(f,g)\right)(x) =_{def} \sum_{z=0}^{g(x)} f(z)$$

$$\left(\prod(f,g)\right)(x) =_{def} \prod_{z=0}^{g(x)} f(z)$$

Theorem 15.

Let $g, g' \in FP$ be functions s.t. $g'(x) \leq p(|x|)$ for some polynomial p.

(1.) If $f, f' \in \#P$ then

$$f \circ g,\ f+f',\ f \cdot f',\ \binom{f}{g'},\ \sum(f,g),\ \prod(f,g') \in \#P$$

(2.) If $f, f' \in$ GapP then

$$f \circ g,\ f+f',\ f \cdot f',\ f-f',\ \sum(f,g),\ \prod(f,g') \in \text{GapP}$$

Proof: Δ

Lemma 16.

For any function f, the following are equivalent

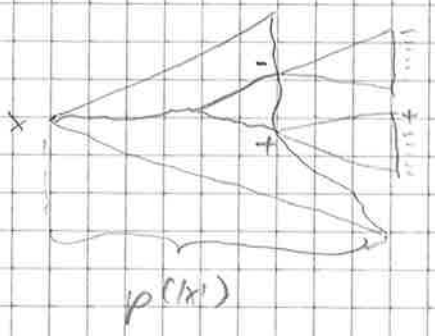
(1.) $f \in \#P$

(2.) There ex. NPTM M, polynomial p such that $f = acc_M$ and all comp. paths of M on x branch exactly $p(|x|)$ times.

(3.) There ex. $B \in P$, polynomial p s.t. $f = h_{B,p}$

Proof:

(1) $\Rightarrow$ (2): Let $f \in \#P$ via NPTM M s.t. $f = acc_M$. Define NPTM M' to work as follows:



- $acc_{M'}(x) = acc_M(x)$
- exactly $p(|x|)$ branches on each path

(2) $\Rightarrow$ (3): Let M, p be as supposed in statement (2). Define

$$B = \{(x,z) \mid |z| = p(|x|) \wedge M \text{ acc. } x \text{ along } z\}$$

Clearly, $B \in P$ and $f = h_{B,p}$.

(3) $\Rightarrow$ (1): Let $f = h_{B,p}$, $B \in P$, p polynomial. Define M to be that NPTM that, on input x, guesses path z, $|z| = p(|x|)$ and acc. along z iff $(x,z) \in B$. Thus, $acc_M(x) = h_{B,p}(x) = f(x)$. ∎

Theorem 17.

$$GapP = \#P - \#P = \#P - FP = FP - \#P.$$

Proof:

- $GapP \subseteq \#P - \#P$: Let $f \in GapP$ via NPTM M s.t. $f(x) = acc_M(x) - rej_M(x)$. Define $\overline{M}$ to be that NPTM that, on input x, accepts along z iff M rejects along z. Hence, $f(x) = acc_M(x) - rej_M(x) = acc_M(x) - acc_{\overline{M}}(x) \in \#P - \#P$. Thus, $f \in \#P - \#P$.
- $\#P - \#P \subseteq \#P - FP$: Let $f \in \#P - \#P$ via NPTM's M, M'. We obtain

$$\begin{aligned} f(x) &= acc_M(x) - acc_{M'}(x) && \text{poly. of Lemma 16.} \\ &= acc_M(x) - (2^{p(|x|)} - rej_{M'}(x)) \\ &= acc_M(x) + rej_{M'}(x) - 2^{p(|x|)} \\ &= \underbrace{acc_M(x) + acc_{\overline{M}}(x)}_{\in \#P} - \underbrace{2^{p(|x|)}}_{\in FP} \end{aligned}$$

- $\#P - FP \subseteq FP - \#P$ Let $f \in \#P - FP$ via NPTM M, $g \in FP$ and polynomial p s.t. $|g(x)| \leq p(|x|)$ and $DTIME_M(x|z) \leq p(|x|)$. We obtain:

$$\begin{aligned} f(x) &= acc_M(x) - g(x) \\ &= (2^{p(|x|)} - rej_M(x)) - g(x) \\ &= \underbrace{(2^{p(|x|)} - g(x))}_{\in FP} - \underbrace{rej_M(x)}_{\in \#P} \end{aligned}$$

- $FP - \#P \subseteq GapP$: Follows from Prop. 14, Theorem 15. ∎

Complete (hardest) functions in #P.

