Versions algébriques de la question « $\mathrm{P} = \mathrm{PSPACE}$? »

Pascal Koiran Sylvain Perifel

LIP, ENS Lyon

Le 27 février 2007

Introduction

- Problèmes de décision
  Langages (sur $\mathbb{R}$), modèle de Blum-Shub-Smale
  Exemple : décider si un polynôme à plusieurs variables a une racine réelle ($\mathrm{NP}_{\mathbb{R}}$-complet)

Introduction

- Problèmes de décision
  Langages (sur $\mathbb{R}$), modèle de Blum-Shub-Smale
  Exemple : décider si un polynôme à plusieurs variables a une racine réelle ($\mathrm{NP}_{\mathbb{R}}$-complet)

- Problèmes d'évaluation
  Familles de polynômes, modèle de Valiant
  Exemple : calculer le permanent d'une matrice
  (VNP-complet)

Plan

1. P et PSPACE
2. P et PSPACE dans le modèle BSS
3. P et PSPACE dans le modèle de Valiant
4. Conditions de signe
5. Un vecteur orthogonal

si $\mathrm{VP} = \mathrm{VPSPACE}$ alors $\mathrm{P}_{\mathbb{R}} = \mathrm{PAR}_{\mathbb{R}}$

P et PSPACE

- Classe P : langages sur $\{0,1\}$ reconnus par machine de Turing déterministe en temps polynomial.
- Classe PSPACE : langages sur $\{0,1\}$ reconnus par machine de Turing en espace polynomial.

P et PSPACE

- Classe P : langages sur $\{0,1\}$ reconnus par machine de Turing déterministe en temps polynomial.
- Classe PSPACE : langages sur $\{0,1\}$ reconnus par machine de Turing en espace polynomial.

- Machines de Turing $\longleftrightarrow$ circuits booléens (portes $\wedge$, $\vee$, $\neg$).
- Reconnaissance de langages : un circuit par taille d'entrée.

P et PSPACE

- Classe P : langages sur $\{0,1\}$ reconnus par machine de Turing déterministe en temps polynomial.
- Classe PSPACE : langages sur $\{0,1\}$ reconnus par machine de Turing en espace polynomial.

- Machines de Turing $\longleftrightarrow$ circuits booléens (portes $\wedge$, $\vee$, $\neg$).
- Reconnaissance de langages : un circuit par taille d'entrée.
- Classe P : langages reconnus par circuits booléens de taille polynomiale ($+$ uniformité).
- Classe PSPACE : langages reconnus par circuits booléens de *profondeur* polynomiale (taille éventuellement exponentielle) ($+$ uniformité).

P et PSPACE dans le modèle BSS

- Circuits algébriques : portes $+$, $-$, $\times$ et $\leq$.
- Langages sur $\mathbb{R}$: ensemble de mots sur l'alphabet $\mathbb{R}$, i.e. $A \subseteq \cup_{n \geq 0} \mathbb{R}^n$.
- Reconnaissance de langages sur $\mathbb{R}$: un circuit par taille d'entrée.

P et PSPACE dans le modèle BSS

- Circuits algébriques : portes $+$, $-$, $\times$ et $\leq$.
- Langages sur $\mathbb{R}$: ensemble de mots sur l'alphabet $\mathbb{R}$, i.e. $A \subseteq \cup_{n \geq 0} \mathbb{R}^n$.
- Reconnaissance de langages sur $\mathbb{R}$: un circuit par taille d'entrée.
- Classe $\mathrm{P}_{\mathbb{R}}$: langages sur $\mathbb{R}$ reconnus par circuits algébriques de taille polynomiale ($+$ uniformité).

P et PSPACE dans le modèle BSS

- Circuits algébriques : portes $+$, $-$, $\times$ et $\leq$.
- Langages sur $\mathbb{R}$: ensemble de mots sur l'alphabet $\mathbb{R}$, i.e. $A \subseteq \cup_{n \geq 0} \mathbb{R}^n$.
- Reconnaissance de langages sur $\mathbb{R}$: un circuit par taille d'entrée.
- Classe $\mathrm{P}_{\mathbb{R}}$: langages sur $\mathbb{R}$ reconnus par circuits algébriques de taille polynomiale ($+$ uniformité).
- Classe $\mathrm{PAR}_{\mathbb{R}}$: langages sur $\mathbb{R}$ reconnus par circuits algébriques de *profondeur* polynomiale (taille éventuellement exponentielle) ($+$ uniformité).

P et PSPACE dans le modèle de Valiant

- Circuits arithmétiques : portes $+$, $-$ et $\times$, entrées $x_1, \ldots, x_n$ et constante $1 \longrightarrow$ calcul d'un polynôme à coefficients entiers.
- Famille de polynômes (f_n) : un circuit C_n par polynôme $f_n \in \mathbb{Z}[x_1, \ldots, x_{u(n)}]$.

