Difficulté du résultant et des grands déterminants

Bruno Grenet
avec Pascal Koiran et Natacha Portier

Laboratoire de l'Informatique du Parallélisme
École Normale Supérieure de Lyon

http://perso.ens-lyon.fr/bruno.grenet/

Rencontre du GT CMF - ÉNS Cachan
24 juin 2009

Introduction

- Résultant : existence d'une solution à un système polynomial ?

Introduction

- Résultant : existence d'une solution à un système polynomial ?
- Canny (1988) :

Introduction

- Résultant : existence d'une solution à un système polynomial ?
- Canny (1988) :
  - résultant $\in$ PSPACE

Introduction

- Résultant : existence d'une solution à un système polynomial ?
- Canny (1988) :
  - résultant $\in$ PSPACE
  - résultant NP-dur (pas de preuve ?)

Introduction

- Résultant : existence d'une solution à un système polynomial ?
- Canny (1988) :
  - résultant $\in$ PSPACE
  - résultant NP-dur (pas de preuve ?)
  - Quelle est la complexité exacte du résultant ?

Introduction

- Résultant : existence d'une solution à un système polynomial ?
- Canny (1988) :
  - résultant $\in$ PSPACE
  - résultant NP-dur (pas de preuve ?)
  - Quelle est la complexité exacte du résultant ?
- Résultant = pgcd de grands déterminants

Introduction

- Résultant : existence d'une solution à un système polynomial ?
- Canny (1988) :
  - résultant $\in$ PSPACE
  - résultant NP-dur (pas de preuve ?)
  - Quelle est la complexité exacte du résultant ?
- Résultant = pgcd de grands déterminants
  - formalisme pour les étudier ?

Introduction

- Résultant : existence d'une solution à un système polynomial ?
- Canny (1988) :
  - résultant $\in$ PSPACE
  - résultant NP-dur (pas de preuve ?)
  - Quelle est la complexité exacte du résultant ?
- Résultant = pgcd de grands déterminants
  - formalisme pour les étudier ?
  - difficulté dans le cas général ?

Résultats obtenus

- Résultant :

Résultats obtenus

- Résultant :
  - appartient à AM (sous HRG)

Résultats obtenus

- Résultant :
  - appartient à AM (sous HRG)
  - NP-difficile sous réduction probabiliste

Résultats obtenus

- Résultant :
  - appartient à AM (sous HRG)
  - NP-difficile sous réduction probabiliste
  - NP-difficile sous réduction déterministe ? (en cours)

Résultats obtenus

- Résultant :
  - appartient à AM (sous HRG)
  - NP-difficile sous réduction probabiliste
  - NP-difficile sous réduction déterministe ? (en cours)
- Grands déterminants :

Résultats obtenus

- Résultant :
  - appartient à AM (sous HRG)
  - NP-difficile sous réduction probabiliste
  - NP-difficile sous réduction déterministe ? (en cours)
- Grands déterminants :
  - matrices données par circuit

Résultats obtenus

- Résultant :
  - appartient à AM (sous HRG)
  - NP-difficile sous réduction probabiliste
  - NP-difficile sous réduction déterministe ? (en cours)
- Grands déterminants :
  - matrices données par circuit
  - PSPACE-complet

Résultats obtenus

- Résultant :
  - appartient à AM (sous HRG)
  - NP-difficile sous réduction probabiliste
  - NP-difficile sous réduction déterministe ? (en cours)
- Grands déterminants :
  - matrices données par circuit
  - PSPACE-complet
  - résultant donné par circuit

Résultats obtenus

- Résultant :
  - appartient à AM (sous HRG)
  - NP-difficile sous réduction probabiliste
  - NP-difficile sous réduction déterministe ? (en cours)
- Grands déterminants :
  - matrices données par circuit
  - PSPACE-complet
  - résultant donné par circuit

Plan

Plan

Définition des problèmes

- Entrées :

Définition des problèmes

- Entrées :
  - $\mathtt{HN}_{\mathbb{C}}$: $f_1, \ldots, f_s \in \mathbb{C}[X_1, \ldots, X_n]$;

Définition des problèmes

- Entrées :
  - $\mathtt{HN}_{\mathbb{C}}$: $f_1, \ldots, f_s \in \mathbb{C}[X_1, \ldots, X_n]$;
  - $\mathtt{H_2N}_{\mathbb{C}}$: $f_1, \ldots, f_s \in \mathbb{C}[X_1, \ldots, X_n]$, homogènes ;

Définition des problèmes

- Entrées :
  - $\mathtt{HN}_{\mathbb{C}}$: $f_1, \ldots, f_s \in \mathbb{C}[X_1, \ldots, X_n]$;
  - $\mathtt{H_2N}_{\mathbb{C}}$: $f_1, \ldots, f_s \in \mathbb{C}[X_1, \ldots, X_n]$, homogènes ;
  - $\mathtt{H_2N}_{\mathbb{C}}^{\square}$: $f_1, \ldots, f_n \in \mathbb{C}[X_1, \ldots, X_n]$, homogènes ;

Définition des problèmes

- Entrées :
  - $\mathtt{HN}_{\mathbb{C}}$: $f_1, \ldots, f_s \in \mathbb{C}[X_1, \ldots, X_n]$;
  - $\mathtt{H_2N}_{\mathbb{C}}$: $f_1, \ldots, f_s \in \mathbb{C}[X_1, \ldots, X_n]$, homogènes ;
  - $\mathtt{H_2N}_{\mathbb{C}}^{\square}$: $f_1, \ldots, f_n \in \mathbb{C}[X_1, \ldots, X_n]$, homogènes ;
- Questions :

Définition des problèmes

- Entrées :
  - $\mathtt{HN}_{\mathbb{C}}$: $f_1, \ldots, f_s \in \mathbb{C}[X_1, \ldots, X_n]$;
  - $\mathtt{H_2N}_{\mathbb{C}}$: $f_1, \ldots, f_s \in \mathbb{C}[X_1, \ldots, X_n]$, homogènes ;
  - $\mathtt{H_2N}_{\mathbb{C}}^{\square}$: $f_1, \ldots, f_n \in \mathbb{C}[X_1, \ldots, X_n]$, homogènes ;
- Questions :
  - Existe-t-il $(a_1, \ldots, a_n) \in \mathbb{C}$ tel que $f_i(\bar{a}) = 0$ pour tout i ?

