Théorème de Toda

Yann Strozecki

25 décembre 2007

1. Introduction
2. Premier pas dans les classes de comptage
   - Rappel
   - Propriétés de *GapP*
   - Quelques autres classes de comptage
   - Généralisation de classes
3. Le corps de la preuve
   - Le théorème de Valiant-Vazirani
   - Applications
   - Les ingrédients du théorème de Toda
   - Toda himself
4. Conclusion
   - Résultat
   - Pour aller plus loin

On veut explorer en détail la classe $\sharp P$, par rapport à la réduction Turing.

On veut explorer en détail la classe $\sharp P$, par rapport à la réduction Turing.

- La réduction Turing est très forte !

On veut explorer en détail la classe $\sharp P$, par rapport à la réduction Turing.

- La réduction Turing est très forte !
- Certains problèmes sont $\sharp P$ complets alors que leurs problèmes de décision sont dans P.

On veut explorer en détail la classe $\sharp P$, par rapport à la réduction Turing.

- La réduction Turing est très forte !
- Certains problèmes sont $\sharp P$ complets alors que leurs problèmes de décision sont dans P.
- Si NP était stable par réduction Turing alors $PH = NP$.

On veut explorer en détail la classe $\sharp P$, par rapport à la réduction Turing.

- La réduction Turing est très forte !
- Certains problèmes sont $\sharp P$ complets alors que leurs problèmes de décision sont dans P.
- Si NP était stable par réduction Turing alors $PH = NP$.
- Si $\sharp P$ était stable par réduction Turing, on aurait grâce à cet exposé $PH = UP$

Théorème (Toda 91)

$PH \subseteq P^{\sharp P}$

Théorème (Toda 91)

$PH \subseteq P^{\sharp P}$

On a mieux en fait !

Théorème (Toda 91)

$PH \subseteq P^{\sharp P}$

On a mieux en fait !

Théorème (Toda 91)

$PH \subseteq P^{\sharp P[1]}$

Définition (Classe $\sharp P$)

La classe $\sharp P$ est l'ensemble des fonctions f telles qu'il existe une machine M telle que pour tout x, $f(x)$ est égal au nombre de chemin acceptant de M sur x.

Définition (Classe *GapP*)

La classe *GapP* est l'ensemble des fonctions f telles qu'il existe une machine M telle que pour tout x, $f(x)$ est égal à la différence entre le nombre de chemins acceptants et refusants de M sur x.

Lemme

Les propositions suivantes sont équivalentes :

1. $f \in GapP$.
2. f *est la différence de deux fonctions de* $\sharp P$.
3. f *est la différence d'une fonction de* $\sharp P$ *et d'une fonction de* FP.

Lemme

Les propositions suivantes sont équivalentes :

1. $f \in GapP$.
2. f *est la différence de deux fonctions de* $\sharp P$.
3. f *est la différence d'une fonction de* $\sharp P$ *et d'une fonction de* FP.

Corollaire

$GapP \subseteq FP^{\sharp P[1]}$.

Lemme (Propriétés de clôture)

La classe GapP est close par somme et produit, c'est à dire si $f \in GapP$ et q un polynôme alors les deux fonctions suivantes sont dans GapP :

1. $\sum_{|y| \leq q(|x|)} f(x, y)$
2. $\prod_{0 \leq y \leq q(|x|)} f(x, y)$

Definition (Classe $\oplus P$)

La classe $\oplus P$ est l'ensemble des langages L tels qu'il existe une fonction $f \in \sharp P$ vérifiant

- Si $x \in L$ alors $f(x)$ est impair.
- Si $x \notin L$ alors $f(x)$ est pair.

Definition (Classe UP)

La classe UP est l'ensemble des langages L tels qu'il existe une fonction $f \in \sharp P$ vérifiant

- Si $x \in L$ alors $f(x) = 1$.
- Si $x \notin L$ alors $f(x) = 0$.

Definition (Opérateur *Gap*.)

La classe $Gap.\mathcal{C}$ est constituée des fonctions différences de deux fonctions de comptage associées à un problème de $\mathcal{C}$.

Definition (Opérateur P.)

La classe $P.\mathcal{C}$ est constituée des langages L tels qu'il existe une fonction de $Gap.\mathcal{C}$ f vérifiant

- Si $x \in L$ alors $f(x) > 0$.
- Si $x \notin L$ alors $f(x) \leq 0$.