P et PSPACE dans le modèle de Valiant

- Circuits arithmétiques : portes $+$, $-$ et $\times$, entrées $x_1, \ldots, x_n$ et constante $1 \longrightarrow$ calcul d'un polynôme à coefficients entiers.
- Famille de polynômes (f_n) : un circuit C_n par polynôme $f_n \in \mathbb{Z}[x_1, \ldots, x_{u(n)}]$.
- Classe VP : familles de polynômes calculés par circuits arithmétiques de taille polynomiale (+ uniformité).

$$(= \text{Uniform } \mathrm{VP}^0_{\mathrm{nb}})$$

P et PSPACE dans le modèle de Valiant

- Circuits arithmétiques : portes $+$, $-$ et $\times$, entrées $x_1, \ldots, x_n$ et constante $1 \longrightarrow$ calcul d'un polynôme à coefficients entiers.
- Famille de polynômes (f_n) : un circuit C_n par polynôme $f_n \in \mathbb{Z}[x_1, \ldots, x_{u(n)}]$.
- Classe VP : familles de polynômes calculés par circuits arithmétiques de taille polynomiale (+ uniformité).

  $(= \mathrm{Uniform}\ \mathrm{VP}^0_{\mathrm{nb}})$
- Classe $\mathrm{VPSPACE}$: familles de polynômes calculés par circuits arithmétiques de *profondeur* polynomiale (+ uniformité).

Récapitulatif

- Problèmes de décision sur $\{0, 1\}$: circuits booléens (portes $\wedge$, $\vee$ et $\neg$).
- Problèmes de décision sur $\mathbb{R}$ (BSS) : circuits algébriques (portes $+$, $-$, $\times$, $\leq$).
- Problèmes d'évaluation (Valiant) : circuits arithmétiques (portes $+$, $-$, $\times$).

Récapitulatif

- Problèmes de décision sur $\{0,1\}$: circuits booléens (portes $\wedge$, $\vee$ et $\neg$).
- Problèmes de décision sur $\mathbb{R}$ (BSS) : circuits algébriques (portes $+$, $-$, $\times$, $\leq$).
- Problèmes d'évaluation (Valiant) : circuits arithmétiques (portes $+$, $-$, $\times$).

- Classe P : circuits de taille polynomiale.
- Classe PSPACE : circuits de profondeur polynomiale.

Autres caractérisations de $\mathrm{VPSPACE}$

- Définition originale : fonction coefficient PSPACE.

$$f_n(\bar{x}) = \sum_{\alpha} a(\alpha)\bar{x}^{\alpha}$$

Fonction $a : \{0,1\}^* \to \mathbb{Z}$ calculable chiffre par chiffre en espace polynomial.

Autres caractérisations de $\mathrm{VPSPACE}$

- Définition originale : fonction coefficient PSPACE.

$$f_n(\bar{x}) = \sum_{\alpha} a(\alpha)\bar{x}^{\alpha}$$

  Fonction $a : \{0,1\}^* \to \mathbb{Z}$ calculable chiffre par chiffre en espace polynomial.

- Poizat : circuits de taille polynomiale munis de portes de sommes exponentielles

Autres caractérisations de $\mathrm{VPSPACE}$

- Définition originale : fonction coefficient PSPACE.

$$f_n(\bar{x}) = \sum_{\alpha} a(\alpha)\bar{x}^{\alpha}$$

  Fonction $a : \{0,1\}^* \to \mathbb{Z}$ calculable chiffre par chiffre en espace polynomial.

- Poizat : circuits de taille polynomiale munis de portes de sommes exponentielles
  ou de portes d'évaluation en 0 et 1.

Autres caractérisations de $\mathrm{VPSPACE}$

- Définition originale : fonction coefficient PSPACE.

$$f_n(\bar{x}) = \sum_{\alpha} a(\alpha)\bar{x}^{\alpha}$$

  Fonction $a : \{0,1\}^* \to \mathbb{Z}$ calculable chiffre par chiffre en espace polynomial.
- Poizat : circuits de taille polynomiale munis de portes de sommes exponentielles
  ou de portes d'évaluation en 0 et 1.
- Exemple : résultant d'un système de polynômes à plusieurs variables.

Théorème de transfert

$$\text{Si } \mathrm{VPSPACE} = \mathrm{VP} \text{ alors } \mathrm{PAR}_{\mathbb{R}} = \mathrm{P}_{\mathbb{R}}.$$

Plan de la preuve :

- On prend $A \in \mathrm{PAR}_{\mathbb{R}}$ et on veut décider en temps polynomial si $\bar{x} \in A$.
- Trouver la condition de signe de $\bar{x}$

- Simuler le circuit sur cette condition de signe.