Définition des problèmes

- Entrées :
  - $\mathtt{HN}_{\mathbb{C}}$: $f_1, \ldots, f_s \in \mathbb{C}[X_1, \ldots, X_n]$;
  - $\mathtt{H_2N}_{\mathbb{C}}$: $f_1, \ldots, f_s \in \mathbb{C}[X_1, \ldots, X_n]$, homogènes ;
  - $\mathtt{H_2N}_{\mathbb{C}}^{\square}$: $f_1, \ldots, f_n \in \mathbb{C}[X_1, \ldots, X_n]$, homogènes ;
- Questions :
  - Existe-t-il $(a_1, \ldots, a_n) \in \mathbb{C}$ tel que $f_i(\bar{a}) = 0$ pour tout i ?
  - Cas homogènes : $\bar{a} \neq (0, \ldots, 0)$

Définition des problèmes

- Entrées :
  - $\mathtt{HN}_{\mathbb{C}}$: $f_1, \ldots, f_s \in \mathbb{C}[X_1, \ldots, X_n]$;
  - $\mathtt{H_2N}_{\mathbb{C}}$: $f_1, \ldots, f_s \in \mathbb{C}[X_1, \ldots, X_n]$, homogènes ;
  - $\mathtt{H_2N}^{\square}_{\mathbb{C}}$: $f_1, \ldots, f_n \in \mathbb{C}[X_1, \ldots, X_n]$, homogènes ;
- Questions :
  - Existe-t-il $(a_1, \ldots, a_n) \in \mathbb{C}$ tel que $f_i(\bar{a}) = 0$ pour tout i ?
  - Cas homogènes : $\bar{a} \neq (0, \ldots, 0)$
- Version booléennes $\mathtt{HN}$, $\mathtt{H_2N}$, $\mathtt{H_2N}^{\square}$:

Définition des problèmes

- Entrées :
  - $\mathtt{HN}_{\mathbb{C}}$: $f_1, \ldots, f_s \in \mathbb{C}[X_1, \ldots, X_n]$;
  - $\mathtt{H_2N}_{\mathbb{C}}$: $f_1, \ldots, f_s \in \mathbb{C}[X_1, \ldots, X_n]$, homogènes ;
  - $\mathtt{H_2N}^{\square}_{\mathbb{C}}$: $f_1, \ldots, f_n \in \mathbb{C}[X_1, \ldots, X_n]$, homogènes ;
- Questions :
  - Existe-t-il $(a_1, \ldots, a_n) \in \mathbb{C}$ tel que $f_i(\bar{a}) = 0$ pour tout i ?
  - Cas homogènes : $\bar{a} \neq (0, \ldots, 0)$
- Version booléennes $\mathtt{HN}$, $\mathtt{H_2N}$, $\mathtt{H_2N}^{\square}$:
  - Polynômes à cœfficients entiers

Définition des problèmes

- Entrées :
  - $\mathtt{HN}_{\mathbb{C}}$: $f_1, \ldots, f_s \in \mathbb{C}[X_1, \ldots, X_n]$;
  - $\mathtt{H_2N}_{\mathbb{C}}$: $f_1, \ldots, f_s \in \mathbb{C}[X_1, \ldots, X_n]$, homogènes ;
  - $\mathtt{H_2N}^{\square}_{\mathbb{C}}$: $f_1, \ldots, f_n \in \mathbb{C}[X_1, \ldots, X_n]$, homogènes ;
- Questions :
  - Existe-t-il $(a_1, \ldots, a_n) \in \mathbb{C}$ tel que $f_i(\bar{a}) = 0$ pour tout i ?
  - Cas homogènes : $\bar{a} \neq (0, \ldots, 0)$
- Version booléennes $\mathtt{HN}$, $\mathtt{H_2N}$, $\mathtt{H_2N}^{\square}$:
  - Polynômes à cœfficients entiers
  - Racines complexes ?

Définition des problèmes

- Entrées :
  - $\mathtt{HN}_{\mathbb{C}}$: $f_1, \ldots, f_s \in \mathbb{C}[X_1, \ldots, X_n]$;
  - $\mathtt{H_2N}_{\mathbb{C}}$: $f_1, \ldots, f_s \in \mathbb{C}[X_1, \ldots, X_n]$, homogènes ;
  - $\mathtt{H_2N}^{\square}_{\mathbb{C}}$: $f_1, \ldots, f_n \in \mathbb{C}[X_1, \ldots, X_n]$, homogènes ;
- Questions :
  - Existe-t-il $(a_1, \ldots, a_n) \in \mathbb{C}$ tel que $f_i(\bar{a}) = 0$ pour tout i ?
  - Cas homogènes : $\bar{a} \neq (0, \ldots, 0)$
- Version booléennes $\mathtt{HN}$, $\mathtt{H_2N}$, $\mathtt{H_2N}^{\square}$:
  - Polynômes à cœfficients entiers
  - Racines complexes ?
- Résultant : $\mathtt{H_2N}^{\square}$

Définition des problèmes

- Entrées :
  - $\mathtt{HN}_{\mathbb{C}}$: $f_1, \ldots, f_s \in \mathbb{C}[X_1, \ldots, X_n]$;
  - $\mathtt{H_2N}_{\mathbb{C}}$: $f_1, \ldots, f_s \in \mathbb{C}[X_1, \ldots, X_n]$, homogènes ;
  - $\mathtt{H_2N}^{\square}_{\mathbb{C}}$: $f_1, \ldots, f_n \in \mathbb{C}[X_1, \ldots, X_n]$, homogènes ;
- Questions :
  - Existe-t-il $(a_1, \ldots, a_n) \in \mathbb{C}$ tel que $f_i(\bar{a}) = 0$ pour tout i ?
  - Cas homogènes : $\bar{a} \neq (0, \ldots, 0)$
- Version booléennes $\mathtt{HN}$, $\mathtt{H_2N}$, $\mathtt{H_2N}^{\square}$:
  - Polynômes à cœfficients entiers
  - Racines complexes ?
- Résultant : $\mathtt{H_2N}^{\square}$
- Matrices en jeu de taille $\sim d^{dn}$ où d : degré max des f_i

Borne supérieure

Théorème

Sous l'Hypothèse de Riemann Généralisée, $\mathtt{H_2N}^{\square} \in \mathrm{AM}$.

Borne supérieure

Théorème

Sous l'Hypothèse de Riemann Généralisée, $\mathtt{H}_2\mathtt{N}^{\square} \in \mathrm{AM}$.

- AM : Arthur-Merlin (protocole interactif), entre NP et Π_2.

Borne supérieure

Théorème

Sous l'Hypothèse de Riemann Généralisée, $\mathtt{H_2N}^{\square} \in \mathrm{AM}$.

- AM : Arthur-Merlin (protocole interactif), entre NP et Π_2.
- Se déduit du même résultat sur $\mathtt{HN}$ (Koiran 1996)

Borne inférieure

Théorème

$\mathtt{H_2N}^{\square}$ est NP-difficile sous réduction probabiliste.

Borne inférieure

Théorème

$\mathtt{H_2N}^{\square}$ est NP-difficile sous réduction probabiliste.

- $\mathtt{3\text{-}SAT} \leqslant_m \mathtt{Boolsys} \leqslant_m \mathtt{H_2N} \leqslant_r \mathtt{H_2N}^{\square}$

Borne inférieure

Théorème

$\mathtt{H_2N}^{\square}$ est NP-difficile sous réduction probabiliste.

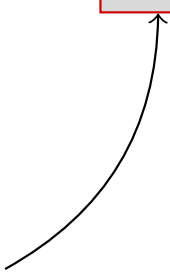
- $\mathtt{3\text{-}SAT} \leqslant_m \mathtt{Boolsys} \leqslant_m \mathtt{H_2N} \leqslant_r \mathtt{H_2N}^{\square}$
  - $X_i = 1$
  - $X_i = \neg X_j$
  - $X_i = X_j \vee X_k$

Borne inférieure

Théorème

$\mathtt{H_2N}^{\square}$ est NP-difficile sous réduction probabiliste.

- $\mathtt{3\text{-}SAT} \leqslant_m \mathtt{Boolsys} \leqslant_m \mathtt{H_2N} \leqslant_r \mathtt{H_2N}^{\square}$
  - $X_i = 1$
  - $X_i = \neg X_j$
  - $X_i = X_j \vee X_k$
- Réduction probabiliste :



Borne inférieure

Théorème

$\mathtt{H_2N}^{\square}$ est NP-difficile sous réduction probabiliste.

