Interpolation en théorie de Valiant

Pascal Koiran Sylvain Perifel

LIP, ENS Lyon

Villeurbanne, le 17 janvier 2008

Introduction

Deux façons de calculer un polynôme à coefficients entiers

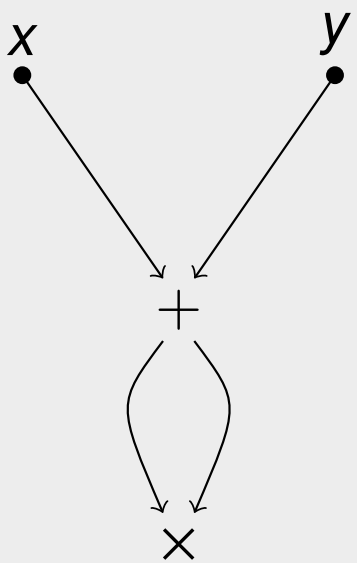
- Algorithme qui évalue le polynôme en un point entier.
  Exemple : $P(x, y) = (x + y)^2$ sur l'entrée $(1, 3) \to 16$.

Introduction

Deux façons de calculer un polynôme à coefficients entiers

- Algorithme qui évalue le polynôme en un point entier.
  Exemple : $P(x, y) = (x + y)^2$ sur l'entrée $(1, 3) \to 16$.

- Circuit arithmétique qui calcule le polynôme.
  Exemple :



Une question de Papadimitriou

Question ♣

Si un polynôme P est évalué par un algorithme en temps polynomial, est-il vrai qu'il est calculable par un circuit arithmétique de taille polynomiale ?

Une question de Papadimitriou

Question ♣

Si un polynôme P est évalué par un algorithme en temps polynomial, est-il vrai qu'il est calculable par un circuit arithmétique de taille polynomiale ?

En d'autres termes, l'utilisation d'opérations booléennes autres que $+$ et $\times$ permet-elle d'accélérer le calcul de manière superpolynomiale ?

Une question de Papadimitriou

Question ♣

Si un polynôme P est évalué par un algorithme en temps polynomial, est-il vrai qu'il est calculable par un circuit arithmétique de taille polynomiale ?

En d'autres termes, l'utilisation d'opérations booléennes autres que $+$ et $\times$ permet-elle d'accélérer le calcul de manière superpolynomiale ?

- Utilisation de familles de polynômes pour donner sens à ces questions.

Divisions

- Strassen : on peut se passer de divisions dans les circuits arithmétiques, si le polynôme a un degré polynomial.
- Idée : remplacer $\frac{1}{1-g(x)}$ par $1 + g(x) + g(x)^2 + \cdots + g(x)^{p(n)}$.

Divisions

- Strassen : on peut se passer de divisions dans les circuits arithmétiques, si le polynôme a un degré polynomial.
- Idée : remplacer $\frac{1}{1-g(x)}$ par $1 + g(x) + g(x)^2 + \cdots + g(x)^{p(n)}$.

- Qu'en est-il si le degré n'est pas polynomial ?

Discussion

- Pour montrer que la question ♣ a une réponse négative, on cherche un polynôme P qu'on puisse évaluer en temps polynomial mais qu'on ne puisse pas calculer par un circuit de taille polynomiale.

Discussion

- Pour montrer que la question ♣ a une réponse négative, on cherche un polynôme P qu'on puisse évaluer en temps polynomial mais qu'on ne puisse pas calculer par un circuit de taille polynomiale.

  Mais pas de candidats : les exemples usuels ne fonctionnent pas (déterminant, permanent, etc.).

Discussion

- Pour montrer que la question ♣ a une réponse négative, on cherche un polynôme P qu'on puisse évaluer en temps polynomial mais qu'on ne puisse pas calculer par un circuit de taille polynomiale.

  Mais pas de candidats : les exemples usuels ne fonctionnent pas (déterminant, permanent, etc.).

- Pour montrer que la question ♣ a une réponse positive, on cherche à transformer un algorithme d'évaluation en un circuit arithmétique.

Résultat principal

Si la question ♣ a une réponse négative, alors $\mathrm{VP} \neq \mathrm{VNP}$.