Théorème de transfert

$$\text{Si } \mathrm{VPSPACE} = \mathrm{VP} \text{ alors } \mathrm{PAR}_{\mathbb{R}} = \mathrm{P}_{\mathbb{R}}.$$

Plan de la preuve :

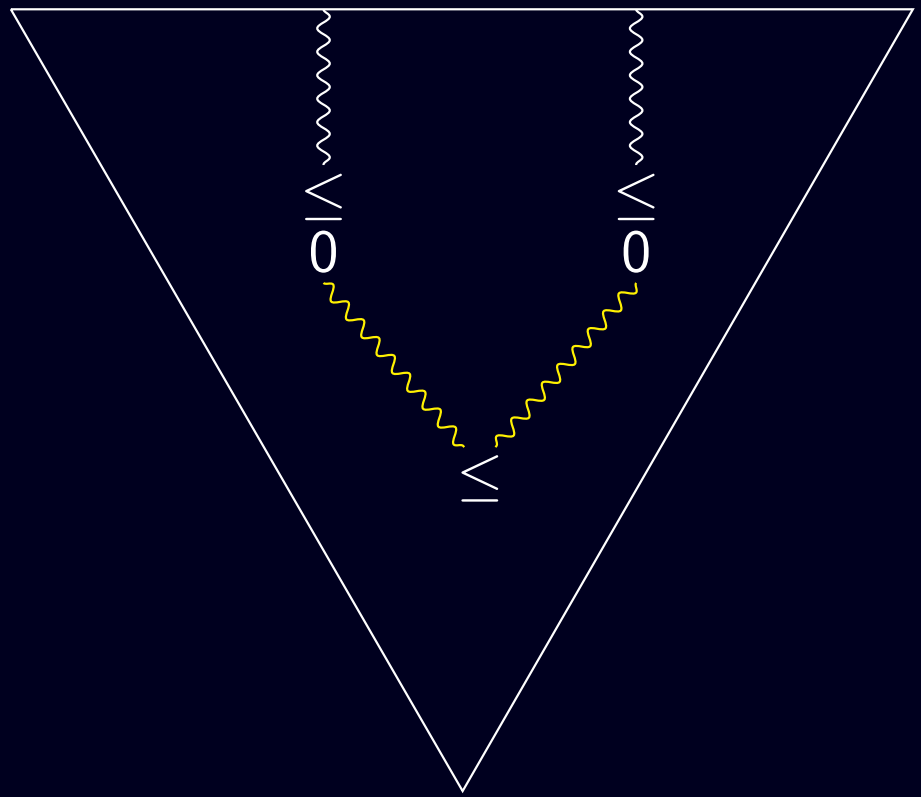
- On prend $A \in \mathrm{PAR}_{\mathbb{R}}$ et on veut décider en temps polynomial si $\bar{x} \in A$.
- Trouver la condition de signe de $\bar{x}$
  - énumération des conditions de signe satisfaisables (Renegar) ;
  - recherche dichotomique (vecteur orthogonal).
- Simuler le circuit sur cette condition de signe.

Polynômes testés par un circuit

Porte de test :
$f(\bar{x}) \leq 0$?

Si les résultats des tests précédents sont fixés, f est un polynôme.

$\longrightarrow$ énumération de tous les polynômes possibles (espace polynomial) : famille $f_1, \ldots, f_s$.