- $\mathtt{3\text{-}SAT} \leqslant_m \mathtt{Boolsys} \leqslant_m \mathtt{H_2N} \leqslant_r \mathtt{H_2N}^{\square}$
  - $X_i = 1$
  - $X_i = \neg X_j$
  - $X_i = X_j \vee X_k$
- Réduction probabiliste :
  - Réduire le nombre de polynômes

$\mathtt{H_2N} \leqslant_r \mathtt{H_2N}^{\square}$ (1)

- $f_1, \ldots, f_s$ homogènes de degré 2

$\mathrm{H_2N} \leqslant_r \mathrm{H_2N}^{\square}$ (1)

- $f_1, \ldots, f_s$ homogènes de degré 2
- $g_1, \ldots, g_n : g_i = \sum_j \alpha_{ij} f_j$ (homogènes de degré 2)

$\mathrm{H_2N} \leqslant_r \mathrm{H_2N}^{\square}$ (1)

- $f_1, \ldots, f_s$ homogènes de degré 2
- $g_1, \ldots, g_n : g_i = \sum_j \alpha_{ij} f_j$ (homogènes de degré 2)
- $$\forall \bar{x} \left(\bigwedge_j f_j(\bar{x}) = 0 \Longrightarrow \bigwedge_i g_i(\bar{x}) = 0 \right)$$

$\mathtt{H_2N} \leqslant_r \mathtt{H_2N}^{\square}$ (1)

- $f_1, \ldots, f_s$ homogènes de degré 2
- $g_1, \ldots, g_n$: $g_i = \sum_j \alpha_{ij} f_j$ (homogènes de degré 2)
- $$\forall \bar{x} \left(\bigwedge_j f_j(\bar{x}) = 0 \Longleftarrow \bigwedge_i g_i(\bar{x}) = 0 \right)$$
- α_{ij} algébriquement indépendants : réciproque vraie.

$\mathrm{H_2N} \leqslant_r \mathrm{H_2N}^{\square}$ (1)

- $f_1, \ldots, f_s$ homogènes de degré 2
- $g_1, \ldots, g_n$: $g_i = \sum_j \alpha_{ij} f_j$ (homogènes de degré 2)
- $$\forall \bar{x} \left(\bigwedge_j f_j(\bar{x}) = 0 \Longleftarrow \bigwedge_i g_i(\bar{x}) = 0 \right)$$
- α_{ij} algébriquement indépendants : réciproque vraie.
  - Inutilisable

$\mathrm{H_2N} \leqslant_r \mathrm{H_2N}^{\square}$ (2)

$$\Phi(\bar{\alpha}) \equiv \forall \bar{x} \left(\bigwedge_j f_j(\bar{x}) = 0 \Longleftarrow \bigwedge_i g_i(\bar{x}) = 0 \right)$$

$\mathtt{H_2N} \leqslant_r \mathtt{H_2N}^{\square}$ (2)

$$\Phi(\bar{\alpha}) \equiv \forall \bar{x} \left(\bigwedge_j f_j(\bar{x}) = 0 \Longleftarrow \bigwedge_i \sum_j \alpha_{ij} f_j(\bar{x}) = 0 \right)$$

$\mathrm{H_2N} \leqslant_r \mathrm{H_2N}^{\square}$ (2)

$$\Phi(\bar{\alpha}) \equiv \forall \bar{x} \left(\bigwedge_j f_j(\bar{x}) = 0 \Longleftarrow \bigwedge_i \sum_j \alpha_{ij} f_j(\bar{x}) = 0 \right)$$

- Idée : remplacer par des entiers aléatoires

$\mathtt{H_2N} \leqslant_r \mathtt{H_2N}^{\square}$ (2)

$$\Phi(\bar{\alpha}) \equiv \forall \bar{x} \left(\bigwedge_j f_j(\bar{x}) = 0 \Longleftarrow \bigwedge_i \sum_j \alpha_{ij} f_j(\bar{x}) = 0 \right)$$

- Idée : remplacer par des entiers aléatoires
  - Elimination des quantificateurs de $\Phi(\bar{\alpha})$

$\mathtt{H_2N} \leqslant_r \mathtt{H_2N}^{\square}$ (2)

$$\Phi(\bar{\alpha}) \equiv \forall \bar{x} \left(\bigwedge_j f_j(\bar{x}) = 0 \Longleftarrow \bigwedge_i \sum_j \alpha_{ij} f_j(\bar{x}) = 0 \right)$$

- Idée : remplacer par des entiers aléatoires
  - Elimination des quantificateurs de $\Phi(\bar{\alpha})$

$$\bigvee_k \left(\bigwedge_l P_{kl}(\bar{\alpha}) = 0 \wedge \bigwedge_m Q_{km}(\bar{\alpha}) \neq 0 \right)$$

$\mathtt{H_2N} \leqslant_r \mathtt{H_2N}^{\square}$ (2)

$$\Phi(\bar{\alpha}) \equiv \forall \bar{x} \left(\bigwedge_j f_j(\bar{x}) = 0 \Longleftarrow \bigwedge_i \sum_j \alpha_{ij} f_j(\bar{x}) = 0 \right)$$

- Idée : remplacer par des entiers aléatoires
  - Elimination des quantificateurs de $\Phi(\bar{\alpha})$

$$\bigwedge_l P_{kl}(\bar{\alpha}) = 0 \wedge \bigwedge_m Q_{km}(\bar{\alpha}) \neq 0$$

$\mathtt{H_2N} \leqslant_r \mathtt{H_2N}^{\square}$ (2)

$$\Phi(\bar{\alpha}) \equiv \forall \bar{x} \left(\bigwedge_j f_j(\bar{x}) = 0 \Longleftarrow \bigwedge_i \sum_j \alpha_{ij} f_j(\bar{x}) = 0 \right)$$

- Idée : remplacer par des entiers aléatoires
  - Elimination des quantificateurs de $\Phi(\bar{\alpha})$

$$\bigwedge_l P_{kl}(\bar{\alpha}) = 0 \wedge \bigwedge_m Q_{km}(\bar{\alpha}) \neq 0$$

$\mathtt{H_2N} \leqslant_r \mathtt{H_2N}^{\square}$ (2)

$$\Phi(\bar{\alpha}) \equiv \forall \bar{x} \left(\bigwedge_j f_j(\bar{x}) = 0 \Longleftarrow \bigwedge_i \sum_j \alpha_{ij} f_j(\bar{x}) = 0 \right)$$

- Idée : remplacer par des entiers aléatoires
  - Elimination des quantificateurs de $\Phi(\bar{\alpha})$

$$\bigwedge_m Q_{km}(\bar{\alpha}) \neq 0$$

$\mathtt{H_2N} \leqslant_r \mathtt{H_2N}^{\square}$ (2)

$$\Phi(\bar{\alpha}) \equiv \forall \bar{x} \left(\bigwedge_j f_j(\bar{x}) = 0 \Longleftarrow \bigwedge_i \sum_j \alpha_{ij} f_j(\bar{x}) = 0 \right)$$

- Idée : remplacer par des entiers aléatoires
  - Elimination des quantificateurs de $\Phi(\bar{\alpha})$

$$\prod_m Q_{km}(\bar{\alpha}) \neq 0$$

$\mathrm{H_2N} \leqslant_r \mathrm{H_2N}^{\square}$ (2)

$$\Phi(\bar{\alpha}) \equiv \forall \bar{x} \left(\bigwedge_j f_j(\bar{x}) = 0 \Longleftarrow \bigwedge_i \sum_j \alpha_{ij} f_j(\bar{x}) = 0 \right)$$

- Idée : remplacer par des entiers aléatoires
  - Elimination des quantificateurs de $\Phi(\bar{\alpha})$

$$\prod_m Q_{km}(\bar{\alpha}) \neq 0$$

  - Zéros évités *via* le lemme de Schwartz-Zippel

Soit $P \in \mathbb{C}[X_1, \ldots, X_n]$ de degré d. Alors si on choisit $\bar{a} \in \{1, \ldots, q\}^n$ aléatoirement, $\Pr[P(\bar{a}) = 0] \leqslant d/q$.

