Computational Complexity - Lecture 21.

Recap: - #SAT, Perm are #P-complete.
- Toda: $PH \subseteq P^{\#P}$
- Approx counting $\in BPP^{NP}$

A puzzle:

You will be given x, y: $-N \leq x, y \leq N$.
Find an "expression" $h(x,y)$ s.t

$$h(x,y) \text{ is } \begin{cases} >0 & \text{if both } x,y \text{ are positive} \\ <0 & \text{if one of them is negative.} \end{cases}$$

Agenda: - The classes GapP & PP.
- Its connection to #P
- Beigel-Reingold-Spielman theorem.

Qn: Is this fn in #P? $f(x) = x^2 + 4x - 5$

No... any fn in #P is non-negative

Defn (GapP): $f: \Sigma^* \to \mathbb{N} \in$ GapP if there is a polytime machine $M(\,,\,)$ s.t

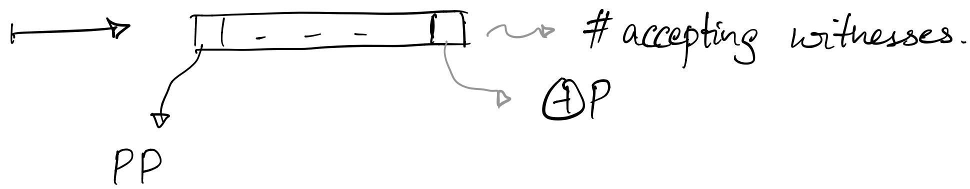
$$f(x) = \underbrace{\left|\{r : M(x,r)=1\}\right| - \left|\{r : M(x,r)=0\}\right|}_{Gap(M,x)}.$$

Some properties of GapP (similar to #P).

Obs: $f \in \#P \Rightarrow f \in$ GapP.

$f, g \in$ GapP $\Rightarrow$

- $f+g \in$ GapP.
- $fg \in$ GapP.
- $f-g \in$ GapP
- $f^3 + 3f^2g - 10f^4 + g^5 - 7 \in$ GapP
- $2^n \cdot f \in$ GapP

#P : x 

Defn: (Probabilistic poly time or PP): A language $L \subseteq \Sigma^*$ is in PP if there is a polytime machine $M(x, r)$ with $|r| \leq p(|x|)$ s.t.

$$x \in L \Leftrightarrow \Pr_r[M(x,r) \text{ accepts}] \geq 1/2$$
$$x \notin L \Leftrightarrow \Pr_r[M(x,r) \text{ accepts}] < 1/2.$$

(or)

$$x \in L \Leftrightarrow \#\text{acc. paths} \geq 2^{|r|-1}$$
$$x \notin L \Leftrightarrow \#\text{acc. paths} < 2^{|r|-1}.$$

Qn: If $L \in PP$, is $\bar{L}$ also in PP?

Obs: We can actually make the inequalities strict on both sides. ie

$$x \in L \Leftrightarrow \Pr_r[M(x,r)=1] > 1/2$$
$$x \notin L \Leftrightarrow \Pr_r[M(x,r)=1] < 1/2.$$

Pf: Say M was a machine for L acc. to above defn.
Say M uses m random bits

M': Pick $r_1, \ldots, r_m$. Let $b = M(x, r)$
If $b = 1$: return 1
If $b = 0$:
Toss $m+1$ random coins.
Acc if all were heads.
Rej o/w.

Btw, how many of you have heard of sinh, cosh, tanh?
(the hyperbolic trig fns)

What is the prob that M' accepts x?

$$\Pr[M'(x,r')=1] = \Pr[M(x,r)=1] + \Pr[M(x,r)=0 \ \& \ m+1 \text{ heads}] \quad (*)$$

If $x \in L$: $\quad (*) = p + (1-p)\cdot\frac{1}{2^{m+1}} > \frac{1}{2}$

If $x \notin L$: $\quad (*) \leqslant \frac{1}{2} - \frac{1}{2^m} + \frac{1}{2^{m+1}}\cdot(1-p) < 1/2$ $\square$.

$\therefore$ PP is the class where you have a randomised algo with some non-zero advatage.

Cor: $f \in PP \iff \neg f \in PP$.

Pf: With strict ineq on both sides, this is trivial. $\square$.

What is the connection to #P?

Obviously, $PP \subseteq P^{\#P}$.

Compute the # acc. paths & just return MSB.

$L = \{(M,x) : \text{If } M \text{ has} \geq 2^{m-1} \text{ acc. paths}\}$

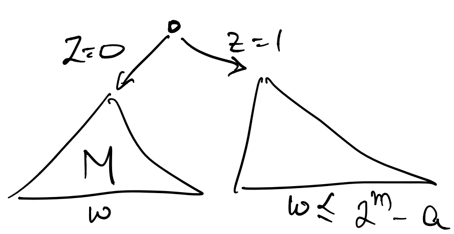
Lemma: $\#P \subseteq FP^{PP}$.

If you can compute the MSB, you can compute all bits.

Pf: $f: \Sigma^* \to$ [1 1 ...]

$f(x) = N \leq 2^n$ $\qquad$ PP: Is $N \geq 2^{n-1}$

Can I use PP oracle to check if $N \geq a$



$\#$ acc. paths $= f(x) + 2^m - a$

$\geq 2^m$ if $f(x) \geq a$

$\square$

$\therefore$ With PP as an oracle, we can simulate #P.

$\therefore$ Toda $\Rightarrow$ $PH \subseteq P^{\#P} \subseteq P^{PP}$.