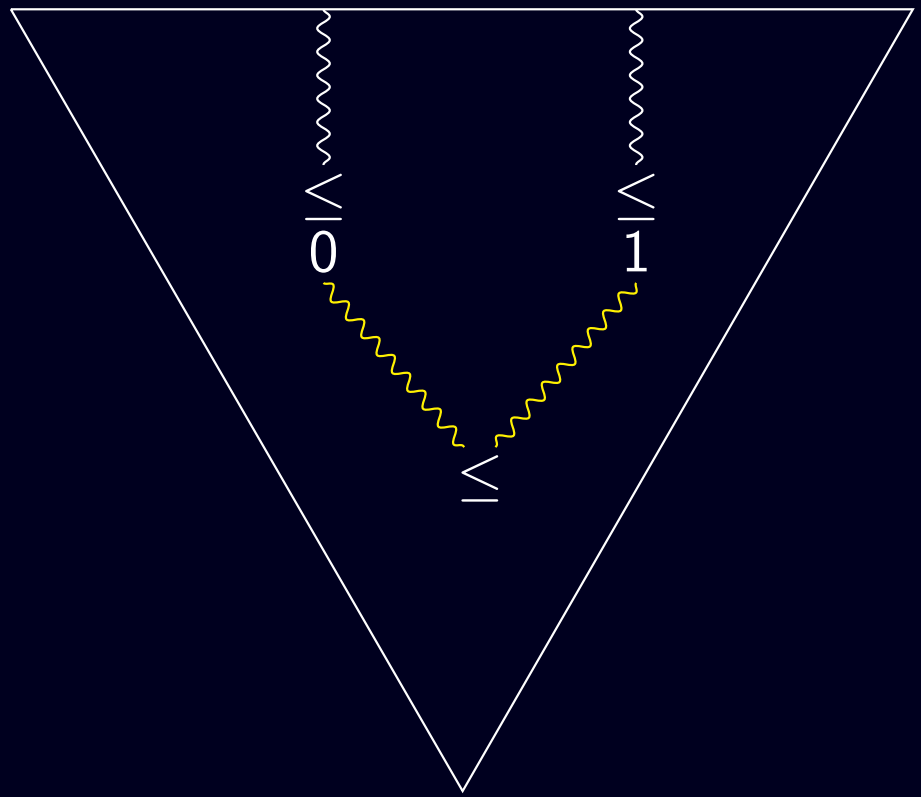


Polynômes testés par un circuit

Porte de test :
$f(\bar{x}) \leq 0$?

Si les résultats des tests précédents sont fixés, f est un polynôme.

$\longrightarrow$ énumération de tous les polynômes possibles (espace polynomial) : famille $f_1, \ldots, f_s$.



Conditions de signe

- Condition de signe $S \in \{-1, 0, 1\}^s$: signe des polynômes $f_1, \ldots, f_s$.
- Condition de signe de $\bar{x}$: $(\mathrm{sign}(f_1(\bar{x})), \ldots, \mathrm{sign}(f_s(\bar{x})))$.

Conditions de signe

- Condition de signe $S \in \{-1, 0, 1\}^s$: signe des polynômes $f_1, \ldots, f_s$.
- Condition de signe de $\bar{x}$: $(\mathrm{sign}(f_1(\bar{x})), \ldots, \mathrm{sign}(f_s(\bar{x})))$.

- Si $\bar{x}$ et $\bar{y}$ ont la même condition de signe alors tous les tests donnent le même résultat $\longrightarrow$ $\bar{x}$ et $\bar{y}$ sont simultanément dans le langage ou hors du langage.
- Il suffit d'étudier la condition de signe (objet booléen).

Conditions de signe satisfaisables

- Condition de signe $S \in \{-1, 0, 1\}^s$: signe des polynômes $f_1, \ldots, f_s$.
- Toutes les conditions de signe ne sont pas satisfaisables.
- Exemple : $x^2 + 1$ donne toujours 1 (toujours positif sur $\mathbb{R}$).

Conditions de signe satisfaisables

- Condition de signe $S \in \{-1, 0, 1\}^s$: signe des polynômes $f_1, \ldots, f_s$.
- Toutes les conditions de signe ne sont pas satisfaisables.
- Exemple : $x^2 + 1$ donne toujours 1 (toujours positif sur $\mathbb{R}$).

Théorème (Thom-Milnor 1964, Grigoriev 1988, Renegar 1992)

- *Il y a $N = (sd)^{O(n)}$ conditions de signe satisfaisables (s : nombre de polynômes, n : nombre de variables, d : degré max).*
- *On peut énumérer les conditions de signes satisfaisables dans* PSPACE.

Trouver la condition de signe partielle

- On s'intéresse seulement à savoir si c'est $= 0$ ou $\neq 0$.
- On ordonne les css partielles « par inclusion » :

Trouver la condition de signe partielle

- On s'intéresse seulement à savoir si c'est $= 0$ ou $\neq 0$.
- On ordonne les css partielles « par inclusion » :

- On cherche la css minimale S qui satisfait

$$\forall k \leq s, S_k = 0 \Longrightarrow f_k(\bar{x}) = 0.$$

Trouver la condition de signe partielle

- On s'intéresse seulement à savoir si c'est $= 0$ ou $\neq 0$.
- On ordonne les css partielles « par inclusion » :

- On cherche la css minimale S qui satisfait

$$\forall k \leq s, S_k = 0 \Longrightarrow f_k(\bar{x}) = 0.$$

- Recherche dichotomique grâce aux tests $\mathrm{VPSPACE}$

$$\prod_{j \leq i} \left(\sum_{S_k^{(j)}=0} f_k(\bar{x})^2 \right) = 0 \quad \text{(vrai ssi } S \leq i\text{)}$$

Trouver la condition de signe partielle

- On s'intéresse seulement à savoir si c'est $= 0$ ou $\neq 0$.
- On ordonne les css partielles « par inclusion » :