Conclusion

Complexité de la nullité du résultant :

Conclusion

Complexité de la nullité du résultant :

- NP-difficile sous réduction probabiliste

Conclusion

Complexité de la nullité du résultant :

- NP-difficile sous réduction probabiliste
- NP-difficile sous réduction déterministe ? (en cours)

Conclusion

Complexité de la nullité du résultant :

- NP-difficile sous réduction probabiliste
- NP-difficile sous réduction déterministe ? (en cours)
- Appartient à AM (« juste au dessus » de NP)

Plan

Représentations par circuit

- Graphe $G = (V, E)$ représenté par le circuit C_G :

$$C_G(i,j) = 1 \iff (i,j) \in E$$

Représentations par circuit

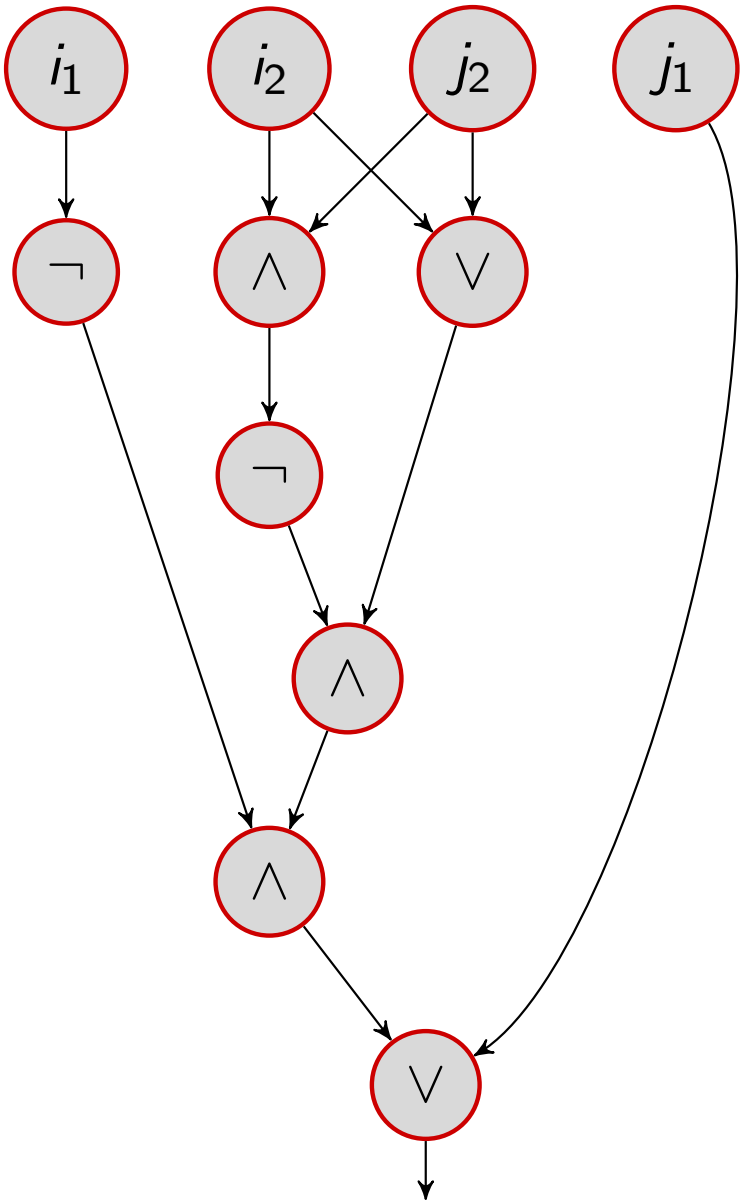
- Graphe $G = (V, E)$ représenté par le circuit C_G :

$$C_G(i,j) = 1 \iff (i,j) \in E$$

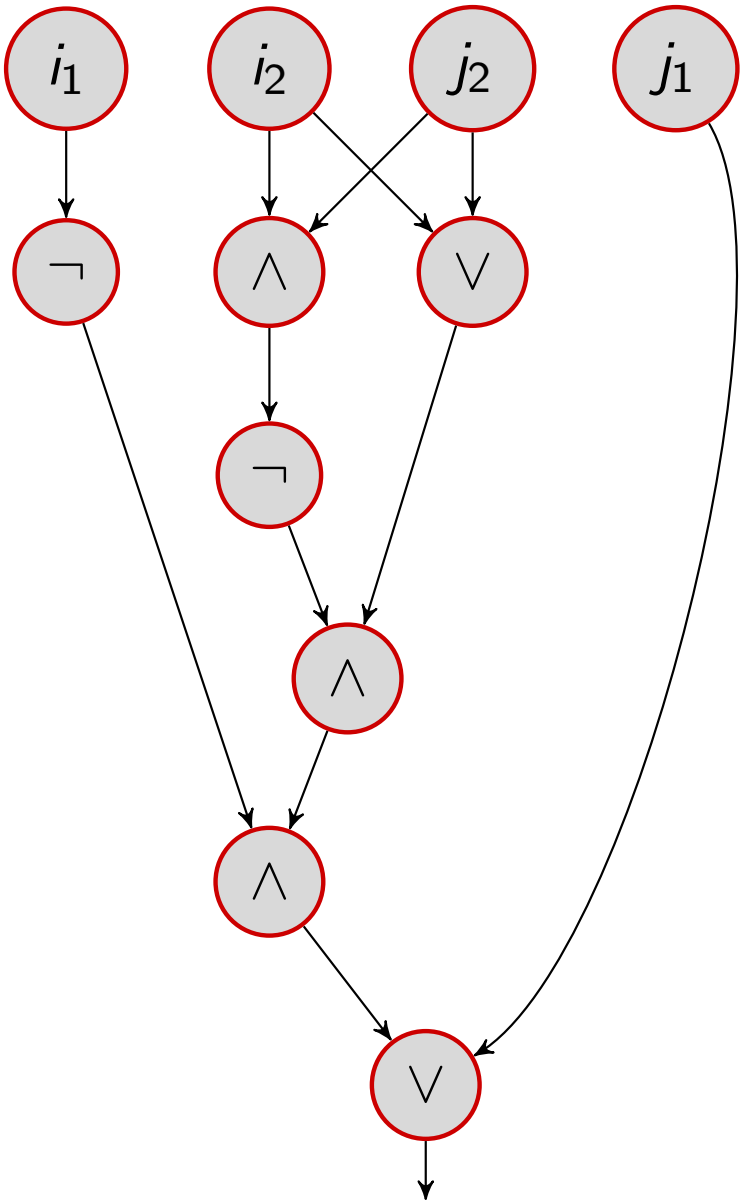
- Matrice $(M_{ij})_{i,j}$ représentée par le circuit C_M :