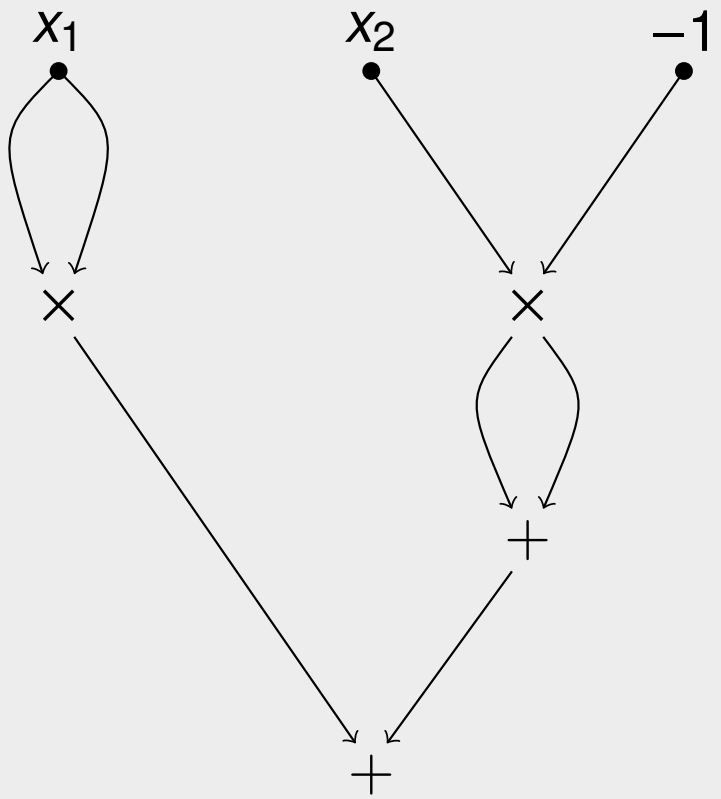
Plan

Plan

Circuits arithmétiques

Circuits arithmétiques :

- portes $+$ et $\times$
- entrées $x_1, \ldots, x_n$ et la constante -1
- $\rightarrow$ polynôme à plusieurs variables et à coefficients entiers.



Avertissement

Nous passerons sous le tapis le problème des constantes et de l'uniformité. . .

- Famille de polynômes (f_n) : un circuit C_n par polynôme $f_n \in \mathbb{Z}[x_1, \ldots, x_{u(n)}]$.

- Famille de polynômes (f_n) : un circuit C_n par polynôme $f_n \in \mathbb{Z}[x_1, \ldots, x_{u(n)}]$.

- VP : familles de polynômes de degré polynomial calculés par des circuits arithmétiques de taille polynomiale.
  Exemple : le déterminant

$$\det_n(x_{1,1}, \ldots, x_{1,n}, x_{2,1}, \ldots, x_{n,n}) = \sum_{\sigma \in \mathcal{S}_n} \epsilon(\sigma) \prod_{i=1}^{n} x_{i,\sigma(i)}.$$

- VNP : somme exponentielle de famille VP. Plus précisément, $(g_n) \in \mathrm{VNP}$ s'il existe $(f_n(x_1, \ldots, x_{u(n)}, y_1, \ldots, y_{p(n)})) \in \mathrm{VP}$ tel que

$$g_n(x_1, \ldots, x_{u(n)}) = \sum_{\bar{\epsilon} \in \{0,1\}^{p(n)}} f_n(\bar{x}, \bar{\epsilon})$$

Exemple : le permanent (VNP-complet)

$$\mathrm{per}_n(x_{1,1}, \ldots, x_{1,n}, x_{2,1}, \ldots, x_{n,n}) = \sum_{\sigma \in \mathcal{S}_n} \prod_{i=1}^{n} x_{i,\sigma(i)}.$$

Plan

Classes de comptage

- Langages (PP) ou fonctions ($\sharp\mathrm{P}$). On va s'intéresser aux langages (i.e. sous-ensembles de $\cup_{n\geq 0}\{0,1\}^n$).

Classes de comptage

- Langages (PP) ou fonctions ($\sharp\mathrm{P}$). On va s'intéresser aux langages (i.e. sous-ensembles de $\cup_{n\geq 0}\{0,1\}^n$).