(1) #3SAT(H) = def number of satisfying assignments of 3CNF H

H holds: For each $f \in \#P$ there ex. $g \in FP$ s.t.
$f(x) = \#3SAT(g(x))$ (i.e. $f \leq_m^p \#3SAT$)

(2) Let $A = (a_{ij})_{n \times n}$ be a matrix. Define determinant of A

$$\det(A) =_{def} \sum_{\pi \in S_n} sgn(\pi) \prod_{i=1}^{n} a_{i\pi(i)}$$

Then, $\det \in FP$. Define permanent of A

$$perm(A) =_{def} \sum_{\pi \in S_n} \prod_{i=1}^{n} a_{i\pi(i)}$$

H holds: For $f \in \#P$ there is a PoTM M s.t.
M^{perm} computes f (i.e., $f \in FP^{perm}$).

Thus, $perm \in FP \Rightarrow \#P = FP$ (Valiant 79)

6.4 The class PP

Re-state charact. of NP in terms of #P: The following are equivalent for language L:

(1) $L \in NP$

(2) there ex. $B \in P$, polynomial p s.t. for all $x \in \Sigma^*$

$$x \in L \Leftrightarrow h_{B,p}(x) > 0$$

(3.) there is $f \in \#P$ s.t. for all $x \in \Sigma^*$

$$x \in L \Leftrightarrow f(x) > 0$$

Theorem 18.

The following are equivalent for language L:

(1) $L \in PP$

(2.) there ex. $B \in P$, polynomial p s.t. for all $x \in \Sigma^*$:

$$x \in L \Leftrightarrow h_{B,p}(x) > 2^{p(|x|)-1}$$

(3.) There ex. $f \in \#P$, $g \in FP$ s.t. for all $x \in \Sigma^*$

$$x \in L \Leftrightarrow f(x) > g(x)$$

(4.) There ex. $f \in Gap P$ s.t. for all $x \in \Sigma^*$

$$x \in L \Leftrightarrow f(x) > 0$$

Proof:

(3) $\Leftrightarrow$ (4): Trivial ($Gap P = \#P - FP$)

(2) $\Rightarrow$ (3): Trivial ($h_{B,p} \in \#P$, $x \mapsto 2^{p(|x|)-1} \in FP$)

(1) $\Rightarrow$ (2): Trivial (Lemma 8)

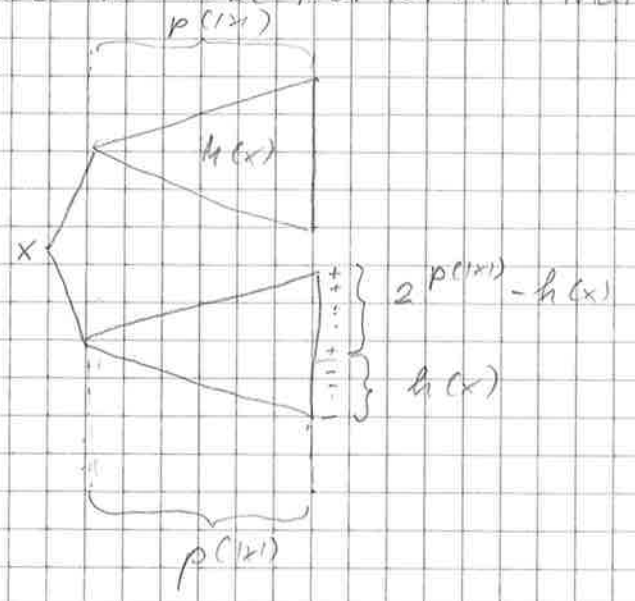
(3) $\Rightarrow$ (1): Let $f \in \#P$ via NPTM M, polynomial p, let $g \in FP$ s.t. $x \in L \Leftrightarrow f(x) > g(x)$. or $x \in L \Leftrightarrow acc_M(x) > g(x)$

Define

$$h(x) =_{def} \min\{g(x), 2^{p(|x|)}\}$$

Thus, $x \in L \Leftrightarrow acc_M(x) > h(x)$.