$$C_M(i,j) = M_{ij}$$

Un exemple

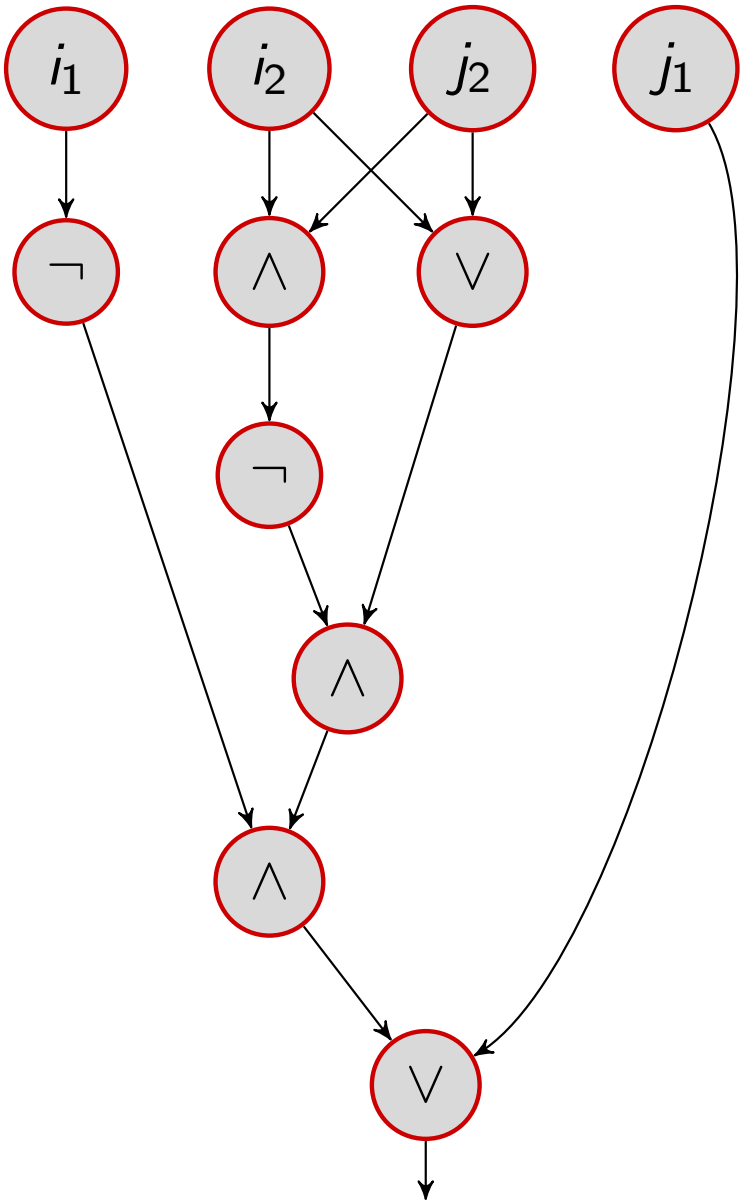


Un exemple

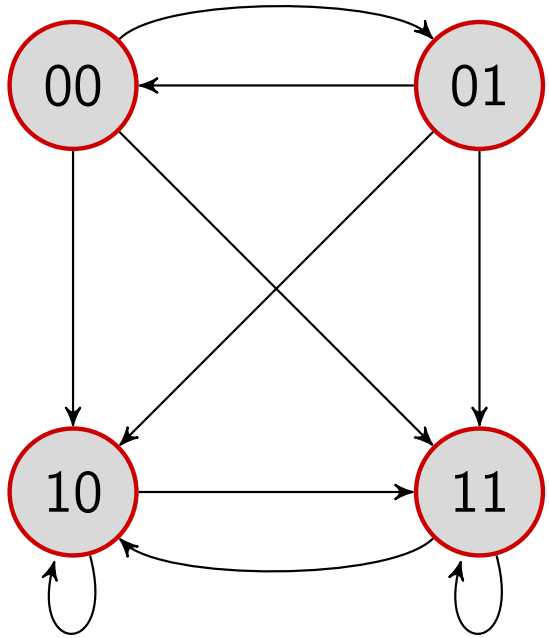


$$\begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix}$$

Un exemple



$$\begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix}$$



Résultat principal

Définition

$\mathtt{Det}_s$: décider la nullité du déterminant d'une matrice donnée par circuit.

Résultat principal

Définition

$\mathtt{Det}_s$: décider la nullité du déterminant d'une matrice donnée par circuit.

Théorème

$\mathtt{Det}_s$ est PSPACE-complet.

Résultat principal

Définition

$\mathtt{Det}_s$: décider la nullité du déterminant d'une matrice donnée par circuit.

Théorème

$\mathtt{Det}_s$ est PSPACE-complet.

- Appartenance à PSPACE : deux ingrédients :

Résultat principal

Définition

$\mathtt{Det}_s$: décider la nullité du déterminant d'une matrice donnée par circuit.

Théorème

$\mathtt{Det}_s$ est PSPACE-complet.

- Appartenance à PSPACE : deux ingrédients :
  - calcul du déterminant en espace polylogarithmique ;

Résultat principal

Définition

$\mathtt{Det}_s$: décider la nullité du déterminant d'une matrice donnée par circuit.

Théorème

$\mathtt{Det}_s$ est PSPACE-complet.

- Appartenance à PSPACE : deux ingrédients :
  - calcul du déterminant en espace polylogarithmique ;
  - simulation d'un circuit en espace linéaire en sa profondeur.

Résultat principal

Définition

$\mathtt{Det}_s$: décider la nullité du déterminant d'une matrice donnée par circuit.

Théorème

$\mathtt{Det}_s$ est PSPACE-complet.

- Appartenance à PSPACE : deux ingrédients :
  - calcul du déterminant en espace polylogarithmique ;
  - simulation d'un circuit en espace linéaire en sa profondeur.
- Réduction : $\mathtt{UQBF} \leqslant_m \mathtt{Access}_s \leqslant_m \mathtt{Det}_s$

$\underline{\mathtt{UQBF}} \leqslant_m \mathtt{Access}_s \leqslant_m \mathtt{Det}_s$

Notation

$\exists! x\, \varphi(x)$: il existe un unique x tel que $\varphi(x)$

$\underline{\texttt{UQBF}} \leqslant_m \texttt{Access}_s \leqslant_m \texttt{Det}_s$

Notation

$\exists! x\, \varphi(x)$: il existe un unique x tel que $\varphi(x)$

Définition

UQBF : formules quantifiées avec $\forall$ et $\exists!$, vraies et prénexes

$\underline{\mathtt{UQBF}} \leqslant_m \mathtt{Access}_s \leqslant_m \mathtt{Det}_s$

Notation

$\exists! x\, \varphi(x)$: il existe un unique x tel que $\varphi(x)$

Définition

UQBF : formules quantifiées avec $\forall$ et $\exists!$, vraies et prénexes

$$\forall x \exists! y \forall z \exists! t \Big[(x \wedge y) \vee \big((\neg x \vee t) \wedge \neg (z \vee \neg t) \big) \Big]$$

$\underline{\texttt{UQBF}} \leqslant_m \texttt{Access}_s \leqslant_m \texttt{Det}_s$

Notation

$\exists! x\, \varphi(x)$: il existe un unique x tel que $\varphi(x)$

Définition

UQBF : formules quantifiées avec $\forall$ et $\exists!$, vraies et prénexes

$$\forall x \exists! y \forall z \exists! t \Big[(x \wedge y) \vee \big((\neg x \vee t) \wedge \neg (z \vee \neg t) \big) \Big]$$

Théorème

UQBF est PSPACE-complet.