- Compter le nombre d'éléments vérifiant une propriété décidable en temps polynomial :
  une fonction $f : \{0,1\}^* \to \mathbb{N}$ est dans $\sharp\mathrm{P}$ s'il existe un langage $B \in \mathrm{P}$ et un polynôme p tel que

$$f(x) = \#\{y \in \{0,1\}^{p(|x|)} \mid (x,y) \in B\}.$$

Classes de comptage

- Langages (PP) ou fonctions ($\sharp\mathrm{P}$). On va s'intéresser aux langages (i.e. sous-ensembles de $\cup_{n\geq 0}\{0,1\}^n$).

- Compter le nombre d'éléments vérifiant une propriété décidable en temps polynomial :
  une fonction $f : \{0,1\}^* \to \mathbb{N}$ est dans $\sharp\mathrm{P}$ s'il existe un langage $B \in \mathrm{P}$ et un polynôme p tel que

$$f(x) = \#\{y \in \{0,1\}^{p(|x|)} \mid (x,y) \in B\}.$$

- Décider si plus de la moitié des éléments satisfont une propriété décidable en temps polynomial :
  un langage A est dans PP s'il existe un langage $B \in \mathrm{P}$ et un polynôme p tel que

$$x \in B \iff \#\{y \in \{0,1\}^{p(|x|)} \mid (x,y) \in B\} \geq 2^{p(|x|)-1}.$$

Hiérarchie de comptage

- Opérateur de majorité **C** : si C est une classe de complexité, savoir si plus de la moitié des éléments satisfont une propriété décidable dans C.

Hiérarchie de comptage

- Opérateur de majorité **C** : si $\mathcal{C}$ est une classe de complexité, savoir si plus de la moitié des éléments satisfont une propriété décidable dans $\mathcal{C}$.

  C.$\mathcal{C}$ est l'ensemble des langages A tels qu'il existe un langage $B \in \mathcal{C}$ vérifiant :

$$x \in A \iff \#\{y \in \{0,1\}^{p(|x|)} \mid (x,y) \in B\} \geq 2^{p(|x|)-1}.$$

- $C_0P = \mathrm{P}$ et $C_{i+1}P = \mathbf{C}.C_iP$. Alors $\mathrm{CH} = \cup_i C_iP$.

Hiérarchie de comptage

- Opérateur de majorité **C** : si C est une classe de complexité, savoir si plus de la moitié des éléments satisfont une propriété décidable dans C.