Define M' to be that NPTM that, on input x, works as follows:



$$acc_{M'}(x) = acc_M(x) + 2^{p(|x|)} - h(x)$$

number of paths: $2^{p(|x|)+1}$

We obtain:

$$\begin{aligned} x \in L &\Leftrightarrow acc_M(x) > h(x) \\ &\Leftrightarrow acc_M(x) + 2^{p(|x|)} - h(x) > 2^{p(|x|)} \\ &\Leftrightarrow acc_{M'}(x) > 2^{p(|x|)} \\ &\Leftrightarrow prob_{M'}(x) > \frac{1}{2} \end{aligned}$$

■

Theorem 19.

$$P^{PP} = P^{\#P} = P^{GapP}$$

Proof:

- $P^{\#P} = P^{GapP}$ $(\#P \subseteq GapP \subseteq \#P - FP)$
- $P^{PP} \subseteq P^{GapP}$: $L \in PP$ if there ex. $f \in GapP$ s.t. $x \in L \Leftrightarrow f(x) > 0$. Use f instead of L as an oracle.
- $P^{\#P} = P^{PP}$: Δ

■

Theorem 20.

PP is closed under $\cap, \cup, \leq_m^p$.

Proof (only $\cap$ [Beigel, Reingold, Spielman 95])

Let $L_1, L_2 \in PP$ via $f_1, f_2 \in GapP$ s.t. $x \in L_1 \Leftrightarrow f_1(x) > 0$,
$x \in L_2 \Leftrightarrow f_2(x) > 0$.

We have to find some $f_3 \in GapP$ s.t.

$$x \in L_1 \cap L_2 \Leftrightarrow f_3(x) > 0$$
$$\Leftrightarrow f_1(x) > 0 \wedge f_2(x) > 0$$

Define

$$R(u,z) =_{def} (u-1) \prod_{i=0}^{z} (u - 2^i)^2$$

$$S(u,z) =_{def} -R(u,z) - R(-u,z)$$

Claim:

(i) $1 \leq u \leq 2^z \rightarrow 0 \leq \frac{R(u,z)}{S(u,z)} < \frac{1}{3}$

(ii) $-2^z < u \leq -1 \Rightarrow \frac{R(u,z)}{S(u,z)} \leq -1$ □

W.l.o.g. $f_1(x) \neq 0$ (otherwise consider $2f_1(x) - 1$)

Let p be a polynomial s.t. $-2^{p(|x|)} < f_1(x) < 2^{p(|x|)}$

We obtain

$$x \in L_1 \cap L_2 \Leftrightarrow f_1(x) > 0 \wedge f_2(x) > 0$$
$$\Leftrightarrow 0 \leq \frac{R(f_1(x), p(|x|))}{S(f_1(x), p(|x|))} < \frac{1}{3} \wedge 0 \leq \frac{R(f_2(x), p(|x|))}{S(f_2(x), p(|x|))} < \frac{1}{3}$$
$$\overset{a),(ii)}{\Leftrightarrow} 0 \leq \frac{R(f_1(x), p(|x|))}{S(f_1(x), p(|x|))} + \frac{R(f_2(x), p(|x|))}{S(f_2(x), p(|x|))}$$

$$\Leftrightarrow 0 < R(f_1, p) S(f_2, p) + R(f_2, p) S(f_1, p) + 1$$

Moreover,

$x \mapsto R(f_i(x), p(|x|)) = (f_i(x)-1) \prod_{j=0}^{p(|x|)} (f_i(x)-2^j)^2$ $\in$ GapP (Theorem 15)

$S(f_i(x), p(|x|)) \in$ GapP.

Define function f_3

$$f_3(x) =_{df} 1 + R(f_1(x), p(|x|)) S(f_2(x), p(|x|)) + R(f_2(x), p(|x|)) \cdot S(f_1(x), p(|x|))$$

Hence, $f_3 \in$ GapP and $x \in L_1 \cap L_2 \Leftrightarrow f_3(x) > 0$. So, $L_1 \cap L_2 \in$ PP. ∎

Remark:

MAJ-SAT $=_{df}$ {# | H is a prop. formula s.t. majority of assignments are satisfying}

6.5 The class $\oplus P$

Definition 21.

