INF581: Du calcul probabiliste au calcul quantique **Hiver 2011**

Cours 4 — 31 janvier

Enseignant : David XIAO *Rédacteur : Romain PREVOST*

Le but de ce cours est de définir le concept de preuve interactive et de l'appliquer sur des exemples simples.

4.1 Définition du modèle

Définition 4.1. *(rappel)*
$NP = \{L : \exists V$ *un algo déterministe (appelé vérificateur) tq* $\forall x \in L$,
$\exists \pi \in \{0,1\}^* \ |\pi| \leq |x|^c \Leftrightarrow V(x,\pi) = 1$ *et* V *se termine en* $n \leq |x|^c$ *etapes* $\}$

Exemple : $3-SAT = \{\varphi$ formule 3-CNF satisfiable $\}$

Contre-exemple : $\overline{3-SAT} = \{\varphi$ formule 3-CNF non satisfiable $\}$

L'idée des preuves interactives est d'avoir en plus un prouveur tout puissant avec lequel le vérificateur puisse interagir en posant des questions. Le vérificateur décide alors en fonction des réponses du prouveur.

Définition 4.2 (Preuve interactive déterministe).
Soient V *un vérificateur déterministe efficace,* P *un prouveur*
$q_1 = V(x,1), \quad r_1 = P(x,1,q_1)$
...
$q_i = V(x,i,r_1,...,r_{i-1}), \quad r_i = P(x,i,q_1,...,q_i)$
Le protocole de questions-réponses se termine après m *messages et on note le résultat :*
$< P,V > (x)$ *accepte ou rejette*

Définition 4.3.
$IP_{dét} = \{L : \exists V$ *un vérificateur déterministe efficace et* P *un prouveur tq*
$x \in L \Rightarrow < P,V > (x)$ *accepte*
$x \notin L \Rightarrow \forall P^* < P^*,V > (x)$ *rejette* $\}$

Exercice : $IP_{dét}$ vs. NP ?
Ces deux classes sont égales.

- $NP \subset IP_{dét}$: il suffit d'un seul message
- $IP_{dét} \subset NP$: le prouveur connaît l'entrée x et le fonctionnement du vérificateur donc il sait déjà toutes les questions que le vérificateur va lui poser. On pose donc $\pi = (r_1,...r_m)$ et $V'(x,\pi)$ tq que V' exécute simplement les $V(x,i,r_1,...,r_{i-1})$.

Définition 4.4 (Preuve interactive probabiliste).
Soient V un vérificateur déterministe efficace, P un prouveur, $\omega \leftarrow \{0,1\}^{|x|^c}$ un suite aléatoire

$$q_1 = V(x, 1, \omega), \quad r_1 = P(x, 1, q_1, \omega)$$
$$...$$
$$q_i = V(x, i, r_1, ..., r_{i-1}, \omega), \quad r_i = P(x, i, q_1, ..., q_i, \omega)$$

Le protocole de questions-réponses se termine après m messages et on note le résultat :

$$< P, V > (x, \omega) \text{ accepte ou rejette}$$

Définition 4.5.
$IP = \{L : \exists V$ *un vérificateur probabiliste efficace et P un prouveur tq*

$$x \in L \Rightarrow \Pr_{\omega}(< P, V > (x, \omega) \text{ accepte}) = 1$$
$$x \notin L \Rightarrow \forall P^* \Pr_{\omega}(< P^*, V > (x, \omega) \text{ accepte}) \leq 1/2\}$$


On définit aussi $IP[m]$ l'ensemble des langages ayant une preuve interactive avec m messages.

4.2 Premiers exemples

4.2.1 Graphes non-isomorphes

Définition 4.6.
Soit $G = (V, E)$ où $V = \{1, ..., n\}$ un graphe et $\pi \in \mathcal{S}_n$, on définit $\pi(G) = (V, E')$ le graphe permuté tq : $(u, v) \in E \Leftrightarrow (\pi(u), \pi(v)) \in E'$.
$G_0 \cong G_1$ si il existe $\pi \in \mathcal{S}_n$ tq $\pi(G_0) = G_1$.
$GNI = \{(G_0, G_1) : G_0 \ncong G_1\}$

Théorème 4.7. $\overline{GNI} \in NP$

Preuve: Il suffit de donner la permutation. □

Lemme 4.8. *Si $(G_0, G_1) \notin GNI$ alors $\forall T$ un ensemble de graphes*

$$\Pr_{\pi \in \mathcal{S}_n}(\pi(G_0) \in T) = \Pr_{\pi \in \mathcal{S}_n}(\pi(G_1) \in T)$$

Preuve: Soit σ tq $\sigma(G_0) = G_1$, alors :

$$\frac{|\{\pi : \pi(G_0) \in T\}|}{n!} = \frac{|\{\pi : \pi \circ \sigma(G_0) \in T\}|}{n!}$$

□

Théorème 4.9. $GNI \in IP$

Preuve:
Protocole :

- $b \in \{0, 1\}$ et $\pi \in \mathcal{S}_n$ sont choisis aléatoirement.
- (G_0, G_1) est envoyé au vérificateur V et au prouveur P.
- Le vérificateur envoie $H = \pi(G_b)$ au prouveur.
- Le prouveur (qui peut tout faire) calcule si $H \cong G_0$ et répond $b' = 0$ si oui et $b' = 1$ sinon.