$\underline{\texttt{UQBF}} \leqslant_m \texttt{Access}_s \leqslant_m \texttt{Det}_s$

Notation

$\exists! x\, \varphi(x)$: il existe un unique x tel que $\varphi(x)$

Définition

UQBF : formules quantifiées avec $\forall$ et $\exists!$, vraies et prénexes

$$\forall x \exists! y \forall z \exists! t \Big[(x \wedge y) \vee \big((\neg x \vee t) \wedge \neg (z \vee \neg t) \big) \Big]$$

Théorème

UQBF est PSPACE-complet.

Preuve. Similaire à QBF

$\mathtt{UQBF} \leqslant_m \underline{\mathtt{Access}_s} \leqslant_m \mathtt{Det}_s$

$\mathtt{Access}_s$

Entrée : un circuit C_G décrivant un graphe G, deux sommets s et t.
Question : Existe-t-il un chemin de s vers t ?

$\mathtt{UQBF} \leqslant_m \underline{\mathtt{Access}_s} \leqslant_m \mathtt{Det}_s$

$\mathtt{Access}_s$

Entrée : un circuit C_G décrivant un graphe G, deux sommets s et t.
Question : Existe-t-il un chemin de s vers t ?

Théorème

$\mathtt{Access}_s$ est PSPACE-difficile.

$\mathtt{UQBF} \leqslant_m \mathtt{Access}_s \leqslant_m \mathtt{Det}_s$

$\mathtt{Access}_s$

Entrée : un circuit C_G décrivant un graphe G, deux sommets s et t.
Question : Existe-t-il un chemin de s vers t ?

Théorème

$\mathtt{Access}_s$ est PSPACE-difficile.

Preuve. Réduction depuis (U)QBF :

$\mathtt{UQBF} \leqslant_m \mathtt{Access}_s \leqslant_m \mathtt{Det}_s$

$\mathtt{Access}_s$

Entrée : un circuit C_G décrivant un graphe G, deux sommets s et t.
Question : Existe-t-il un chemin de s vers t ?

Théorème

$\mathtt{Access}_s$ est PSPACE-difficile.

Preuve. Réduction depuis (U)QBF :

- Transformation formule $\longrightarrow$ graphe ($+$ s et t) ;

$\mathtt{UQBF} \leqslant_m \mathtt{Access}_s \leqslant_m \mathtt{Det}_s$

$\mathtt{Access}_s$

Entrée : un circuit C_G décrivant un graphe G, deux sommets s et t.
Question : Existe-t-il un chemin de s vers t ?

Théorème

$\mathtt{Access}_s$ est PSPACE-difficile.

Preuve. Réduction depuis (U)QBF :

- Transformation formule $\longrightarrow$ graphe (+ s et t) ;
- Chemin de s à t ssi formule vraie.

$\mathtt{UQBF} \leqslant_m \mathtt{Access}_s \leqslant_m \mathtt{Det}_s$

$\mathtt{Access}_s$

Entrée : un circuit C_G décrivant un graphe G, deux sommets s et t.
Question : Existe-t-il un chemin de s vers t ?

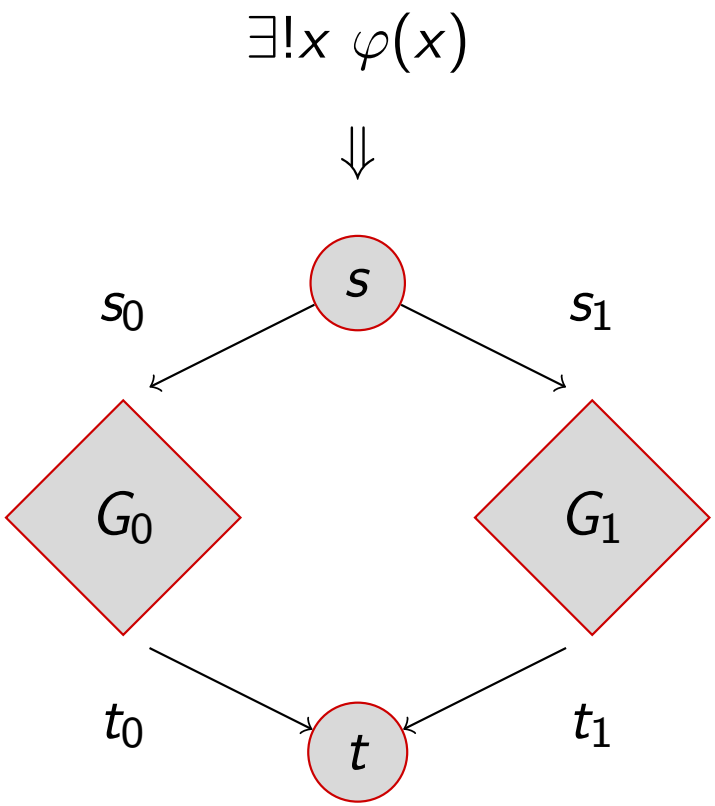
Théorème

$\mathtt{Access}_s$ est PSPACE-difficile.

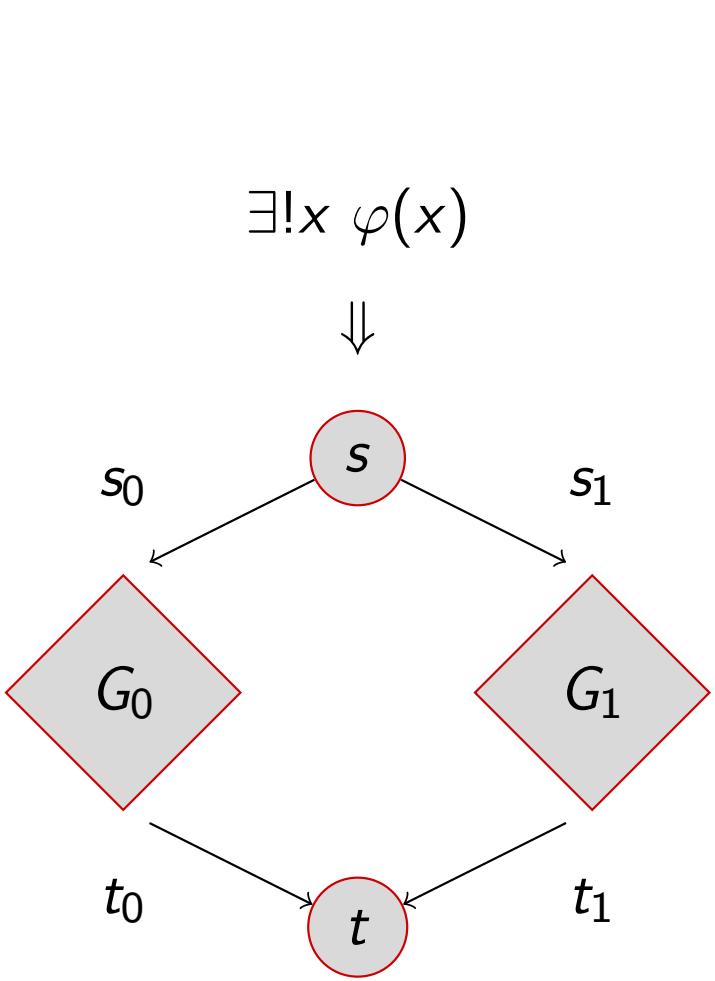
Preuve. Réduction depuis (U)QBF :