- On cherche la css minimale S qui satisfait

$$\forall k \leq s, S_k = 0 \Longrightarrow f_k(\bar{x}) = 0.$$

- Recherche dichotomique grâce aux tests $\mathrm{VPSPACE}$

$$\prod_{j \leq i} \left(\sum_{S_k^{(j)}=0} f_k(\bar{x})^2 \right) = 0 \quad \text{(vrai ssi } S \leq i\text{)}$$

Trouver la condition de signe partielle

- On s'intéresse seulement à savoir si c'est $= 0$ ou $\neq 0$.
- On ordonne les css partielles « par inclusion » :

- On cherche la css minimale S qui satisfait

$$\forall k \leq s, S_k = 0 \Longrightarrow f_k(\bar{x}) = 0.$$

- Recherche dichotomique grâce aux tests $\mathrm{VPSPACE}$

$$\prod_{j \leq i} \left(\sum_{S_k^{(j)}=0} f_k(\bar{x})^2 \right) = 0 \quad \text{(vrai ssi } S \leq i\text{)}$$

Trouver la condition de signe partielle

- On s'intéresse seulement à savoir si c'est $= 0$ ou $\neq 0$.
- On ordonne les css partielles « par inclusion » :

- On cherche la css minimale S qui satisfait

$$\forall k \leq s, S_k = 0 \Longrightarrow f_k(\bar{x}) = 0.$$

- Recherche dichotomique grâce aux tests $\mathrm{VPSPACE}$

$$\prod_{j \leq i} \left(\sum_{S_k^{(j)}=0} f_k(\bar{x})^2 \right) = 0 \quad \text{(vrai ssi } S \leq i\text{)}$$

Condition de signe complète

- On connaît la condition de signe partielle : on sait quels polynômes s'annulent. On cherche maintenant le signe des autres.
- Il n'y a pas d'ordre naturel dans lequel la cs serait un maximum.
- On va éliminer les candidats au fur et à mesure.

Recherche dichotomique

- Nouvelle convention : 0 pour positif et 1 pour négatif.
- « Produit scalaire » sur $\{0,1\}^s$: $u.v = \sum_{i=1}^{s} u_i v_i \mod 2$.
- Soit S la condition de signe de $\bar{x}$. Soit $u \in \{0,1\}^s$. On a :

$$u.S = 1 \iff \prod_{i|u_i=1} f_i(\bar{x}) < 0$$

Recherche dichotomique

- Nouvelle convention : 0 pour positif et 1 pour négatif.
- « Produit scalaire » sur $\{0,1\}^s$: $u.v = \sum_{i=1}^{s} u_i v_i \mod 2$.
- Soit S la condition de signe de $\bar{x}$. Soit $u \in \{0,1\}^s$. On a :

$$u.S = 1 \iff \prod_{i|u_i=1} f_i(\bar{x}) < 0$$

- Si u est orthogonal à environ la moitié des css, alors on a « éliminé » environ la moitié des candidats.
  $\longrightarrow$ On répète un nombre logarithmique de fois.

Récapitulatif

Pour montrer que $\mathrm{VPSPACE} = \mathrm{VP} \Rightarrow \mathrm{PAR}_{\mathbb{R}} = \mathrm{P}_{\mathbb{R}}$:

- On prend $A \in \mathrm{PAR}_{\mathbb{R}}$ et on veut décider en temps polynomial si $\bar{x} \in A$.
- On énumère tous les polynômes pouvant être testés dans le cricuit (faisable en espace polynomial).
- Grâce à des tests $\mathrm{VPSPACE}$, on trouve par recherche dichotomique (recherche d'un maximum) la condition de signe partielle de $\bar{x}$.
- Pour trouver la condition de signe complète de $\bar{x}$:
  - on s'est ramené à $\{0, 1\}$;
  - grâce au vecteur orthogonal et à des tests $\mathrm{VPSPACE}$ on élimine à chaque étape la moitié des cs candidates.
- Lorsqu'on a la cs de $\bar{x}$, on peut simuler le circuit et conclure.

Un vecteur orthogonal

Un vecteur orthogonal à environ la moitié d'une famille de vecteur

Pierre Charbit
Emmanuel Jeandel
Pascal Koiran
Sylvain Perifel
Stéphan Thomassé
2006

Un vecteur orthogonal

- Problème : on a une famille de vecteurs $S^{(1)}, \ldots, S^{(k)} \in \{0,1\}^s$. Trouver un vecteur orthogonal à environ la moitié des vecteurs $S^{(i)}$.