An alt. definition for PP:

$$x \in L \iff Gap(M,x) > 0$$
$$x \notin L \iff Gap(M,x) < 0$$

Qn: If $L_1, L_2 \in PP$, is $L_1 \cap L_2$?

That is, if M_1, M_2 are such that

$x \in L_1 \iff Gap(M_1,x) > 0$ | $x \in L_2 \iff Gap(M_2,x) > 0$

$x \notin L_2 \iff Gap(M_1,x) < 0$ | $x \notin L_2 \iff Gap(M_2,x) < 0$.

Is there a machine N s.t

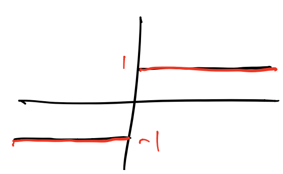
$$Gap(N,x) \text{ is } \begin{cases} >0 & \text{if both } Gap(M_1,x)>0 \;\&\; Gap(M_2,x) > 0 \\ <0 & \text{o/w.} \end{cases}$$

Thm: [Beigel-Reingold-Spielman] PP is closed under intersection.

What do we want to prove?

$f(x) = Gap(M_1,x)$ $\qquad$ $g(x) = Gap(M_2,x)$.

$H(x) = sign(f(x)) + sign(g(x)) - 1$



sign(f(a)) is not a polynomial...

But we know that $-2^m \le f(x) \le 2^m$

Can we approximate sign(x), for $-2^n \le x \le 2^n$ by a polynomial?

Suppose $S(x)$ satisfies the following properties.

- For $x = 1, 2, \ldots, 2^n$, $S(x) \in [1, 1.5]$
- $S(-x) = -S(x)$
- $S(x) = S_0 + S_1 x + \cdots + S_k x^k$
  where each S_i is "small" and k is small.

Issue: No such poly even comes close...

Brilliant idea 1: Let's try rational functions

$$S(x) = \frac{P(x)}{Q(x)}$$

Even if these were great approximations to sign(x), how is this useful in this context?

$$S(a) + S(b) - 1 = \frac{P(a)}{Q(a)} + \frac{P(b)}{Q(b)} - 1$$

$$= \frac{P(a) \cdot Q(b) + Q(a) \cdot P(b) - Q(a)Q(b)}{Q(a)Q(b)}$$

But we only care for the sign of)

$\Rightarrow \operatorname{sign}\left(S(a)+S(b)-1\right) = (\text{Num})\cdot(\text{Denom})$

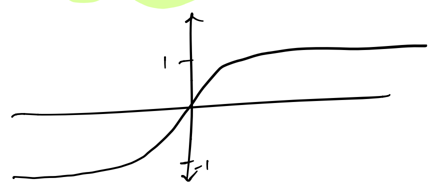
Then the expr: $\left(P(a)Q(b)+\dots+Q(a)Q(b)\right)\cdot Q(a)Q(b)$

$\therefore$ If we can find a good rational approximation $\frac{P(x)}{Q(x)}$ for $\operatorname{sign}(x)$, we will be done.

Where can we find such approximations?

Brilliant idea #2: What about $\tanh(x)$?

$$\tanh(x) = \frac{e^{x}-e^{-x}}{e^{x}+e^{-x}}$$



This is not a rational expr!

Why don't we replace e^x by a polynomial?

Attempt 1: $P_n(x) = \sum_{i=0}^{n} \frac{x^i}{i!}$

Define $S_n(x) = \frac{P_n(x) - P_n(-x)}{P_n(x)+P_n(-x)}$

Does this work?

$$\frac{P(x) - P(-x)}{P(x) + P(-x)} = \frac{P(x) + P(-x)}{P(x) + P(-x)} - \frac{2\,P(-x)}{P(x) + P(-x)}$$

$$= 1 + \frac{2}{\left(\frac{P(x)}{-P(-x)} - 1\right)}$$

What we want is for $\underline{P}(x) \gg -P(-x)$

Brilliant idea 3:

$$P_n(x) = (x+1)\prod_{i=1}^{n}(x+2^i)^2.$$

Newman.
Rational approx for $|x|$

Claim: For any $1 \leq x \leq 2^n$, $\quad P(x) \geq 4 \cdot (-P(-x)) \geq 0$

Pf: Term by term, $\quad P(x) \geq -P(-x). \geq 0$

Suppose $2^{i-1} \leq x \leq 2^i$

$$(x+2^i)^2 \geq 2^{2i}$$

$$(-x+2^i)^2 = (2^i - x)^2 \leq (2^{i-1})^2 = 2^{2i}/4. \quad \square.$$

$\therefore$ $\quad S_n(x) = \dfrac{P(x) - P(-x)}{P(x) + P(-x)}$ $\qquad$ odd function.

And for any $1 \leq x \leq 2^n$

$$S_n(x) = 1 + \frac{2}{\left(\frac{P(x)}{-P(-x)} - 1\right)} \leq 1 + \frac{2}{3} \leq \frac{5}{3}$$

The Gap fn for $L_1 \cap L_2$:

$f(x) = \text{Gap}(M_1, x)$ $\qquad$ $g(x) = \text{Gap}(M_2, x)$.

Define $H(z_1, z_2)$ $\qquad$ where $S(z) = A(z)/B(z)$

$$= \left[A(z_1)B(z_2) + A(z_2)B(z_1) - B(z_1)B(z_2)\right] \times$$
$$B(z_1) \cdot B(z_2)$$

Build a machine N s.t

$$\text{Gap}(N, x) = H(f(x), g(x))$$

$\therefore L_1 \cap L_2 \in PP$. $\square$.

BRS - idea comes from Newman's thm.