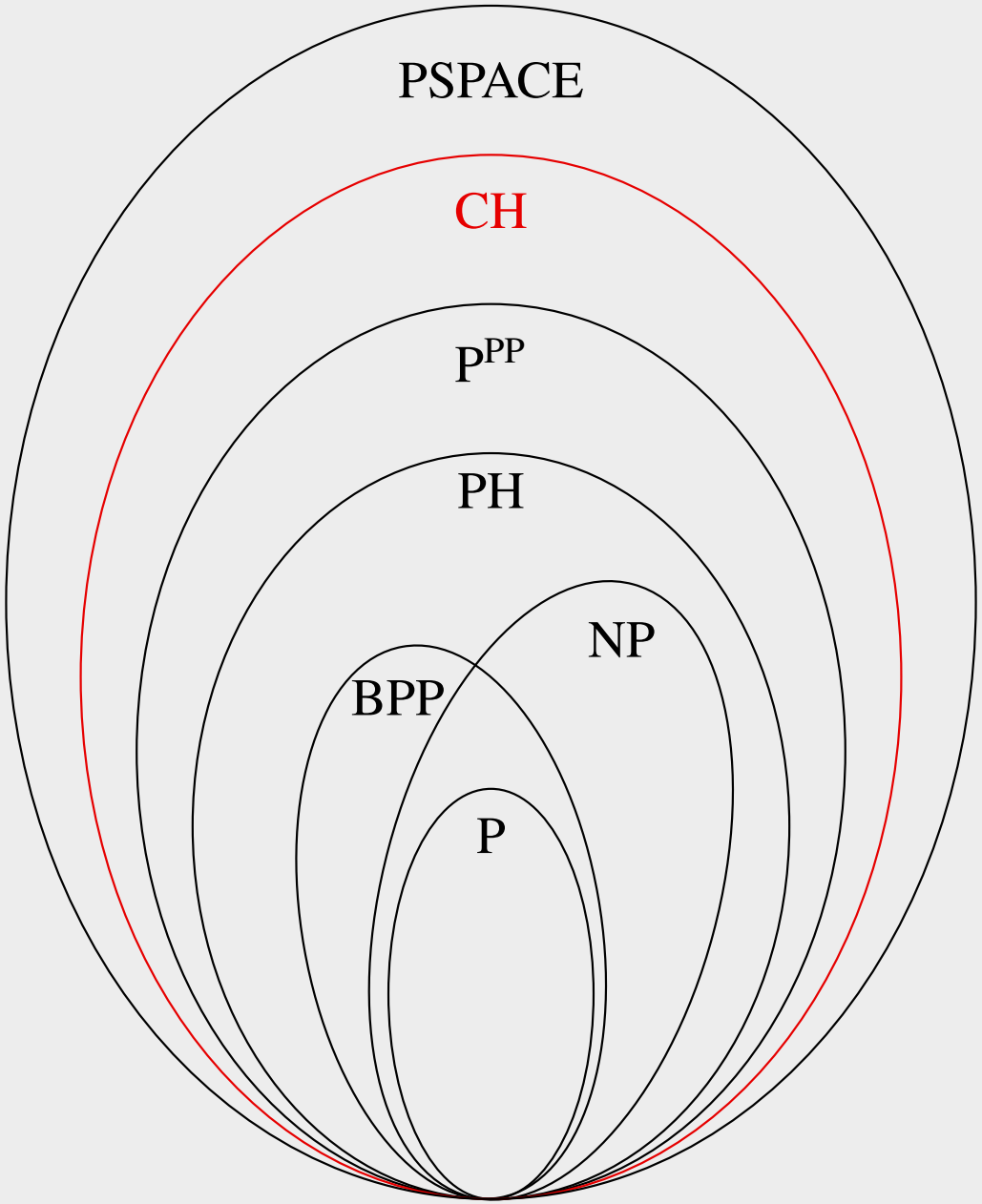
  C.C est l'ensemble des langages A tels qu'il existe un langage $B \in C$ vérifiant :

$$x \in A \iff \#\{y \in \{0,1\}^{p(|x|)} \mid (x,y) \in B\} \geq 2^{p(|x|)-1}.$$

- $C_0P = \mathrm{P}$ et $C_{i+1}P = \mathbf{C}.C_iP$. Alors $\mathrm{CH} = \cup_i C_iP$.

- Remarque : le permanent est complet pour PP.

Quelques inclusions



Un lemme central

Lemme

Si $\mathrm{VP} = \mathrm{VNP}$ *alors* $\mathrm{CH} = \mathrm{P}$*.*

Preuve (idée)

Si $\mathrm{VP} = \mathrm{VNP}$ alors le permanent a des circuits de taille polynomiale. Donc on peut l'évaluer en temps polynomial. Puisque le permanent est PP-complet, on obtient $\mathrm{PP} = \mathrm{P}$, d'où $\mathrm{CH} = \mathrm{P}$. □

Définition

Une suite d'entiers $(a_{n,k})_{k \leq 2^{p(n)}}$ *de taille exponentielle est calculable dans* CH *si*

$$\{(1^n, k, j, b) \mid \textit{le } j\textit{-ème bit de } a_{n,k} \textit{ est } b\} \in \mathrm{CH}.$$

On sait calculer les bits de $(a_{n,k})$ dans la hiérarchie de comptage.

Théorème (Bürgisser)

Si $(a_{n,k})$ *est calculable dans* CH*, alors c'est aussi le cas de*

$$c_n = \sum_{k=0}^{2^{p(n)}} a(n,k) \quad \textit{et} \quad d_n = \prod_{k=0}^{2^{p(n)}} a(n,k).$$

Preuve (idée)

Ingrédient clé : l'addition et la multiplication itérées sont dans LOGTIME-uniforme TC^0 (résultat récent de Hesse, Allender et Barrington pour la multiplication).

TC^0 : circuits de taille polynomiale et de profondeur constante avec portes de majorité.