- Si $b = b'$ alors $< P, V > (G_0, G_1)$ accepte et sinon $< P, V > (G_0, G_1)$ rejette.

Si $(G_0, G_1) \in GNI$ **:**
Posons : $\mathcal{U}_b = \{H : \exists \pi \in \mathcal{S}_n \text{ tq } H = \pi(G_b)\}$. Alors : $\mathcal{U}_0 \cap \mathcal{U}_1 = \emptyset$ donc P donne toujours la bonne réponse ie $\Pr_{b,\pi}(< P, V > (G_0, G_1) \text{ accepte}) = 1$.
Si $(G_0, G_1) \notin GNI$ **:**
Soit P^* un prouveur quelconque. Posons :
$T_0 = \{H : P^* \text{ répond 0 quand V demande H }\}$ et $T_1 = \{H : P^* \text{ répond 1 quand V demande H }\}$
On a alors :

$$\begin{aligned}
&\Pr_{b,\pi}(< P^*, V > (G_0, G_1) \text{ accepte}) \\
&\quad = \frac{1}{2}\Pr_{\pi}(< P^*, V > (G_0, G_1) \text{ accepte} \mid b = 0) + \frac{1}{2}\Pr_{\pi}(< P^*, V > (G_0, G_1) \text{ accepte} \mid b = 1) \\
&\quad = \frac{1}{2}\Pr_{\pi}(\pi(G_0) \in T_0) + \frac{1}{2}\Pr_{\pi}(\pi(G_1) \in T_1) \\
&\quad = \frac{1}{2}\Pr_{\pi}(\pi(G_0) \in T_0) + \Pr_{\pi}(\pi(G_0) \in T_1) \text{ d'après le lemme précédent} \\
&\quad = \frac{1}{2}\Pr_{\pi}(\pi(G_0) \in T_0 \cup T_1) \leq \frac{1}{2} \text{ car } T_0 \text{ et } T_1 \text{ sont disjoints}
\end{aligned}$$

□

4.2.2 $\overline{3-SAT}$

On considère une formule de la forme $\varphi = (x_1 \vee \overline{x_2} \vee x_5) \wedge (x_2 \vee x_3 \vee \overline{x_4}) \wedge ...$ et on lui associe un polynôme P_φ selon les règles suivantes :

- $x \to x$
- $\overline{x} \to 1 - x$
- $x \wedge y \to xy$
- $x \vee y \to 1 - (1 - x)(1 - y)$

Observations :
$\deg P_\varphi \leq 3m$ où m est le nombre de clauses dans φ.
φ est satisfiable $\Leftrightarrow \exists x \in \{0,1\}^n$ tq $P_\varphi(x) = 1$.

Pour que $\varphi \in \overline{3-SAT}$, il suffit de montrer $\sum_{x \in \{0,1\}^n} P_\varphi(x) = 0$ (sur $\mathbb{Z}$).

Définition 4.10 (Protocole $Sumcheck_{q,n}(p, c)$**).**

- *p un polynôme à n variables et c un entier naturel.*
- *Si $n = 1$ on vérifie $p(0) + p(1) = c$, et on accepte ou rejette.*
- *Si $n > 1$ on demande au prouveur de nous envoyer le polynôme $p'(x) = \sum_{x_2,...,x_n \in \{0,1\}} p(x, x_2, ..., x_n)$.*
- *On vérifie si $p'(0) + p'(1) = c$.*
- *Si ce n'est pas le cas, on rejette.*
- *Sinon on tire au hasard $r \in \mathbb{Z}_q$ et on exécute $Sumcheck_{q,n-1}(p(r, ...), p'(r))$.*

Théorème 4.11. *Si* $\sum_{x\in\{0,1\}^n} p(x) = c \mod q$ *alors* $Sumcheck_{q,n}(p,c)$ *accepte.*

Sinon il rejette avec une probabilité $\geq 1 - \frac{nd}{q}$ *où* $d = \deg p$.

Preuve:

Si $\sum_{x\in\{0,1\}^n} p(x) = c \mod q$ **:**

Si $n = 1$ on a bien $p(0) + p(1) = c$ donc $< P, V > (p, c)$ accepte.
Sinon :

$$\begin{aligned} p'(0) + p'(1) &= \sum_{x_2,...,x_n\in\{0,1\}} p(0, x_2, ..., x_n) + \sum_{x_2,...,x_n\in\{0,1\}} p(1, x_2, ..., x_n) \\ &= \sum_{x_1,...,x_n\in\{0,1\}} p(x_1, ..., x_n) = c \end{aligned}$$

Et par induction $Sumcheck_{q,n-1}(p(r, ...), p'(r))$ accepte donc $< P, V > (p, c)$ accepte.

