Classes de complexité probabilistes

François Schwarzentruber

8 mai 2023

1 Définitions

Définition 1 ZPP (*Zero-Error Probabilistic Polynomial time*) est la classe des problèmes de décision décidés par un algorithme probabiliste en **temps polynomial en espérance**.

Définition 2 RP (*Randomized Polynomial time*) est la classe des problèmes de décision L pour lesquels il existe un algorithme probabiliste A dont le temps est polynomial et :
- si $x \in L$, alors $\mathbb{P}(A(x) \text{ répond oui}) \geq 1/2$;
- si $x \notin L$, alors $\mathbb{P}(A(x) \text{ répond non}) = 1$.

Définition 3 $\text{coRP} = \{L \mid \overline{L} \in \text{RP}\}$.

Proposition 4 coRP est la classe des problèmes de décision L pour lesquels il existe un algorithme probabiliste A dont le temps est polynomial et :
- si $x \notin L$, alors $\mathbb{P}(A(x) \text{ répond non}) \geq 1/2$;
- si $x \in L$, alors $\mathbb{P}(A(x) \text{ répond oui}) = 1$.

2 Lien avec P

Proposition 5 $\text{P} \subseteq \text{ZPP}$.

Proposition 6 $\text{P} \subseteq \text{RP}$.

3 Exemples de problèmes

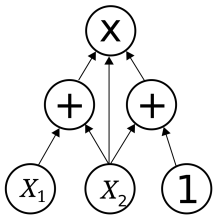
Définition 7 **PRIMES**

entrée : un nombre entier écrit en binaire
sortie : oui, s'il est premier, non sinon.

Le test de primalité de Solovay et Strassen [**?**] (ainsi que celui de Miller-Rabin) montre que **PRIMES** est dans coRP. Adleman et Huang [**?**] ont montré qu'il est aussi dans RP. Finalement, Agrawal-Kayal-Saxena [**?**] ont montré que **PRIMES** est dans P.

Définition 8 **Polynomial identity testing (PIT)**

entrée : un circuit arithmétique représentant un polynôme multivarié
sortie : oui, si le circuit représente le polynôme nul, non sinon.



PIT est dans RP et on ne sait pas s'il est dans P.

4 Lien avec NP

Proposition 9 (reformulation de la définition de NP) Un langage L est dans NP s'il existe un algorithme déterministe V en temps poly tel que :

— si $x \in L$, il existe $y \in \{0,1\}^{poly(|x|)}$ tel que $V(x,y) = 1$.

— si $x \notin L$, pour tout $y \in \{0,1\}^{poly(|x|)}$, on a $V(x,y) = 0$.

Proposition 10 (reformulation de la définition de RP) Un langage L est dans RP s'il existe un algorithme déterministe V en temps poly tel que :

— si $x \in L$, plus de la moitié des $y \in \{0,1\}^{poly(|x|)}$ sont tels que $V(x,y) = 1$.

— si $x \notin L$, pour tout $y \in \{0,1\}^{poly(|x|)}$, on a $V(x,y) = 0$.

Proposition 11 $\mathrm{RP} \subseteq \mathrm{NP}$

5 Lien entre RP et ZPP

Proposition 12 $\mathrm{ZPP} = \mathrm{RP} \cap \mathrm{coRP}$.

Références