$L \in \oplus P \iff$ there ex. $f \in \#P$ s.t. $x \in L \iff f(x) \equiv 1 \ (2)$

Proposition 22

For any language L, the following are equivalent:

(1) $L \in \oplus P$

(2) There ex. $f \in \#P$ s.t. $x \in L \iff f(x) \equiv 0 \ (2)$

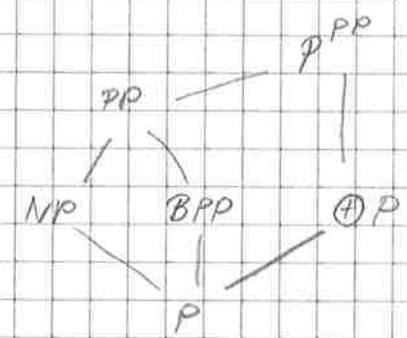
(3.) There ex. $B \in P$, polynomial p s.t. $x \in L \iff h_{B,p}(x) \equiv 1 \ (2)$

(4.) There ex. $B \in P$, poly. p s.t. $x \in L \iff h_{B,p}(x) \equiv 0 \ (2)$ ■

Proposition 23.

$$P \subseteq \oplus P \subseteq P^{PP}$$

Diagram



Theorem 24.

$$\oplus P^{\oplus P} = \oplus P$$

Proof:

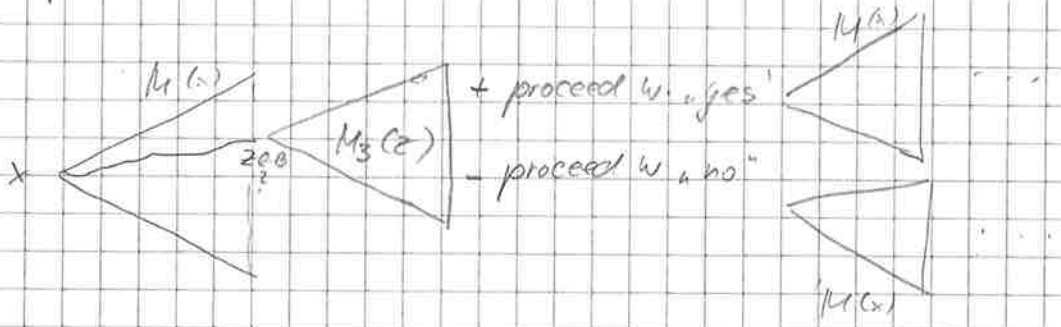
$\supseteq$ Clear.

$\subseteq$ Let $L \in \oplus P^B$ via $B \in \oplus P$. That is, there are NPTM $M_1^{(\cdot)}$, M_2 s.t.

$$x \in L \Leftrightarrow acc_{M_1^B}(x) \equiv 1 (2),$$
$$z \in B \Leftrightarrow acc_{M_2}(z) \equiv 1 (2)$$

Define M_3 to be that NPTM that, on input z, satisfies
$z \in B \Leftrightarrow acc_{M_3}(z) \equiv 1 (2)$, $acc_{M_3}(z) + rej_{M_3}(z) = 2^{p(|z|)} + 1$

Define M_4 to be that NPTM that, on input x, works as follows:



We have to show: $x \in L \Leftrightarrow acc_{M_4}(x) \equiv 1 (2)$.

Case distinction:

(1) $z \in B$: So, $acc_{M_3}(x) \equiv 1 (2)$, $rej_{M_3}(x) \equiv 0 (2)$.
Parity of $acc_{M_4}(x)$ does not depend on behavior along rej. paths, as there is an even number of identical trees, so an even number of acc. paths. Choose some acc. path. There is an even number of further acc. paths, so behavior is for parity not relevant.

(2) $z \notin B$: So, $acc_{M_3}(x) \equiv 0$ (2), $rej_{M_3}(x) \equiv 1$ (2).
Argue like in (1).

We conclude: $acc_{M_4}(x) \equiv acc_{M_1^B}(x)$ (2)

Thus, $x \in L \Leftrightarrow acc_{M_4}(x) \equiv 1$ (2)

Corollary 25.

$\oplus P$ is closed under $\cup, \cap, \overline{\ }, \leq_m^p, \leq_T^p$.

Lemma 26.