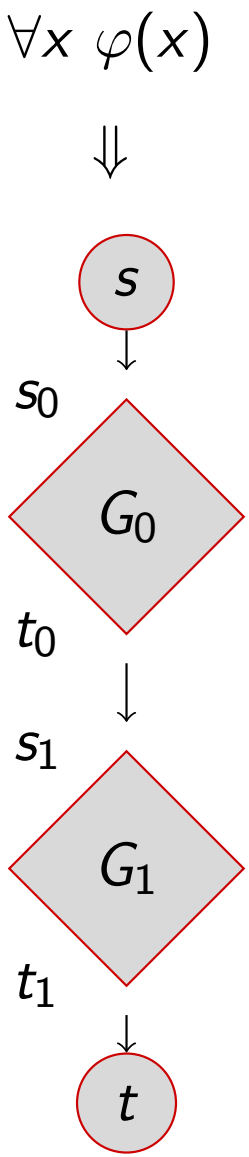
- Transformation formule $\longrightarrow$ graphe ($+$ s et t) ;
- Chemin de s à t ssi formule vraie.
- Depuis UQBF : chemin unique s'il existe.

$\mathtt{UQBF} \leqslant_m \mathtt{Access}_s \leqslant_m \mathtt{Det}_s$



$\mathtt{UQBF} \leqslant_m \mathtt{Access}_s \leqslant_m \mathtt{Det}_s$





$\mathtt{UQBF} \leqslant_m \mathtt{Access}_s \leqslant_m \underline{\mathtt{Det}_s}$

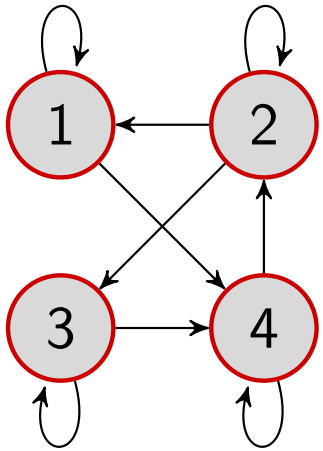
Définition

Couverture par cycle de $G = (V, E)$: partition de $V = V_1 \sqcup V_2 \sqcup \cdots \sqcup V_n$ telle que pour tout i, V_i est un cycle de G.

$\mathtt{UQBF} \leqslant_m \mathtt{Access}_s \leqslant_m \underline{\mathtt{Det}_s}$

Définition

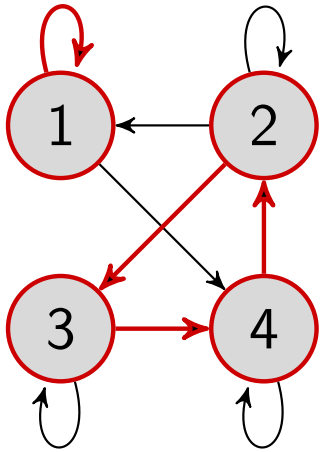
Couverture par cycle de $G = (V, E)$: partition de $V = V_1 \sqcup V_2 \sqcup \cdots \sqcup V_n$ telle que pour tout i, V_i est un cycle de G.



$\mathtt{UQBF} \leqslant_m \mathtt{Access}_s \leqslant_m \underline{\mathtt{Det}_s}$

Définition

Couverture par cycle de $G = (V, E)$: partition de $V = V_1 \sqcup V_2 \sqcup \cdots \sqcup V_n$ telle que pour tout i, V_i est un cycle de G.



$\mathtt{UQBF} \leqslant_m \mathtt{Access}_s \leqslant_m \underline{\mathtt{Det}_s}$

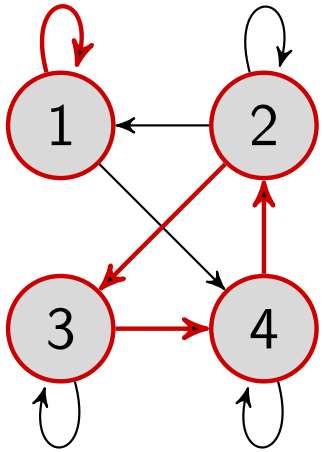
Définition

Couverture par cycle de $G = (V, E)$: partition de $V = V_1 \sqcup V_2 \sqcup \cdots \sqcup V_n$ telle que pour tout i, V_i est un cycle de G.

Lemme

G graphe dont les cycles sont impairs, M sa matrice d'adjacence :

$$\#\text{couvertures} = \det M$$



$\mathtt{UQBF} \leqslant_m \mathtt{Access}_s \leqslant_m \underline{\mathtt{Det}_s}$

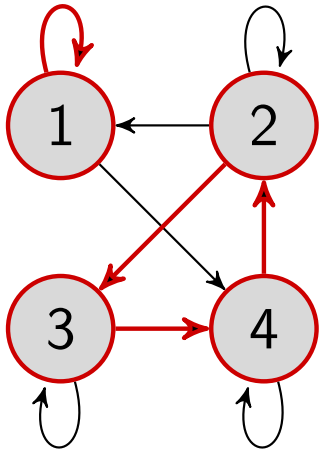
Définition

Couverture par cycle de $G = (V, E)$: partition de $V = V_1 \sqcup V_2 \sqcup \cdots \sqcup V_n$ telle que pour tout i, V_i est un cycle de G.

Lemme

G graphe dont les cycles sont impairs, M sa matrice d'adjacence :

$$\#\text{couvertures} = \det M$$



$$\det \begin{pmatrix} 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \end{pmatrix} = 3$$

$\mathtt{UQBF} \leqslant_m \mathtt{Access}_s \leqslant_m \underline{\mathtt{Det}_s}$

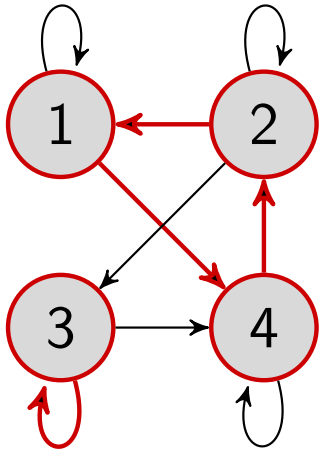
Définition

Couverture par cycle de $G = (V, E)$: partition de $V = V_1 \sqcup V_2 \sqcup \cdots \sqcup V_n$ telle que pour tout i, V_i est un cycle de G.

