Protocoles interactifs.

Deux machines discutent : le *prouveur* $\mathscr{P}$ et le *vérificateur* $\mathscr{V}$. Le prouveur a une puissance de calcul illimitée, et le vérificateur ne fait pas initialement « confiance » au prouveur.

Exemple 1. On donne un protocole interactif pour SAT : étant donnée une formule booléenne $F(x_1, \ldots, x_n)$,

1. le prouveur $\mathscr{P}$ envoie $(a_1, \ldots, a_n) \in \{0,1\}^n$ au vérificateur $\mathscr{V}$;
2. le vérifieur $\mathscr{V}$ accepte si $(a_1, \ldots, a_n)$ satisfait F.

Analysons ce protocole :

- ▷ si $F \notin$ SAT alors $\mathscr{V}$ rejette toujours ;
- ▷ si $F \in$ SAT alors $\mathscr{P}$ peut convaincre $\mathscr{V}$ d'accepter.

Exemple 2. On donne un protocole interactif pour le *non-isomorphisme de graphes*.

On définit le problème ISOGRAPH :

ISOGRAPH	**Entrée.** Deux graphes G_0 et G_1 **Sortie.** Est-ce que G_0 est isomorphe à G_1 ?

où un *isomorphisme* entre (W, E) et $(W, E') = \pi(W, E)$ est une permutation $\pi : W \to W$ des sommets avec

$$E' := \big\{ (i,j) \;\big|\; \big(\pi(i), \pi(j)\big) \in E \big\}.$$

On notera alors $(W, E) \cong (W, E')$.

On a que IsoGraph $\in$ NP (avec π le certificat). Mais, on ne sait pas si le problème est NP-complet, il existe un algorithme en temps $n^{O(\log n)}$.

Par définition, le problème de *non*-isomorphisme de graphe est dans coNP (par définition).

Étant donnée une paire de graphe (G_0, G_1) sur le même ensemble de sommets W,

1. le vérificateur $\mathcal{V}$ choisit un bit aléatoire $b \in \{0, 1\}$, et une permutation aléatoire π sur W, et $\mathcal{V}$ envoie à $\mathcal{P}$ le graphe $G' = \pi(G_b)$;
2. quand $\mathcal{P}$ reçoit G', alors $\mathcal{P}$ renvoie à $\mathcal{V}$ un bit $b' \in \{0, 1\}$;
3. le vérificateur $\mathcal{V}$ accepte si $b = b'$.

Le but de $\mathcal{P}$ est de convaincre $\mathcal{V}$ que $G_0 \not\cong G_1$.

- ▷ Si $G_0 \not\cong G_1$ alors G' est isomorphe à un unique graphe $G_{b'}$ et renvoie b' au vérificateur.
- ▷ Si $G_0 \cong G_1$, alors pour tout prouveur, $\Pr[\mathcal{V} \text{ accepte}] = 1/2$. En effet, pour tout G',

$$\Pr[\mathcal{V} \text{ renvoie } G' \mid b = 0] = \Pr[\mathcal{V} \text{ renvoie } G' \mid b = 1],$$

notons $p_{i,j} := \Pr[\mathcal{P} \text{ envoie } b' = j \mid b = i]$ et on observe que $p_{11} = p_{21}$, d'où

$$\Pr[\mathcal{V} \text{ accepte}] = \frac{1}{2}(p_{11} + p_{22}) = \frac{1}{2}(p_{21} + p_{22}) = \frac{1}{2}.$$

On peut réduire l'erreur en répétant le protocole k fois, et on accepte si (G_0, G_1) est toujours accepté par $\mathcal{V}$, et on aura $\Pr[\mathcal{V} \text{ accepte}] \leq 1/2^k$.