LOGTIME-uniforme : condition d'uniformité très forte. □

Plan

Résultat principal (bis)

Si la question ♣ a une réponse négative, alors $\mathrm{VP} \neq \mathrm{VNP}$.

Résultat principal (bis)

Si la question ♣ a une réponse négative, alors $\mathrm{VP} \neq \mathrm{VNP}$.

En d'autres termes, si $\mathrm{VP} = \mathrm{VNP}$ alors la question ♣ a une réponse positive : on sait transformer un algorithme d'évaluation en un circuit arithmétique.

Des outils rangés dans Lagrange

Passer de l'évaluation aux points entiers au calcul : interpolation de Lagrange.

Passer de l'évaluation aux points entiers au calcul : interpolation de Lagrange.

Lemme (interpolation de Lagrange)

Soit $p(x)$ un polynôme en une variable de degré $\leq d$. Alors

$$p(x) = \sum_{i=0}^{d} p(i) \prod_{j \neq i} \frac{x-j}{i-j},$$

où l'entier j varie de 0 à d.

Preuve

Les deux polynômes sont de degré $\leq d$ et coïncident sur $d+1$ points. □

Lemme

Soit $p(x_1, \ldots, x_n)$ un polynôme de degré $\leq d$. Alors

$$p(x_1, \ldots, x_n) = \sum_{0 \leq i_1, \ldots, i_n \leq d} p(i_1, \ldots, i_n) \prod_{k=1}^{n} \left(\prod_{j_k \neq i_k} \frac{x_k - j_k}{i_k - j_k} \right),$$

où les entiers j_k varient de 0 à d.

Résultat principal (ter)

Définition

Soit $(f_n(x_1, \ldots, x_{u(n)}))$ *une famille de polynômes. On dit que* (f_n) *est évaluable dans* CH *aux points entiers si*

$$\{(1^n, i_1, \ldots, i_{u(n)}, j, b) \mid \textit{le } j\textit{-ème bit de } f_n(i_1, \ldots, i_{u(n)}) \textit{ est } b\} \in \mathrm{CH}.$$

On sait calculer $f_n(i_1, \ldots, i_{u(n)})$ bit par bit dans la hiérarchie de comptage.

Résultat principal (ter)

Définition

Soit $(f_n(x_1, \ldots, x_{u(n)}))$ *une famille de polynômes. On dit que* (f_n) *est évaluable dans* CH *aux points entiers si*

$$\{(1^n, i_1, \ldots, i_{u(n)}, j, b) \mid \textit{le } j\textit{-ème bit de } f_n(i_1, \ldots, i_{u(n)}) \textit{ est } b\} \in \mathrm{CH}.$$

On sait calculer $f_n(i_1, \ldots, i_{u(n)})$ bit par bit dans la hiérarchie de comptage.

Nous allons montrer que :

(si $\mathrm{VP} = \mathrm{VNP}$ et f est évaluable dans CH aux points entiers)
alors f a un circuit de taille polynomiale

Critère de Valiant

Définition $\mathrm{VP}_{\mathrm{nb}}$: idem VP mais sans la contrainte de degré polynomial

$\longrightarrow$ familles de polynômes calculées par circuits de taille polynomiale.

Définition $\mathrm{VP_{nb}}$: idem VP mais sans la contrainte de degré polynomial
$\longrightarrow$ familles de polynômes calculées par circuits de taille polynomiale.

Lemme

Soit

$$f_n(x_1, \ldots, x_n) = \sum_{\alpha^{(1)},\ldots,\alpha^{(n)}} a(n, \alpha^{(1)}, \ldots, \alpha^{(n)}) x_1^{\alpha^{(1)}} \cdots x_n^{\alpha^{(n)}},$$

où $a(n, \alpha^{(1)}, \ldots, \alpha^{(n)})$ *est une suite d'entiers calculable dans* CH.
Si $\mathrm{VP} = \mathrm{VNP}$ *alors* $(f_n) \in \mathrm{VP_{nb}}$.

Théorème principal

Théorème

Soit $(f_n(x_1, \ldots, x_{u(n)}))$ *une famille de polynômes à plusieurs variables. Supposons que* (f_n) *puisse être évaluée dans* CH *aux points entiers. Si* $\mathrm{VP} = \mathrm{VNP}$ *alors* $(f_n) \in \mathrm{VP}_{\mathrm{nb}}$.