For each set $L \in \oplus P$ and each polynomial p, there is a function $f \in \#P$ such that for all $x \in \Sigma^*$,

(i) $x \in L \Leftrightarrow f(x) \equiv 1 \ (2^{p(|x|)})$

(ii) $x \notin L \Leftrightarrow f(x) \equiv 0 \ (2^{p(|x|)})$

Proof: Let $L \in \oplus P$ via $f \in \#P$ s.t. $x \in L \Leftrightarrow f(x) \equiv 1$ (2) and $x \in L \Leftrightarrow f(x) \equiv 0$ (2). Define

$$f_p(x) =_{df} \left((f(x)+1)^{p(|x|)} + 1 \right)^{p(|x|)}$$

Clearly, $f_p \in \#P$.

We use the following facts:

(a) $a \equiv 0 \ (b) \Rightarrow a^k \equiv 0 \ (b^k)$ for each $k \geq 1$, $b \geq 2$.

(b) $a \equiv 1 \ (b) \Rightarrow a^k \equiv 1 \ (b^k)$ for each $k \geq 1$, $b \geq 2$.

We obtain:

$$\begin{aligned}
x \in L &\Rightarrow f(x) \equiv 1 \ (2) \\
&\Rightarrow f(x) + 1 \equiv 0 \ (2) \\
&\overset{(a)}{\Rightarrow} (f(x)+1)^{p(|x|)} \equiv 0 \ (2^{p(|x|)}) \\
&\Rightarrow (f(x)+1)^{p(|x|)} + 1 \equiv 1 \ (2^{p(|x|)}) \\
&\overset{(b)}{\Rightarrow} \left((f(x)+1)^{p(|x|)} + 1 \right)^{p(|x|)} \equiv 1 \ (2^{p(|x|)})
\end{aligned}$$

$$
\begin{aligned}
x \notin L \Rightarrow \quad & f(x) \equiv 0 \quad (2) \\
\Rightarrow \quad & f(x) + 1 \equiv 1 \quad (2) \\
\overset{(6)}{\Rightarrow} \quad & (f(x)+1)^{p(|x|)} \equiv 1 \quad (2) \\
\Rightarrow \quad & (f(x)+1)^{p(|x|)} + 1 \equiv 0 \quad (2) \\
\overset{(a)}{\Rightarrow} \quad & \left((f(x)+1)^{p(|x|)} + 1\right)^{p(|x|)} \equiv 0 \quad (2)
\end{aligned}
$$

Theorem 27.

$$\oplus P^{BPP} \subseteq BPP^{\oplus P} \qquad \text{(oracle swapping)}$$

6.6 PH and PP

Lemma 28. (Valiant, Vazirani 1986)

For each set $L \in NP$, there ex. $B \in P$, polynomial p such that for all $x \in \Sigma^*$

(i) $x \in L \Rightarrow \underset{|u|=p(|x|)}{\text{prob}} \left[\| \{ z \mid |z| = p(|x|) \wedge (x,u,z) \in B \} \| \geq 1 \right] = 1$

(ii) $x \in L \Rightarrow \underset{|u|=p(|x|)}{\text{prob}} \left[\| \{ z \mid |z| = p(|x|) \wedge (x,u,z) \in B \} \| = 1 \right] \geq \frac{1}{8}$

(iii) $x \notin L \Rightarrow \underset{|u|=p(|x|)}{\text{prob}} \left[\| \{ z \mid |z| = p(|x|) \wedge (x,u,z) \in B \} \| = 0 \right] = 1$

■

Theorem 29.

$$NP \subseteq BPP^{\oplus P}$$

Proof: Let $L \in NP$ and suppose B, p are as described as in Lemma 27. Define

$$D =_{df} \{ (x,u) \mid \| \{ z \mid |z| = p(|x|) \wedge (x,u,z) \in B \} \| \equiv 1 \ (2) \}$$

Then, $D \in \oplus P$ and it holds that:

- $x \in L \rightarrow \underset{|u|=p(|x|)}{\text{prob}} \left[(x,u) \in D \right] \geq \frac{1}{8}$
- $x \notin L \rightarrow \underset{|u|=p(|x|)}{\text{prob}} \left[(x,u) \in D \right] = 0$

Define the set E as follows:

$$E =_{df} \{ (x, u_1, \ldots, u_9) \mid (x,u_1) \in D \vee \ldots \vee (x,u_9) \in D \}$$