1 La classe IP.

On a la situation représentée en figure 1, où

- le x est l'entrée du problème (de taille n) ;
- le r est la donnée des choix aléatoires de v (de taille polynomiale en n) ;
- les y_i sont les messages de $\mathcal{V}$ à $\mathcal{P}$ (de taille polynomiale en n) ;
- les z_i sont les messages de $\mathcal{P}$ à $\mathcal{V}$ (de taille polynomiale en n) ;
- le s est la longueur de l'échange (avec s polynomial en n).

La puissance de calcul de $\mathcal{P}$ est *non-bornée*, et celle de $\mathcal{V}$ est polynomialement bornée. La *décision finale du vérificateur* est $\mathcal{V}(x, r, z_1, \ldots, z_s) \in \{0, 1\}$.

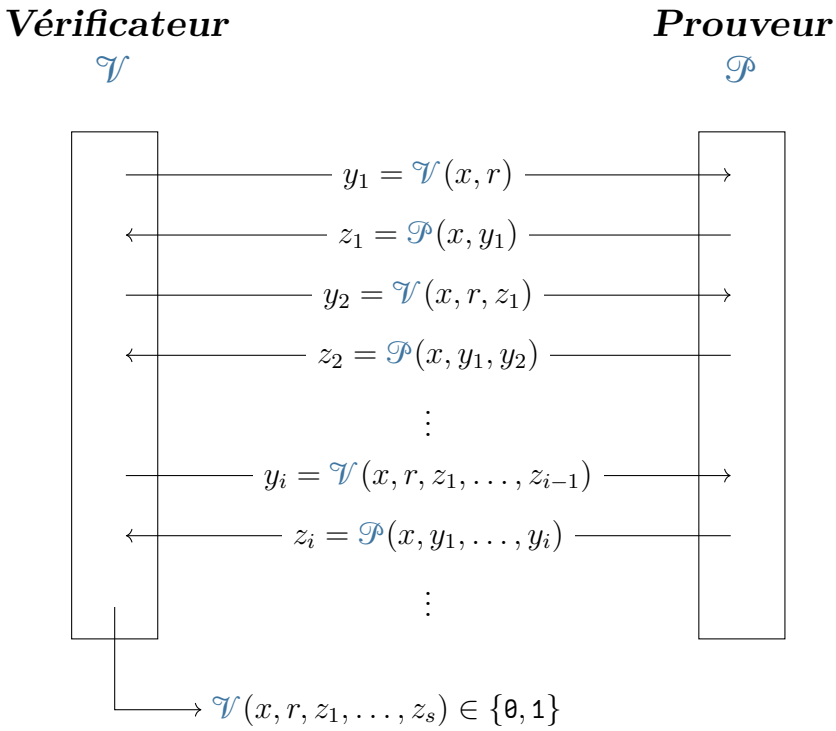

Figure 1 | *Protocole interactif*

Définition 1. On définit IP la classe des langages que l'on peut reconnaitre à l'aide d'un protocole interactif avec probabilité d'er-

reur inférieur à 1/3.

Exemple 3. On a Sat $\in$ IP et $\Sigma^\star \setminus$ IsoGraph $\in$ IP.

Théorème 1. On a IP = PSPACE.

Remarque 1. On a IP $\subseteq$ PSPACE, c'est le « sens facile ».

En revanche, le résultat PSPACE $\subseteq$ IP ***ne se relativise pas*** : il existe A tel que PSPACE^A n'est pas inclus dans IP^A (et même coNP^A n'est pas inclus dans IP^A).

Pour montrer PSPACE $\subseteq$ IP, on utilise le fait que QBF est PSPACE-complet : il suffira donc de montrer que QBF $\in$ IP, et on pourra utiliser les propriétés spécifiques de QBF, en particulier l'***arithmétisation*** (on peut voir des formules booléennes comme des polynômes).

Définition 2. On définit le problème $\sharp$Sat par

$\sharp$Sat	**Entrée.** Une formule booléenne ϕ sous CNF et $k \in \mathbb{N}$ **Sortie.** La formule ϕ est-elle satisfaite par exactement k valuations ?

Théorème 2. On a $\sharp$Sat $\in$ IP.