Théorème (Valiant-Vazirani 86)

Soit f une fonction $\sharp P$, alors il existe une fonction g de $\sharp P$ et deux polynômes q et t tels que

1. *Si $f(x) = 0$ alors $g(x, r) = 0$ pour tout $r \in \Sigma^{q(n)}$*
2. *Si $f(x) > 0$ alors $Pr_{r \in \Sigma^{q(n)}}(g(x, r) = 1) \geq \frac{1}{t(n)}$*

Théorème (Valiant-Vazirani 86)

Soit f une fonction $\sharp P$, alors il existe une fonction g de $\sharp P$ et deux polynômes q et t tels que

1. *Si $f(x) = 0$ alors $g(x, r) = 0$ pour tout $r \in \Sigma^{q(n)}$*
2. *Si $f(x) > 0$ alors $Pr_{r \in \Sigma^{q(n)}}(g(x, r) = 1) \geq \frac{1}{t(n)}$*

Remarque : Ce théorème signifie qu'on peut associer à une fonction $\sharp P$ une fonction de signe dans $\sharp P$.

Théorème (Valiant-Vazirani 86)

Soit f une fonction $\sharp P$, alors il existe une fonction g de $\sharp P$ et deux polynômes q et t tels que

1. *Si $f(x) = 0$ alors $g(x, r) = 0$ pour tout $r \in \Sigma^{q(n)}$*
2. *Si $f(x) > 0$ alors $Pr_{r \in \Sigma^{q(n)}}(g(x, r) = 1) \geq \frac{1}{t(n)}$*

Remarque : Ce théorème signifie qu'on peut associer à une fonction $\sharp P$ une fonction de signe dans $\sharp P$.

Remarque : Pour démontrer ce théorème on utilise la technique du universal hashing (hachage universel ?) qui sert aussi à démontrer $BPP \subseteq \Sigma_2^p$

Lemme

$\sharp.P^{NP} = \sharp.coNP$

Lemme

$\sharp.P^{NP} = \sharp.coNP$

Des lemme et théorème précédents on déduit le résultats suivants :

Lemme

Soit $f \in \sharp.P^{NP}$ et p un polynôme. Il existe une fonction g de GapP et un polynôme q tels que

$$Pr_{r \in \Sigma^{q(n)}}(g(x, r) = f(x)) \geq 1 - 2^{-p(n)}$$

On déduit par induction des lemmes précédents le théorème suivant :

Théorème

Soit $f \in Gap.P^{PH}$ et p un polynôme. Il existe une fonction g de $GapP$ et un polynôme q tels que

$$Pr_{r \in \Sigma^{q(n)}}(g(x, r) = f(x)) \geq 1 - 2^{-p(n)}$$

Lemme

$PH \subseteq P.\oplus P$

Démonstration :

- Soit un langage L de PH, il existe χ fonction indicatrice L dans $GapP^{PH}$.

Démonstration :

- Soit un langage L de PH, il existe χ fonction indicatrice L dans $GapP^{PH}$.
- On applique le théorème d'approximation par une fonction g $GapP$ pour une précision $\frac{3}{4}$.

Démonstration :

- Soit un langage L de PH, il existe χ fonction indicatrice L dans $GapP^{PH}$.
- On applique le théorème d'approximation par une fonction g $GapP$ pour une précision $\frac{3}{4}$.
- $Pr_{r \in \Sigma^{q(n)}}(g(x,r) = \chi(x) \geq \frac{3}{4}$.

Démonstration :

- Soit un langage L de PH, il existe χ fonction indicatrice L dans $GapP^{PH}$.
- On applique le théorème d'approximation par une fonction g $GapP$ pour une précision $\frac{3}{4}$.
- $Pr_{r \in \Sigma^{q(n)}}(g(x,r) = \chi(x) \geq \frac{3}{4}$.
- Si $x \in L$ alors pour plus de la moitié des r, $g(x,r) = 1$.

Démonstration :

- Soit un langage L de PH, il existe χ fonction indicatrice L dans $GapP^{PH}$.
- On applique le théorème d'approximation par une fonction g $GapP$ pour une précision $\frac{3}{4}$.
- $Pr_{r \in \Sigma^{q(n)}}(g(x,r) = \chi(x) \geq \frac{3}{4}$.
- Si $x \in L$ alors pour plus de la moitié des r, $g(x,r) = 1$.
- On pose A le langage constitué des paires (x,r) telles que $g(x,r)$ est impair, comme g est $GapP$, A est dans $\oplus P$.

