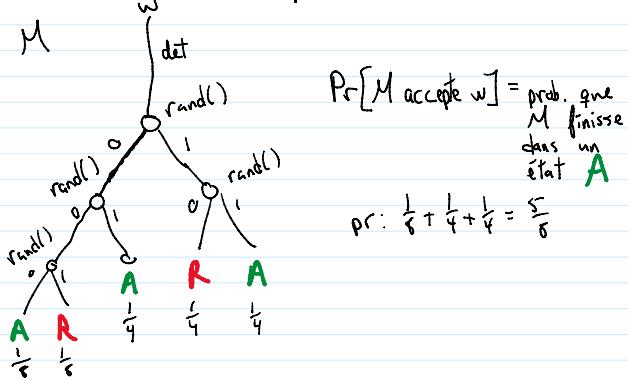


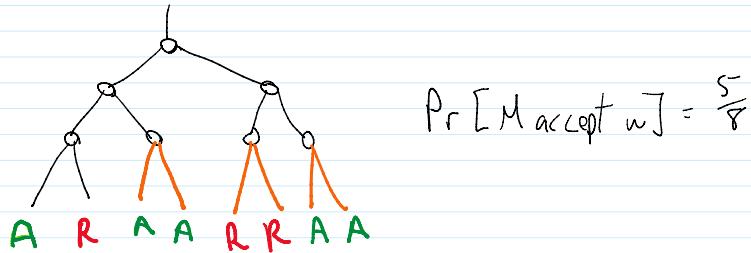
MT probabiliste : MT qui a accès à une fonction `rand()`
qui retourne 0 avec prob $\frac{1}{2}$
1 avec prob $\frac{1}{2}$



$$\Pr[M \text{ accepte } w] = \text{prob. que } M \text{ finisse dans un état A}$$

$$\Pr: \frac{1}{8} + \frac{1}{4} + \frac{1}{4} = \frac{5}{8}$$

Pour simplifier, on suppose que chaque chemin racine-feuille utilise le même # de `rand()`



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

$$\begin{aligned}\Pr[M \text{ accepte } w] &= \# \text{feuilles accept} / \# \text{feuilles} \\ &= (\# \text{chemins accept}) / 2^{\# \text{appel rand}}\end{aligned}$$

BPP (Bounded Probabilistic Polynomial)

On dit que $L \in \text{BPP}$ si \exists MT prob. M telle que

- $\forall w$, chaque chemin de calcul de M est en temps $O(n^k)$ (k constante)
- si $w \in L$, alors $\Pr[M \text{ accepte } w] \geq \frac{2}{3}$
- si $w \notin L$, alors $\Pr[M \text{ accepte } w] \leq \frac{1}{3}$

Prop: $P \subseteq \text{BPP}$

Trivial, car si $L \in P$, alors M qui décide L est un cas spécial d'une MT prob.

$$w \in L \Rightarrow \Pr[M \text{ acc. } w] = 1 \geq \frac{2}{3} \quad w \notin L \Rightarrow \Pr[M \text{ acc. } w] = 0 \leq \frac{1}{3}$$

Prop: $\text{BPP} \subseteq \text{PSPACE}$

Soit $L \in \text{BPP}$ et M est MT prob. en temps $O(n^k)$ et t_2 .

$$w \in L \Rightarrow \Pr[M \text{ acc. } w] \geq \frac{2}{3} \quad w \notin L \Rightarrow \Pr[M \text{ acc. } w] \leq \frac{1}{3}$$

global nbacc=0 global nbfeuille=0

w
1

$$w \in L \Rightarrow \Pr[M_{acc}, w] = 3 \quad w \notin L \Rightarrow \Pr[M_{acc}, w] \leq 3$$

global nbacc=0, global nbfeuille=0

derando(w, cfg_2)

simuler M à partir de cfg_2 jusqu'à une cfg_2 qui est finale, ou qui s'appelle rand

si cfg_2 est acceptante

$$nbacc += 1$$

$$nbfeuille += 1$$

si cfg_2 est rejettante

$$nbfeuille += 1$$

sinon //rand()

soit cfg_2a la config suivant cfg_2 si $rand() = 0$

derando(w, cfg_2a)

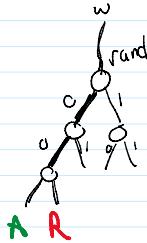
soit cfg_2b la config suivant cfg_2 si $rand() = 1$

! derando(w, cfg_2b)

derando(w, cfg_{init})

si $nbacc / nbfeuille \geq \frac{2}{3}$, accepter

sinon, rejeter // $\leq \frac{1}{3}$



Cet algo décide L correctement par les propriétés de M .

L'algo explore un arbre récursif de profondeur $O(n^k)$

car M roule en temps $O(n^k)$ sur toute combinaison de $rand()$, et l'algo n'explorera jamais plus profond que le # d'instructions de M .

De plus, l'espace requis par appel est au plus l'espace pour stocker $cfg_2, cfg_2a, cfg_2b, cfg_2b$, chacune $O(n^k)$

\Rightarrow L'algo roule en espace $O(n^k \cdot n^k) = O(n^{2k})$

$\Rightarrow L \in PSPACE$.