Un vecteur orthogonal

- Problème : on a une famille de vecteurs $S^{(1)}, \ldots, S^{(k)} \in \{0,1\}^s$. Trouver un vecteur orthogonal à environ la moitié des vecteurs $S^{(i)}$.
- Grigoriev 1998 : il existe toujours un vecteur orthogonal à au moins $k/3$ et au plus $2k/3$ vecteurs. Non-constructif.

Un vecteur orthogonal

- Problème : on a une famille de vecteurs $S^{(1)}, \ldots, S^{(k)} \in \{0,1\}^s$. Trouver un vecteur orthogonal à environ la moitié des vecteurs $S^{(i)}$.
- Grigoriev 1998 : il existe toujours un vecteur orthogonal à au moins $k/3$ et au plus $2k/3$ vecteurs. Non-constructif.
- CJKPT 2006 :
  - un vecteur au hasard $\longrightarrow$ intervalle $[k/2 - \sqrt{k}; k/2 + \sqrt{k}]$ avec probabilité $3/4$ (inégalité de Tchebycheff, toujours non-constructif) ;

Un vecteur orthogonal

- Problème : on a une famille de vecteurs $S^{(1)}, \ldots, S^{(k)} \in \{0,1\}^s$. Trouver un vecteur orthogonal à environ la moitié des vecteurs $S^{(i)}$.
- Grigoriev 1998 : il existe toujours un vecteur orthogonal à au moins $k/3$ et au plus $2k/3$ vecteurs. Non-constructif.
- CJKPT 2006 :
  - un vecteur au hasard $\longrightarrow$ intervalle $[k/2 - \sqrt{k}; k/2 + \sqrt{k}]$ avec probabilité $3/4$ (inégalité de Tchebycheff, toujours non-constructif) ;
  - on peut dérandomiser en parallèle (donc espace logarithmique).

Un argument probabiliste

Théorème

Il existe un vecteur u orthogonal à au moins $k/2 - \sqrt{k}/2$ vecteurs et au plus $k/2 + \sqrt{k}/2$:

$$-\sqrt{k}/2 \leq |\{i | u.S^{(i)} = 0\}| - k/2 \leq \sqrt{k}/2.$$

Un argument probabiliste

Théorème

Il existe un vecteur u orthogonal à au moins $k/2 - \sqrt{k}/2$ vecteurs et au plus $k/2 + \sqrt{k}/2$:

$$-\sqrt{k}/2 \leq |\{i | u.S^{(i)} = 0\}| - k/2 \leq \sqrt{k}/2.$$

Preuve On prend $u \in \{0,1\}^s$ aléatoire. Soit Y_i la variable aléatoire

$$Y_i = \begin{cases} 1 & \text{si } u.S^{(i)} = 0 \\ -1 & \text{sinon.} \end{cases}$$

Soit $Y = \sum_{i=1}^{k} Y_i$: on veut montrer qu'il existe u tel que

$$|Y| \leq \sqrt{k}, \text{ soit } Y^2 \leq k.$$

Un argument probabiliste – suite

Il est facile de montrer que :

- $P(Y_i = 1) = 1/2$ et $E(Y_i) = 0$;

Un argument probabiliste – suite

Il est facile de montrer que :

- $P(Y_i = 1) = 1/2$ et $E(Y_i) = 0$;
- $E(Y_i^2) = 1$;

Un argument probabiliste – suite

Il est facile de montrer que :

- $P(Y_i = 1) = 1/2$ et $E(Y_i) = 0$;
- $E(Y_i^2) = 1$;
- les événements $\{Y_i = 1\}$ sont deux-à-deux indépendants, donc $E(Y_i Y_j) = E(Y_i)E(Y_j) = 0$.

Un argument probabiliste – suite

Il est facile de montrer que :

- $P(Y_i = 1) = 1/2$ et $E(Y_i) = 0$;
- $E(Y_i^2) = 1$;
- les événements $\{Y_i = 1\}$ sont deux-à-deux indépendants, donc $E(Y_i Y_j) = E(Y_i)E(Y_j) = 0$.

On a donc :

$$E(Y^2) = E(\sum_{i=1}^{k} Y_i^2 + \sum_{i \neq j} Y_i Y_j) = k. \quad \square$$

Remarques

- La taille $\sqrt{k}$ de l'intervalle est « presque optimale » : il existe une famille de vecteurs $S^{(i)}$ pour laquelle tout vecteur u est à distance $\Omega(\sqrt{k}/(\log k)^{1/4})$ de $k/2$.

Remarques

- La taille $\sqrt{k}$ de l'intervalle est « presque optimale » : il existe une famille de vecteurs $S^{(i)}$ pour laquelle tout vecteur u est à distance $\Omega(\sqrt{k}/(\log k)^{1/4})$ de $k/2$.