Lemme

G graphe dont les cycles sont impairs, M sa matrice d'adjacence :

$$\#\text{couvertures} = \det M$$



$$\det \begin{pmatrix} 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \end{pmatrix} = 3$$

$\mathtt{UQBF} \leqslant_m \mathtt{Access}_s \leqslant_m \underline{\mathtt{Det}_s}$

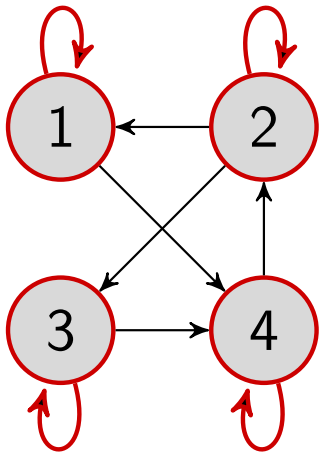
Définition

Couverture par cycle de $G = (V, E)$: partition de $V = V_1 \sqcup V_2 \sqcup \cdots \sqcup V_n$ telle que pour tout i, V_i est un cycle de G.

Lemme

G graphe dont les cycles sont impairs, M sa matrice d'adjacence :

$$\#\text{couvertures} = \det M$$



$$\det \begin{pmatrix} 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \end{pmatrix} = 3$$

Preuve du résultat principal

Théorème (rappel)

$\mathtt{Det}_s$ est PSPACE-complet.

Preuve du résultat principal

Théorème (rappel)

$\mathtt{Det}_s$ est PSPACE-complet.

- Réduction $\mathtt{UQBF} \leqslant_m \mathtt{Access}_s \leqslant_m \mathtt{Det}_s$

Preuve du résultat principal

Théorème (rappel)

$\mathtt{Det}_s$ est PSPACE-complet.

- Réduction $\mathtt{Access}_s \leqslant_m \mathtt{Det}_s$
- Modification mineure du graphe
  - Uniquement cycles impairs
  - Chemin de s à t ssi couverture par cycles

Preuve du résultat principal

Théorème (rappel)

$\mathtt{Det}_s$ est PSPACE-complet.

- Réduction $\mathtt{UQBF} \leqslant_m \mathtt{Access}_s \leqslant_m \mathtt{Det}_s$
- Modification mineure du graphe
  - Uniquement cycles impairs
  - Chemin de s à t ssi couverture par cycles
- $\Phi \in \mathtt{UQBF}$

Preuve du résultat principal

Théorème (rappel)

$\mathtt{Det}_s$ est PSPACE-complet.

- Réduction $\mathtt{UQBF} \leqslant_m \mathtt{Access}_s \leqslant_m \mathtt{Det}_s$
- Modification mineure du graphe
  - Uniquement cycles impairs
  - Chemin de s à t ssi couverture par cycles
- $\Phi \in \mathtt{UQBF} \iff s \rightsquigarrow t$

Preuve du résultat principal

Théorème (rappel)

$\mathtt{Det}_s$ est PSPACE-complet.

- Réduction $\mathtt{UQBF} \leqslant_m \mathtt{Access}_s \leqslant_m \mathtt{Det}_s$
- Modification mineure du graphe
  - Uniquement cycles impairs
  - Chemin de s à t ssi couverture par cycles
- $\Phi \in \mathtt{UQBF} \iff s \rightsquigarrow t \iff G$ couvrable par cycles

Preuve du résultat principal

Théorème (rappel)

$\mathtt{Det}_s$ est PSPACE-complet.

- Réduction $\mathtt{UQBF} \leqslant_m \mathtt{Access}_s \leqslant_m \mathtt{Det}_s$
- Modification mineure du graphe
  - Uniquement cycles impairs
  - Chemin de s à t ssi couverture par cycles
- $\Phi \in \mathtt{UQBF} \iff s \rightsquigarrow t \iff G$ couvrable par cycles $\iff \det M \neq 0$

Preuve du résultat principal

Théorème (rappel)

$\mathtt{Det}_s$ est PSPACE-complet.

- Réduction $\mathtt{UQBF} \leqslant_m \mathtt{Access}_s \leqslant_m \mathtt{Det}_s$
- Modification mineure du graphe
  - Uniquement cycles impairs
  - Chemin de s à t ssi couverture par cycles
- $\Phi \in \mathtt{UQBF} \iff s \rightsquigarrow t \iff G$ couvrable par cycles $\iff \det M \neq 0$
- $\det M \neq 0 \iff \det M = 1$

Conclusion

- Réponse (partielle) à la question de Canny

Conclusion

- Réponse (partielle) à la question de Canny
- Formalisme des représentations succinctes de matrices :

Conclusion

- Réponse (partielle) à la question de Canny
- Formalisme des représentations succinctes de matrices :
  - Adapté des graphes

Conclusion

- Réponse (partielle) à la question de Canny
- Formalisme des représentations succinctes de matrices :
  - Adapté des graphes
  - Applicable à d'autres problèmes :

Conclusion

- Réponse (partielle) à la question de Canny
- Formalisme des représentations succinctes de matrices :
  - Adapté des graphes
  - Applicable à d'autres problèmes :
    - ★ théorie des nombres : Cheng, Tarasov, Vyalyi (2009)

Conclusion

- Réponse (partielle) à la question de Canny
- Formalisme des représentations succinctes de matrices :
  - Adapté des graphes
  - Applicable à d'autres problèmes :
    - ★ théorie des nombres : Cheng, Tarasov, Vyalyi (2009)
    - ★ quantique : Jordan, Love (2009), Jordan, Wocjan (2009), Harrow, Hassidim, Lloyd (2009)

Conclusion

- Réponse (partielle) à la question de Canny
- Formalisme des représentations succinctes de matrices :
  - Adapté des graphes
  - Applicable à d'autres problèmes :
    - ★ théorie des nombres : Cheng, Tarasov, Vyalyi (2009)
    - ★ quantique : Jordan, Love (2009), Jordan, Wocjan (2009), Harrow, Hassidim, Lloyd (2009)
    - ★ ...

Conclusion

- Réponse (partielle) à la question de Canny
- Formalisme des représentations succinctes de matrices :
  - Adapté des graphes
  - Applicable à d'autres problèmes :
    - ★ théorie des nombres : Cheng, Tarasov, Vyalyi (2009)
    - ★ quantique : Jordan, Love (2009), Jordan, Wocjan (2009), Harrow, Hassidim, Lloyd (2009)
    - ★ ...
- Perspectives :

Conclusion

- Réponse (partielle) à la question de Canny
- Formalisme des représentations succinctes de matrices :
  - Adapté des graphes
  - Applicable à d'autres problèmes :
    - ★ théorie des nombres : Cheng, Tarasov, Vyalyi (2009)
    - ★ quantique : Jordan, Love (2009), Jordan, Wocjan (2009), Harrow, Hassidim, Lloyd (2009)
    - ★ ...
- Perspectives :
  - Finir de répondre à la question de Canny (en bonne voie !)

Conclusion

- Réponse (partielle) à la question de Canny
- Formalisme des représentations succinctes de matrices :
  - Adapté des graphes
  - Applicable à d'autres problèmes :
    - ★ théorie des nombres : Cheng, Tarasov, Vyalyi (2009)
    - ★ quantique : Jordan, Love (2009), Jordan, Wocjan (2009), Harrow, Hassidim, Lloyd (2009)
    - ★ ...
- Perspectives :
  - Finir de répondre à la question de Canny (en bonne voie !)
  - Regarder des problèmes *via* les représentations succinctes

Merci de votre attention !