

# Théorème PCP. Applications à l'inapproximabilité. PC 9.

Soit  $q, r : \mathbb{N} \rightarrow \mathbb{N}$ . Un  $(r(n), q(n))$ -vérificateur de preuve probabiliste est un algorithme  $V$  en temps polynomial. Pour une entrée  $x$  et une preuve (= un certificat) que l'on considère être un mot  $P \in \{0, 1\}^*$ , l'algorithme  $V$  reçoit  $x$  et un vecteur  $r \in \{0, 1\}^{\mathcal{O}(r(|x|))}$  de bits aléatoires.  $V$  calcule alors un total de  $\mathcal{O}(q(|x|))$  positions et reçoit les valeurs des bits de  $P$  à ces positions précises. Avec cette information,  $V$  décide ou non d'accepter le triplet  $\langle x, r, P \rangle$ .

Un langage  $L$  appartient à  $\text{PCP}(r(n), q(n))$  s'il existe un  $(\mathcal{O}(r(n)), \mathcal{O}(q(n)))$  vérificateur tel que :

- $x \in L$  implique que  $\Pr(V \text{ accepte } x) = 1$ .
- $x \notin L$  implique que  $\Pr(V \text{ accepte } x) \leq 1/2$ .

On peut toujours supposer la preuve de longueur au plus  $q(n)2^{\mathcal{O}(r(n))}$ , où  $n = |x|$ .

## 1 De PCP au théorème PCP

1. Montrer que :
  - (a)  $\text{P} = \text{PCP}(0, 0)$ .
  - (b)  $\text{NP} = \text{PCP}(0, \text{poly})$ .
  - (c)  $\text{coRP} = \text{PCP}(\text{poly}, 0)$ .
2. Montrer que si  $L \in \text{PCP}(r(n), q(n))$  alors  $L$  est reconnaissable en temps non-déterministe  $2^{\mathcal{O}(r(n) + \log(n))}$ .

## 2 Problème MAX3SAT : Approximabilité

Montrer qu'il existe un algorithme en temps polynomial qui, étant donnée une formule  $\phi$  en  $3\text{CNF}$  avec  $n$  variables et  $m$  clauses, telle que chaque clause possède trois variables distinctes, produit une affectation qui satisfait  $7m/8$  clauses.

### 3 Problème MAX3SAT : Difficulté d'approximation

Rappel : le théorème PCP affirme le résultat surprenant  $NP = PCP(\log n, 1)$ .

On va l'utiliser pour montrer la difficulté d'approximer MAX3SAT.

1. Montrer que s'il existe  $\delta > 0$ , et un problème NP complet  $K$  et une réduction  $f$  de  $K$  vers 3SAT calculable en temps polynomial telle que
  - $x \in K$  implique que  $f(x)$  est une formule satisfiable
  - $x \notin K$  implique que au plus  $(1 - \delta) \cdot m$  clauses de  $f(x)$  sont satisfiables (on parle de *réduction écartante*) alors MAX3SAT n'est pas approximable en temps polynomial avec un rapport meilleur que  $1 - \delta$ , sauf si  $P = NP$ .
2. Utiliser le théorème PCP pour montrer que pour un certain  $\delta > 0$ , il existe une réduction  $f$  de 3SAT vers 3SAT telle que
  - (a) si  $\phi$  est une formule satisfiable, alors  $f(\phi)$  est satisfiable
  - (b) si  $\phi$  est insatisfiable, alors une fraction au plus  $1 - \delta$  des clauses de  $f(\phi)$  sont satisfiables simultanément.
3. Montrer que MAX3SAT n'est pas  $\alpha$ -approximable pour un certain  $\alpha$ , sauf si  $P = NP$ .

### 4 Calcul du permanent

Soit  $A = (a_{i,j})$  une matrice carrée à coefficients entiers. Le *permanent* est la quantité

$$\sum_{\sigma} \prod_{i=1}^n a_{i,\sigma(i)}.$$

1. Rappeler la définition du déterminant. Quelle est la complexité du calcul du déterminant.
2. Rappeler la formule de développement selon la première colonne du déterminant. Donner une formule similaire pour le permanent.
3. En utilisant ce développement, proposer un protocole de preuve interactif pour le permanent.