Si $\sum_{x\in\{0,1\}^n} p(x) \neq c \mod q$ **:**

La preuve se fait aussi par induction sur n. Posons :
$\mathcal{H}_n$: $\forall p$ polynôme à n-1 variables et c tq $\sum_{x\in\{0,1\}^n} p(x) \neq c \mod q$ on a $\Pr(Sumcheck_{q,n}(p, c)$ accepte$) \leq \frac{dn}{q}$ avec $d = \deg p$.
Si $n = 1$ le vérificateur rejette donc $\mathcal{H}_1$ est vrai.
Soit n un entier, supposons $\mathcal{H}_{n-1}$ vrai. Si $p'(x) = \sum_{x_2,...,x_n\in\{0,1\}} p(x, x_2, ..., x_n)$ (ie P est le prouveur honnête) alors $p'(0) + p'(1) \neq c$ donc le vérificateur rejette.
Sinon $p'(x) \neq \sum_{x_2,...,x_n\in\{0,1\}} p(x, x_2, ..., x_n)$ et on en déduit :

$$\begin{aligned} &\Pr(Sumcheck_{q,n}(p, c) \text{ accepte}) \\ &\quad \leq \Pr_r\Big(\sum_{x_2,...,x_n\in\{0,1\}} p(r, x_2, ..., x_n) = p'(r)\Big) \\ &\qquad + \Pr_r(Sumcheck_{q,n-1}(p(r, ...), p'(r)) \text{ accepte et } \sum_{x_2,...,x_n\in\{0,1\}} p(r, x_2, ..., x_n) \neq p'(r)) \\ &\quad \leq \frac{d}{q} + \frac{d(n-1)}{q} = \frac{dn}{q}. \end{aligned}$$

Ce qui montre $\mathcal{H}_n$ et termine la démonstration. □

Corollaire 4.12. $\overline{3 - SAT} \in IP$

Preuve: Soit q premier $\geq 3^m$ il suffit d'exécuter $Sumcheck_{q,n}(P_\varphi, 0)$.
φ non satisfiable $\Rightarrow$ $Sumcheck_{q,n}(P_\varphi, 0)$ accepte.
φ satisfiable $\Rightarrow \Pr(Sumcheck_{q,n}(P_\varphi, 0)$ rejette$) \geq 1 - \frac{3mn}{3^m}$. □

4.3 Divers résultats

Corollaire 4.13. $\overline{3-SAT} \in IP[O(n)]$ *et* $GNI \in IP[O(1)]$

Théorème 4.14. $IP[k+1] \subset IP[k]$

Théorème 4.15. $IP = PSPACE$

Définition 4.16.
$IP_{c,s} = \{L : L$ *a une preuve interactive* P, V *tq*
$x \in L \Rightarrow \Pr_{\omega}(< P, V > (x, \omega)$ *accepte*$) \geq c$
$x \notin L \Rightarrow \forall P^* \Pr_{\omega}(< P^*, V > (x, \omega)$ *accepte*$) \leq s\}$

Théorème 4.17. $\forall c > s$ *constants,* $IP_{c,s} = IP_{1-2^{-n},2^{-n}} = IP_{1,2^{-n}}$

Preuve ($IP_{1-2^{-n},2^{-n}} = IP_{1,2^{-n}}$):
On tire aléatoirement ω dans $\{0,1\}^t$ et le prouveur trouve des $s_1, ..., s_m$ dans $\{0,1\}^t$ qui satisfont certaines conditions.
On répète le protocole habituel en rempla ant le paramètre aléatoire de la session i par le paramètre $s_i \oplus \omega$ (où $\oplus$ désigne le "ou exclusif").
V accepte si et seulement si il existe une session i qui accepte.

Si $x \in L$ alors :
$\exists s_1, ..., s_m$ tq $\forall \omega \ \exists i \in \{1, ..., m\}$ tq $< P, V > (x, s_1 \oplus \omega)$ accepte.
On en déduit :
$\Pr_{s_1,...s_m}(\forall \omega \ \exists i \in \{1, ..., m\}$ tq $< P, V > (x, s_1 \oplus \omega)$ accepte$) > 0$
et
$\Pr_{s_1,...s_m}(\forall \omega \ \exists i \in \{1, ..., m\}$ tq $< P, V > (x, s_1 \oplus \omega)$ rejette$)$
$\leq 2^t \Pr_{s_1,...s_m}(\exists i \in \{1, ..., m\}$ tq $< P, V > (x, s_1 \oplus \omega)$ rejette$) \leq 2^t(1-c)^m$
Il suffit de prendre : $m = O(t/(\log \frac{1}{1-c}))$

Si $x \notin L$ alors : $\forall P^* \ \forall s_1, ..., s_m$
$\Pr_{\omega}(\exists i \in \{1, ..., m\}$ tq $< P^*, V > (x, s_1 \oplus \omega)$ accepte$)$
$\leq m \Pr_{\omega}(< P^*, V > (x, s_1 \oplus \omega)$ accepte$) \leq m2^{-n}$ □