- Si l'on choisi un vecteur aléatoire, il est dans l'intervalle $[k/2 - \sqrt{k}; k/2 + \sqrt{k}]$ avec probabilité $3/4$ (Tchebycheff, variance calculable par 2 à 2 indépendance des Y_i)
  $\longrightarrow$ algorithme randomisé trivial.

Remarques

- La taille $\sqrt{k}$ de l'intervalle est « presque optimale » : il existe une famille de vecteurs $S^{(i)}$ pour laquelle tout vecteur u est à distance $\Omega(\sqrt{k}/(\log k)^{1/4})$ de $k/2$.

- Si l'on choisi un vecteur aléatoire, il est dans l'intervalle $[k/2 - \sqrt{k}; k/2 + \sqrt{k}]$ avec probabilité $3/4$ (Tchebycheff, variance calculable par 2 à 2 indépendance des Y_i)
  $\longrightarrow$ algorithme randomisé trivial.

- On peut dérandomiser cet algorithme par la méthode des espérances conditionnelles
  $\longrightarrow$ algorithme déterministe polynomial (compliqué).

Remarques

- La taille $\sqrt{k}$ de l'intervalle est « presque optimale » : il existe une famille de vecteurs $S^{(i)}$ pour laquelle tout vecteur u est à distance $\Omega(\sqrt{k}/(\log k)^{1/4})$ de $k/2$.

- Si l'on choisi un vecteur aléatoire, il est dans l'intervalle $[k/2 - \sqrt{k}; k/2 + \sqrt{k}]$ avec probabilité $3/4$ (Tchebycheff, variance calculable par 2 à 2 indépendance des Y_i)
  $\longrightarrow$ algorithme randomisé trivial.

- On peut dérandomiser cet algorithme par la méthode des espérances conditionnelles
  $\longrightarrow$ algorithme déterministe polynomial (compliqué).

- On peut prouver l'existence par une « méthode déterministe »
  $\longrightarrow$ algorithme déterministe polynomial simple.

Un algorithme parallèle

« Bon vecteur » = vecteur orthogonal à au moins $k/2 - \sqrt{k}/2$ et au plus $k/2 + \sqrt{k}/2$ vecteurs $S^{(i)}$.

Un algorithme parallèle

« Bon vecteur » = vecteur orthogonal à au moins $k/2 - \sqrt{k}/2$ et au plus $k/2 + \sqrt{k}/2$ vecteurs $S^{(i)}$.

On veut un algorithme qui trouve un bon vecteur en espace polylogarithmique
$\longleftrightarrow$ algorithme parallèle en temps polylogarithmique.

Un algorithme parallèle

« Bon vecteur » = vecteur orthogonal à au moins $k/2 - \sqrt{k}/2$ et au plus $k/2 + \sqrt{k}/2$ vecteurs $S^{(i)}$.

On veut un algorithme qui trouve un bon vecteur en espace polylogarithmique
$\longleftrightarrow$ algorithme parallèle en temps polylogarithmique.

Idée de l'algorithme :

- construire un petit ensemble « générique » où on est sûr qu'un bon vecteur existe ;
- effectuer une recherche exhaustive sur cet ensemble générique.

Un algorithme parallèle

« Bon vecteur » = vecteur orthogonal à au moins $k/2 - \sqrt{k}/2$ et au plus $k/2 + \sqrt{k}/2$ vecteurs $S^{(i)}$.

On veut un algorithme qui trouve un bon vecteur en espace polylogarithmique
$\longleftrightarrow$ algorithme parallèle en temps polylogarithmique.

Idée de l'algorithme :

- construire un petit ensemble « générique » où on est sûr qu'un bon vecteur existe ;
- effectuer une recherche exhaustive sur cet ensemble générique.

Remarque : l'ensemble générique conviendra pour toute famille $S^{(1)} \dots S^{(k)}$, comme pour BPP $\subset$ P/poly (Adleman 1978).

Restreindre la recherche

Lemme

Si V est un sous-espace orthogonal à aucun des $S^{(i)} - S^{(j)}$ (c'est-à-dire que pour tous $i \neq j$, il existe $v \in V$ tel que $v.(S^{(i)} - S^{(j)}) = 1$) et à aucun des $S^{(i)}$, alors il existe un bon vecteur dans V.

Restreindre la recherche

Lemme

Si V est un sous-espace orthogonal à aucun des $S^{(i)} - S^{(j)}$ (c'est-à-dire que pour tous $i \neq j$, il existe $v \in V$ tel que $v.(S^{(i)} - S^{(j)}) = 1$) et à aucun des $S^{(i)}$, alors il existe un bon vecteur dans V.

Preuve Les projections des $S^{(i)}$ sur V sont toutes distinctes et non nulles.