Théorème

Soit $(f_n(x_1, \ldots, x_{u(n)}))$ *une famille de polynômes à plusieurs variables. Supposons que* (f_n) *puisse être évaluée dans* CH *aux points entiers. Si* $\mathrm{VP} = \mathrm{VNP}$ *alors* $(f_n) \in \mathrm{VP}_{\mathrm{nb}}$.

Preuve (idée)

- Par les résultats de Bürgisser, on peut calculer les coefficients du polynôme d'interpolation de Lagrange dans CH.
- Par le critère de Valiant, si $\mathrm{VP} = \mathrm{VNP}$ alors $(f_n) \in \mathrm{VP}_{\mathrm{nb}}$. □

Récapitulatif

- Sous l'hypothèse $\mathrm{VP} = \mathrm{VNP}$, on veut montrer qu'une famille « facilement évaluable » possède des circuits de taille polynomiale.

Récapitulatif

- Sous l'hypothèse $\mathrm{VP} = \mathrm{VNP}$, on veut montrer qu'une famille « facilement évaluable » possède des circuits de taille polynomiale.

- Idée : utiliser l'interpolation de Lagrange (permet de passer de l'évaluation au polynôme lui-même).

Récapitulatif

- Sous l'hypothèse $\mathrm{VP} = \mathrm{VNP}$, on veut montrer qu'une famille « facilement évaluable » possède des circuits de taille polynomiale.

- Idée : utiliser l'interpolation de Lagrange (permet de passer de l'évaluation au polynôme lui-même).

- Points techniques :
  - critère de Valiant : si on sait calculer les coefficients dans CH, alors le polynôme a des circuits de taille polynomiale (sous l'hypothèse $\mathrm{VP} = \mathrm{VNP}$)
  - résultat de Bürgisser permettant de calculer dans CH les coefficients du polynôme d'interpolation.

Plan

Conséquence pour la question ♣

Théorème

Si la question ♣ a une réponse négative, alors $\mathrm{VP} \neq \mathrm{VNP}$.

Remarque : si la question ♣ a une réponse positive, alors $\mathrm{P} = \mathrm{PP} \Rightarrow \mathrm{VP} = \mathrm{VNP}$.

Versions bornées ou non-bornées

Théorème

(Dans un contexte sans constante)

$$\mathrm{VP} = \mathrm{VNP} \Rightarrow \mathrm{VP}_{\mathrm{nb}} = \mathrm{VNP}_{\mathrm{nb}}.$$

Remarque : sur les corps de caractéristique non nulle, le résultat a été montré par Malod (2003).

Transfert vers BSS

- Versions algébriques de P et NP : modèle de Blum, Shub et Smale.
- Sur un corps K de caractéristique nulle, opérations $+$, $\times$ et $=$.

Transfert vers BSS

- Versions algébriques de P et NP : modèle de Blum, Shub et Smale.
- Sur un corps K de caractéristique nulle, opérations $+$, $\times$ et $=$.
- Séparation de P_K et NP_K grâce à des problèmes de $\mathrm{NP}_{(K,+,=)}$? (Twenty Questions, Subset Sum, . . .)

Théorème

$\mathrm{VP} = \mathrm{VNP} \Rightarrow \mathrm{NP}_{(K,+,=)} \subseteq \mathrm{P}_{(K,+,\times,=)}$.

On passe par des produits de taille exponentielle.

Conclusion

- La question ♣ est centrale mais difficile : si réponse positive, résultat de transfert ; sinon, séparation de VP et VNP.

Conclusion

- La question ♣ est centrale mais difficile : si réponse positive, résultat de transfert ; sinon, séparation de VP et VNP.

- Peu d'intuition concernant la réponse.

Conclusion

- La question ♣ est centrale mais difficile : si réponse positive, résultat de transfert ; sinon, séparation de VP et VNP.
- Peu d'intuition concernant la réponse.
- Des candidats pour une réponse négative ? (des polynômes que l'on peut évaluer facilement mais qui n'ont pas de circuits de taille polynomiale)