$BPP(f(n), g(n)) = \text{langages } L \text{ pour lesquels } \exists M \text{ T.P.C.P. avec}$

$$PP = BPP\left(>\frac{1}{2}, \frac{1}{2}\right)$$

$$w \in L \Rightarrow \Pr[M_{acc}, w] \geq f(n)$$

$$w \notin L \Rightarrow \Pr[M_{acc}, w] \leq g(n)$$

$$BPP = BPP\left(\frac{2}{3}, \frac{1}{3}\right)$$

$$BPP = BPP\left(1 - \frac{1}{2^{O(n)}}, \frac{1}{2^{O(n)}}\right) \quad (\text{Barnes Chernoff})$$

$$\text{BPP}\left(\frac{2}{3}, \frac{1}{3}\right) = \text{BPP}(0.74, 0.26)$$

- $\text{BPP}\left(\frac{2}{3}, \frac{1}{3}\right) \subseteq \text{BPP}(0.74, 0.26)$

Soit $L \in \text{BPP}\left(\frac{2}{3}, \frac{1}{3}\right)$ $w \in L \rightarrow \Pr \geq \frac{2}{3}$ $w \notin L, \Pr \leq \frac{1}{3}$

et soit M la MT prob. pour L .

On exécute M 3 fois et on prend la majorité.

Si $w \in L$, quelle est la prob. de se tromper et rejeter w ?

Cas où on se trompe:

$$\begin{array}{c} \boxed{000} \quad \boxed{001} \quad \boxed{010} \quad \boxed{100} \\ \frac{1}{3} \cdot \frac{1}{3} \cdot \frac{1}{3} \\ \frac{1}{27} \end{array} + \begin{array}{c} \boxed{001} \\ \frac{1}{3} \cdot \frac{1}{3} \cdot \frac{2}{3} \\ \frac{2}{27} \end{array} + \begin{array}{c} \boxed{010} \\ \frac{2}{3} \\ \frac{2}{27} \end{array} + \begin{array}{c} \boxed{100} \\ \frac{1}{3} \\ \frac{1}{27} \end{array} = \frac{7}{27} < 0.26$$

Prob qu'on ne se trompe pas $> 1 - 0.26 = 0.74$

Si $w \notin L$, prob de se tromper $> 0.74 \Rightarrow \Pr[\text{accept } w] < 0.26$

$$\text{BPP}\left(\frac{1}{2}, \frac{1}{2}\right) \quad w \in L \Rightarrow \Pr[\text{acc. } w] \geq \frac{1}{2} \quad w \notin L \Rightarrow \Pr[\text{acc. } w] \leq \frac{1}{2}$$

sur entrée w : si $\text{rand}() = 0$, accept
sinon rejett

~~$\text{BPP}\left(\frac{2}{3}, \frac{1}{3}\right)$~~

$$\text{BPP} = \text{BPP}\left(\frac{1}{2} + c, \frac{1}{2} - c\right)$$

Question: est-ce que $P = \text{BPP}$?

On pense que $P = \text{BPP}$

- $\text{PRIMES} = \{n : n \text{ est un nb premier et } n \text{ est encodé en binaire}\}$

$\text{PRIMES} \in \text{BPP}$

Pendant longtemps, on ne savait pas si $\text{PRIMES} \in P$.

Cela a été démontré en ≈ 2002

- Polynôme zéro

Polynôme sur n variables: $p(x_1, x_2, \dots, x_n)$

$$\text{ex: } p(x_1, x_2, x_3) = 5x_1 x_2^2 + 4x_1^4 x_3^2 - 10x_1 x_2 x_3 \quad \text{degré 6}$$

Degré = somme max des exposants d'un terme

Une assignation A attribue une valeur dans \mathbb{Z} à

Degré = somme max des exposants d'un terme

Une assignation A attribue une valeur dans \mathbb{Z} à tous les x_i .

On dénote par $p(A)$ la valeur du polynôme avec l'assignation A.

ex: $A = \{x_1=2, x_2=1, x_3=2\}$

$$p(A) = 5 \cdot 2^5 + 4 \cdot 1^4 - 10 \cdot 2^1 \cdot 1^2 \\ = 10 + 256 - 40 = 226$$

$ZERO_{POLY} = \{p(x_1, x_2, \dots, x_n), d\} : p$ est de degré d et l'assignation A, on a $p(A) = 0\}$

Lemme de Schwarz-Zippel

Soit $p(x_1, \dots, x_n)$ de degré d tel que $p(A) \neq 0$ pour au moins un A.

Soit $S \subseteq \mathbb{Z}$ un ensemble fini.

Soit $A = \{x_1=a_1, x_2=a_2, \dots, x_n=a_n\}$ une assignation aléatoire t.q. chaque a_i est choisi au hasard dans S de façon uniforme.

Alors

$$\Pr[p(A) = 0] \leq \frac{d}{|S|}.$$

Algo pour $ZERO_{POLY}$:

sur entrée $p(x_1, x_2, \dots, x_n), d$

soit $S = \{1, 2, \dots, 3d\}$

$A = ()$

pour $i=1 \dots n$
 $a_i = \text{elt aléatoire de } S$

A.ajouter($x_i = a_i$)

val = evaluer $p(A)$

si: val = 0, accepter

sinon rejeter

si $\langle p(x_1, \dots, x_n), d \rangle \in ZERO_{POLY}$, alors peu importe A choisi, $p(A) = 0$

\Rightarrow on accepte $\Rightarrow \Pr[M \text{ accepte}] = 1 \geq \frac{2}{3}$

Sinon $\notin ZERO_{POLY}$

Par le lemme,

$$\Pr[p(A) = 0] \leq \frac{d}{3d} = \frac{1}{3}$$

$$\Rightarrow \Pr[M \text{ accepte}] \leq \frac{1}{3}$$