Démonstration :

- Soit un langage L de PH, il existe χ fonction indicatrice L dans $GapP^{PH}$.
- On applique le théorème d'approximation par une fonction g $GapP$ pour une précision $\frac{3}{4}$.
- $Pr_{r \in \Sigma^{q(n)}}(g(x,r) = \chi(x) \geq \frac{3}{4}$.
- Si $x \in L$ alors pour plus de la moitié des r, $g(x,r) = 1$.
- On pose A le langage constitué des paires (x,r) telles que $g(x,r)$ est impair, comme g est $GapP$, A est dans $\oplus P$.
- La fonction $f = \sharp.A - \sharp.\overline{A}$ est par définition dans $Gap.\oplus P$.

Démonstration :

- Soit un langage L de PH, il existe χ fonction indicatrice L dans $GapP^{PH}$.
- On applique le théorème d'approximation par une fonction g $GapP$ pour une précision $\frac{3}{4}$.
- $Pr_{r \in \Sigma^{q(n)}}(g(x,r) = \chi(x) \geq \frac{3}{4}$.
- Si $x \in L$ alors pour plus de la moitié des r, $g(x,r) = 1$.
- On pose A le langage constitué des paires (x,r) telles que $g(x,r)$ est impair, comme g est $GapP$, A est dans $\oplus P$.
- La fonction $f = \sharp.A - \sharp.\overline{A}$ est par définition dans $Gap.\oplus P$.
- Quand f est positive sur x, $x \in L$ et quand f est négative $x \notin L$ donc $L \in P.\oplus P$.

Lemme (Lemme technique d'amplification)

Pour toute constante k et toute fonction g de GapP, il existe $\hat{g}$ de GapP telle que

1. *Si* $g(x,r) \mod 2 = 1$ *alors* $\hat{g}(x,r) \mod 2^k = 1$
2. *Si* $g(x,r) \mod 2 = 0$ *alors* $\hat{g}(x,r) \mod 2^k = 0$

Démonstration : On construit un polynôme en g qui grâce aux propriétés de clôture par produit de *GapP* reste dans *GapP*.

Récapitulatif :

1. *GapP* est stable par produit.

Récapitulatif :

1. $GapP$ est stable par produit.
2. Valiant-Vazirani : on peut approximer le signe d'une fonction de décision de $\sharp P$ par une fonction de $\sharp P$.

Récapitulatif :

1. $GapP$ est stable par produit.
2. Valiant-Vazirani : on peut approximer le signe d'une fonction de décision de $\sharp P$ par une fonction de $\sharp P$.
3. On peut approximer une fonction de $GapP^{PH}$ par une fonction de $GapP$.

Récapitulatif :

1. $GapP$ est stable par produit.
2. Valiant-Vazirani : on peut approximer le signe d'une fonction de décision de $\sharp P$ par une fonction de $\sharp P$.
3. On peut approximer une fonction de $GapP^{PH}$ par une fonction de $GapP$.
4. $PH \subseteq P.\oplus P$

Récapitulatif :

1. $GapP$ est stable par produit.
2. Valiant-Vazirani : on peut approximer le signe d'une fonction de décision de $\sharp P$ par une fonction de $\sharp P$.
3. On peut approximer une fonction de $GapP^{PH}$ par une fonction de $GapP$.
4. $PH \subseteq P.\oplus P$
5. $P.\oplus P \subseteq P^{GapP[1]}$ en utilisant le lemme d'amplification.

Récapitulatif :

1. $GapP$ est stable par produit.
2. Valiant-Vazirani : on peut approximer le signe d'une fonction de décision de $\sharp P$ par une fonction de $\sharp P$.
3. On peut approximer une fonction de $GapP^{PH}$ par une fonction de $GapP$.
4. $PH \subseteq P.\oplus P$
5. $P.\oplus P \subseteq P^{GapP[1]}$ en utilisant le lemme d'amplification.
6. Caractérisation des fonctions $GapP$: $P^{GapP[1]} = P^{\sharp P[1]}$

On a donc démontré le théorème de Toda

Théorème (Toda 91)

$PH \subseteq P^{\sharp P[1]}$

On a donc démontré le théorème de Toda

Théorème (Toda 91)

$PH \subseteq P^{\sharp P[1]}$

Corollaire

$PH \subseteq MP$

Remarque : Si $\sharp P$ est clos par réduction Turing avec un appel à l'oracle, alors $P^{\sharp P[1]} = \sharp P$.
On en déduit que $PH \subseteq \sharp P$ en voyant $\sharp P$ comme des fonctions indicatrices.
Donc comme annoncé $PH = UP$ ce qui paraît improbable.

Remarque : Si on pouvait avoir une fonction signe dans $\sharp P$ pour toute fonction $\sharp P$, alors on aurait $UP = NP$ et on déduirait en refaisant Toda $PH \subseteq SPP$.