« Produit scalaire » $\odot$ associé à une base de $V \longrightarrow$ bon vecteur u pour $\odot$ pour les projections $\rho(S^{(i)})$.

Mais $u.S^{(i)} = u \odot \rho(S^{(i)}) \longrightarrow u$ est un bon vecteur. □

Restreindre la recherche – suite

Corollaire

Si V n'intersecte pas $\{S^{(i)} - S^{(j)} | i \neq j\} \cup \{S^{(i)}\}$, alors $V^{\perp}$ contient un bon vecteur.

$\longrightarrow$ Trouver un sous-espace V de grande dimension qui n'intersecte pas un ensemble de taille $k(k+1)/2$.

Extension

Idée : travailler dans une extension K de $\mathbb{F}_2$ pour avoir plus de place.

Extension

Idée : travailler dans une extension K de $\mathbb{F}_2$ pour avoir plus de place.

Lemme

Soit K une extension de $\mathbb{F}_2$ de cardinal $\geq sN$. Alors on peut construire $|K|$ hyperplans de K^s tels que tout ensemble $U \subseteq K^s \setminus \{0\}$ de cardinal N a une intersection vide avec l'un d'entre eux.

Extension

Idée : travailler dans une extension K de $\mathbb{F}_2$ pour avoir plus de place.

Lemme

Soit K une extension de $\mathbb{F}_2$ de cardinal $\geq sN$. Alors on peut construire $|K|$ hyperplans de K^s tels que tout ensemble $U \subseteq K^s \setminus \{0\}$ de cardinal N a une intersection vide avec l'un d'entre eux.

Preuve Pour chaque $\theta \in K$, soit H_θ l'hyperplan défini par l'équation

$$x_1 + \theta x_2 + \theta^2 x_3 + \cdots + \theta^{s-1} x_s = 0.$$

Un élément $a = (a_1, \ldots, a_s) \in K^s \setminus \{0\}$ appartient à au plus $s-1$ hyperplans car le polynôme $P(\theta) = a_1 + a_2\theta + \cdots + a_s\theta^{s-1}$ a au plus $s-1$ racines. □

Une famille générique de sous-espaces

Hyperplan de $K^s \longrightarrow$ sous-espace de codimension $\log(sN)$ de $(\mathbb{F}_2)^s$. En travaillant dans l'orthogonal :

Théorème

On peut construire en parallèle une famille de $O(s^2k^4)$ éléments de $(\mathbb{F}_2)^s$ qui contient, pour tous vecteurs $S^{(1)}, \ldots, S^{(k)} \in (\mathbb{F}_2)^s$, un vecteur u satisfaisant

$$-\sqrt{k}/2 \leq |\{i | u.S^{(i)} = 0\}| - k/2 \leq \sqrt{k}/2.$$

Une famille générique de sous-espaces

Hyperplan de $K^s \longrightarrow$ sous-espace de codimension $\log(sN)$ de $(\mathbb{F}_2)^s$. En travaillant dans l'orthogonal :

Théorème

On peut construire en parallèle une famille de $O(s^2k^4)$ éléments de $(\mathbb{F}_2)^s$ qui contient, pour tous vecteurs $S^{(1)}, \ldots, S^{(k)} \in (\mathbb{F}_2)^s$, un vecteur u satisfaisant

$$-\sqrt{k}/2 \leq |\{i | u.S^{(i)} = 0\}| - k/2 \leq \sqrt{k}/2.$$

On effectue une recherche exhaustive dans cette famille générique.

Corollaire

Il existe un algorithme parallèle fonctionnant en temps $O(\log^2 n)$ qui, sur l'entrée $S^{(1)}, \ldots, S^{(k)} \in (\mathbb{F}_2)^s$ (taille $n = ks$), retourne un bon vecteur.

Retour au théorème de transfert

On trouve un vecteur orthogonal à environ la moitié d'une famille de vecteur en espace polylogarithmique.

Entrée de taille exponentielle $\longrightarrow$ espace polynomial.

On peut encoder dans les tests $\mathrm{VPSPACE}$.

Conclusion

- Étude de la question $\mathrm{P} = \mathrm{PSPACE}$ dans différents contextes (booléen, BSS, Valiant).
- Même genre de résultat sur $\mathbb{C}$, mais techniques différentes : une variété ne s'exprime plus par une seule équation (somme de carrés sur $\mathbb{R}$).
- Réciproque ? Sur $\mathbb{C}$, utilisation du Nullstellensatz $\Rightarrow$ à un multiple près.
- L'intervalle de taille $\sqrt{k}$ de notre algorithme est-il optimal ?

Plan

1. P et PSPACE
2. P et PSPACE dans le modèle BSS
3. P et PSPACE dans le modèle de Valiant
4. Conditions de signe
5. Un vecteur orthogonal