We have $E \in \oplus P$ (by Cor. 25) and, moreover,

- $x \in L \rightarrow \underset{|u_1|=|u_2|=\ldots=|u_9|=p(|x|)}{\text{prob}} \left[(x, u_1, \ldots, u_9) \in E \right] \leq \left(\frac{7}{8} \right)^9 \leq \frac{1}{3}$

$$= 1 - \underset{|u_i|=p(|x|)}{\text{prob}} \left[\bigwedge_{i=1}^{9} (x,u_i) \notin D \right] = 1 - \left(\underset{|u|=p(|x|)}{\text{prob}} \left[(x,u) \notin D \right] \right)^9 \geq 2/3$$

• $x \notin L \Rightarrow \underset{|u_1|=\cdots=|u_g|=p(|x|)}{\text{prob}} [(x, u_1, \ldots, u_g) \in E] = 0$

Define M to be that PPTM $M^{(\cdot)}$ that guesses $u_1, \ldots, u_g$ and asks $(x, u_1, \ldots, u_g) \in E$. Then,

• $x \in L \rightarrow \text{prob}_{M^E}(x) \geq \frac{2}{3}$

• $x \notin L \rightarrow \text{prob}_{M^E}(x) = 0 \leq \frac{1}{3}$

Thus, $L \in BPP^{\oplus P}$

Note that all inclusions in this chapter hold relativizably, i.e., $NP^A \subseteq BPP^{\oplus P^A}$, $BPP^{BPP^A} = BPP^A$, $\oplus P^{\oplus P^A} = \oplus P^A$, $\oplus P^{BPP^A} \subseteq BPP^{\oplus P^A}$

Corollary 30. (Toda 1989)

$$PH \subseteq BPP^{\oplus P}$$

Proof: induction on the levels of the polyn. hierarchy.

• $k=1$: Theorem 28. $BPP^{BPP} = BPP$

• $k>1$: we obtain (i.o.)

$$\Sigma_k^P = NP^{\Sigma_{k-1}^P} \subseteq^P NP^{BPP^{\oplus P}}$$

$$\subseteq^{\text{Thm 28}} BPP^{\oplus P^{BPP^{\oplus P}}}$$

$$=^{\text{Thm.}} BPP^{BPP^{\oplus P} \oplus P}$$

$$= BPP^{BPP^{\oplus P}}$$

$$= BPP^{\oplus P}$$

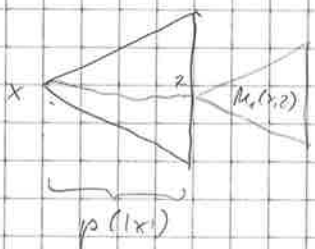
Theorem 31.

$$PP^{\oplus P} \subseteq P^{PP}$$

Proof: Let $L \in PP^{\oplus P}$, i.e., there ex. $B \in P^{\oplus P} = \oplus P$, polynomial p s.t. $x \in L \Leftrightarrow h_{B,p}(x) \geq 2^{p(|x|)} \uparrow -1$, and there is a $f \in \#P$ s.t.

$$(x,z) \in B \Rightarrow f(x,z) \equiv 1 \quad (2^{p(|x|)+1})$$
$$(x,z) \notin B \rightarrow f(x,z) \equiv 0 \quad (2^{p(|x|)+1})$$

Let M_1 be that NPTM that comp. f, i.e., $f = acc_{M_1}$.
Define M_2 to be an NPTM working as follows.



(*)

We obtain

$$acc_{M_2}(x) \equiv \sum_{|z|=p(|x|)} acc_{M_1}(x,z) \quad (2^{p(|x|)+1})$$

$$\equiv \sum_{|z|=p(|x|)} f(x,z) \quad (2^{p(|x|)+1})$$

$$\equiv h_{B,p}(x) \quad (2^{p(|x|)+1})$$

So, $h_{B,p}(x) = mod\left(acc_{M_2}(x), 2^{p(|x|)+1}\right)$

Define $M_3^{(*)}$ to be that POTM that, on input x,

(i) queries oracle $acc_{M_2}(x)$

(ii) accepts iff $mod\left(acc_{M_2}(x), 2^{p(|x|)-1}\right) > 2^{p(|x|)-1}$

Clearly, M_3 accepts L. So, $L \in P^{\#P} = P^{PP}$. ∎

Corollary 32. (Toda 1991)

$$PH \subseteq P^{PP}.$$