Classes PCP
19 mars 2021 10:27

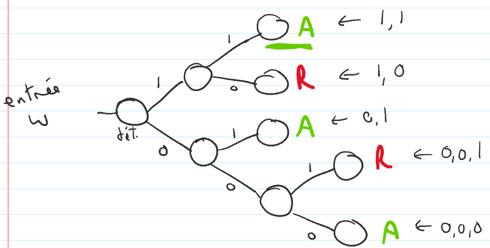
PCP = Probabilistically Checkable Proof

MT probabiliste : MT qui peut lancer une pièce p telle que
$Pr[p=0] = \frac{1}{2}$
$Pr[p=1] = \frac{1}{2}$

La MT peut prendre une décision selon le résultat

Fctionnement interne

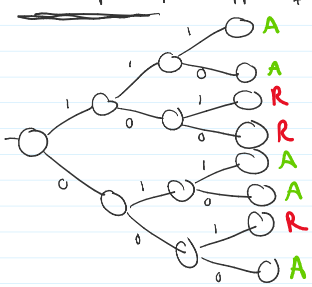
La MT M a accès à un oracle qui, en temps $O(1)$, écrit 0 ou 1 à l'emplacement de la tête chacun avec prob. $\frac{1}{2}$



$Pr[M \text{ accepte } w] = \frac{\#\text{chemins acceptant}}{\#\text{chemins total}}$

ici $= \frac{3}{5} = \frac{24}{40}$

Pour simplifier, on suppose que chaque chemin a la m̂ longueur.



$Pr[M \text{ accepte } w] = \frac{5}{8} = \frac{25}{40}$

Pas équivalent, mais + accepté

Vérificateur probabiliste pour un langage L.

On dit qu'une MT prob. V est un vérif. polynomial prob. pour L si :

1. $w \in L \Rightarrow \exists c$ t.q. $Pr[V \text{ accepte } \langle w,c \rangle] = 1$
2. $w \notin L \Rightarrow \forall c$ $\quad Pr[V \text{ accepte } \langle w,c \rangle] \leq \frac{1}{2}$

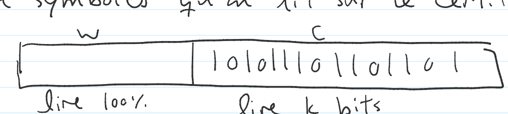
$\binom{NP}{0}$

Vérificateur PCP

Verif. prob. avec limites

- limiter le # de lancer de pièces permis
- limiter le # de symboles qu'on lit sur le certif. c.

↳ entrée :



MT accès au ième bit en $O(1)$

Déf. : vérificateur PCP

Un langage L admet un vérif. $(r(n), q(n))$-PCP s'il existe une MT probabiliste M qui satisfait :

0. sur entrée $\langle w, c \rangle$, M s'exécute en temps $O((|w|+|c|)^k)$
1. M utilise $r(n)$ lancers de pièces, $n = |w|$

⓪ sur entrée $\langle w, c \rangle$, M s'exécute en temps $O((|w|+|c|)^k)$

① M utilise $r(n)$ lancers de pièces, $n = |w|$

② M lit $q(n)$ symboles de c, $n = |w|$

③ M est un vérificateur prob. pour L

- si $w \in L$, $\Pr[M \text{ accepte } \langle w, c \rangle] = 1$ pour un certain c
- si $w \notin L$, $\Pr[M \text{ accepte } \langle w, c \rangle] \leq \frac{1}{2}$ $\forall c$

<u>Déf</u>: On dit que $L \in PCP(r(n), q(n))$ s'il existe des constantes c, d tq. L admet un vérificateur $(c \cdot r(n), d \cdot q(n))$-PCP.
On écrit parfois $L \in PCP(O(r(n)), O(q(n)))$.

<u>Le</u> théorème PCP : $NP = PCP(\underbrace{\log n}_{O(\log n) \text{ lancer de pièce}}, \underbrace{1}_{O(1) \text{ bits de certificat}})$

preuve ultra-profonde

ex : $PCP(\underbrace{0}_{0 \text{ aléatoire}}, \underbrace{\log n}_{\text{certif. } O(\log n)}) = P$