Réduction de la profondeur dans les circuits arithmétiques

Sébastien Tavenas

15 mai 2012

Circuits arithmétiques

Polynômes

$f(x, y) = 4x^2 - 2xy$

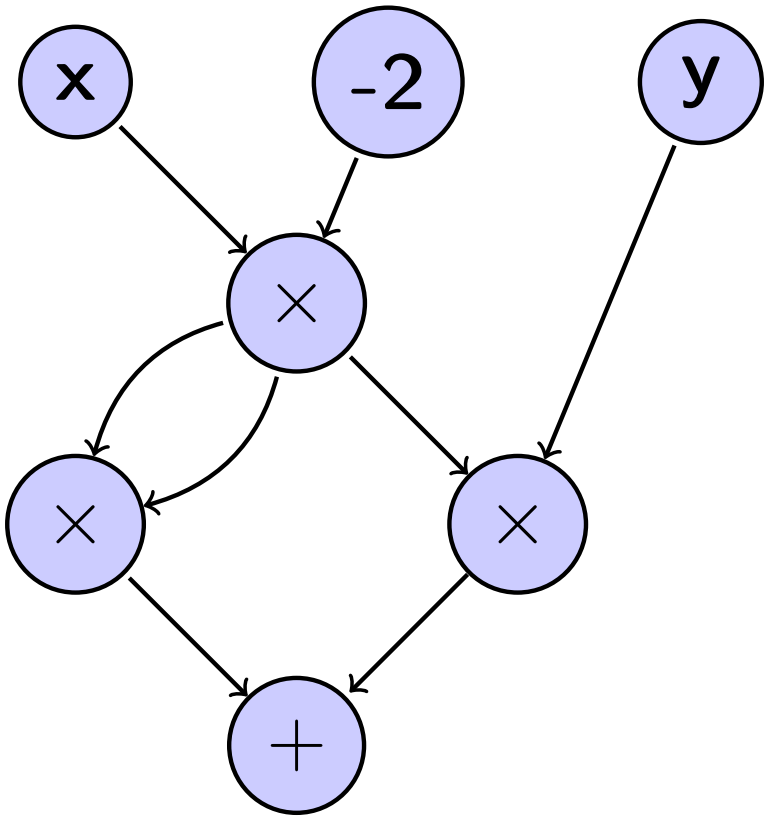
Représentation par des circuits (portes: $+$, $\times$, variables et constantes réelles):

Circuits arithmétiques

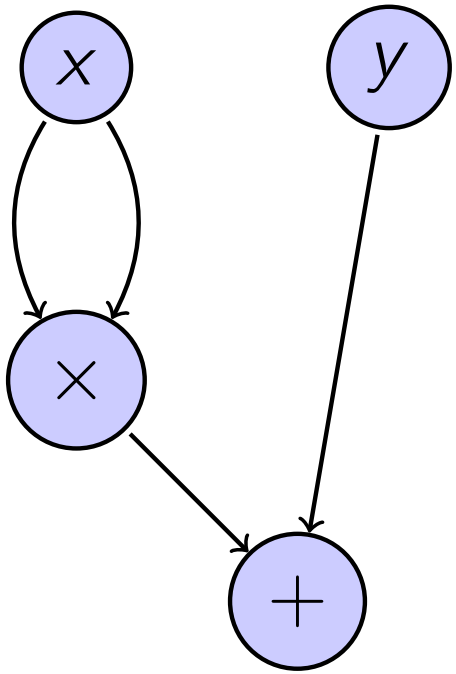
Polynômes

$f(x, y) = 4x^2 - 2xy$

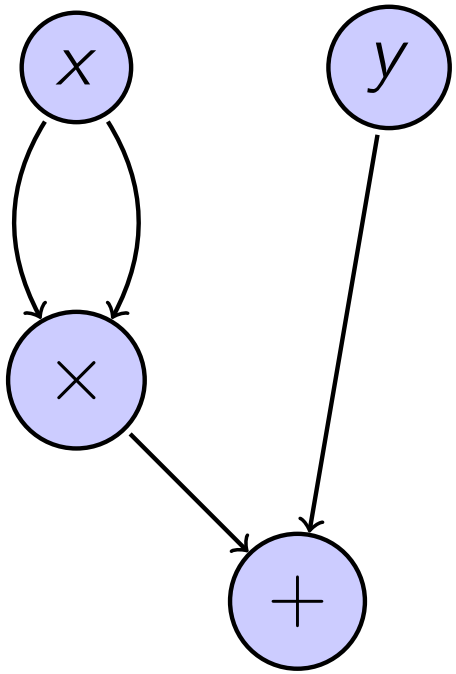
Représentation par des circuits (portes: $+$, $\times$, variables et constantes réelles):



Complexité des circuits - Exemples



Complexité des circuits - Exemples



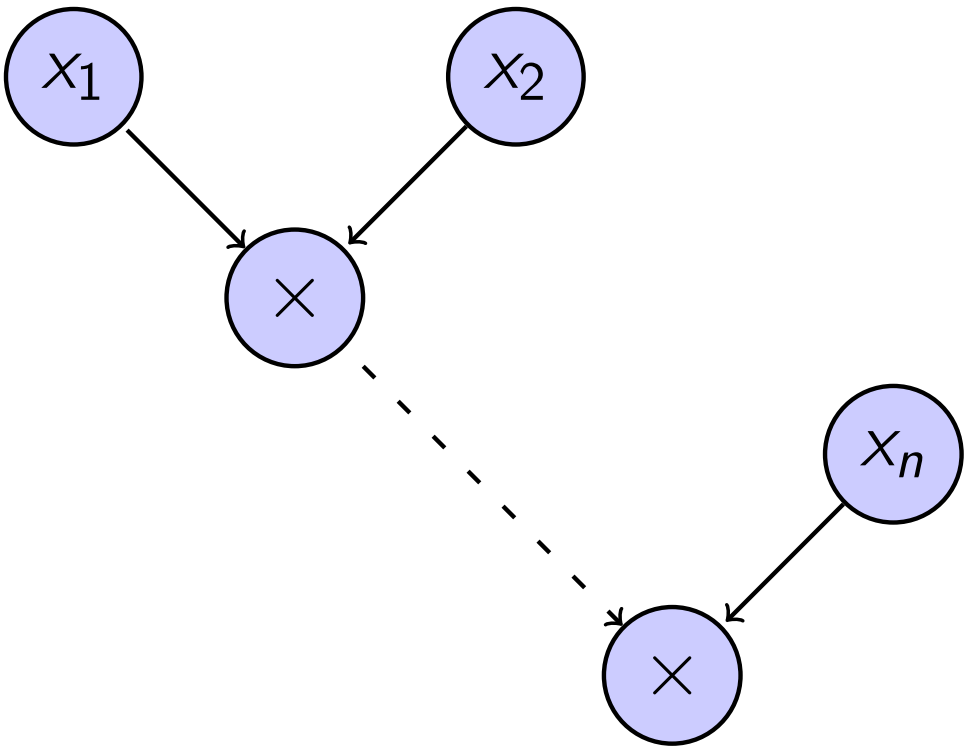
- Polynôme calculé: $P(x) = x^2 + y$.
- Taille: $t = 4$.
- Profondeur: $p = 2$.

Complexité des circuits - Exemples

- Exemple:
  $P_n(x_1, \ldots, x_n) = x_1 \cdot x_2 \cdot \ldots \cdot x_n$

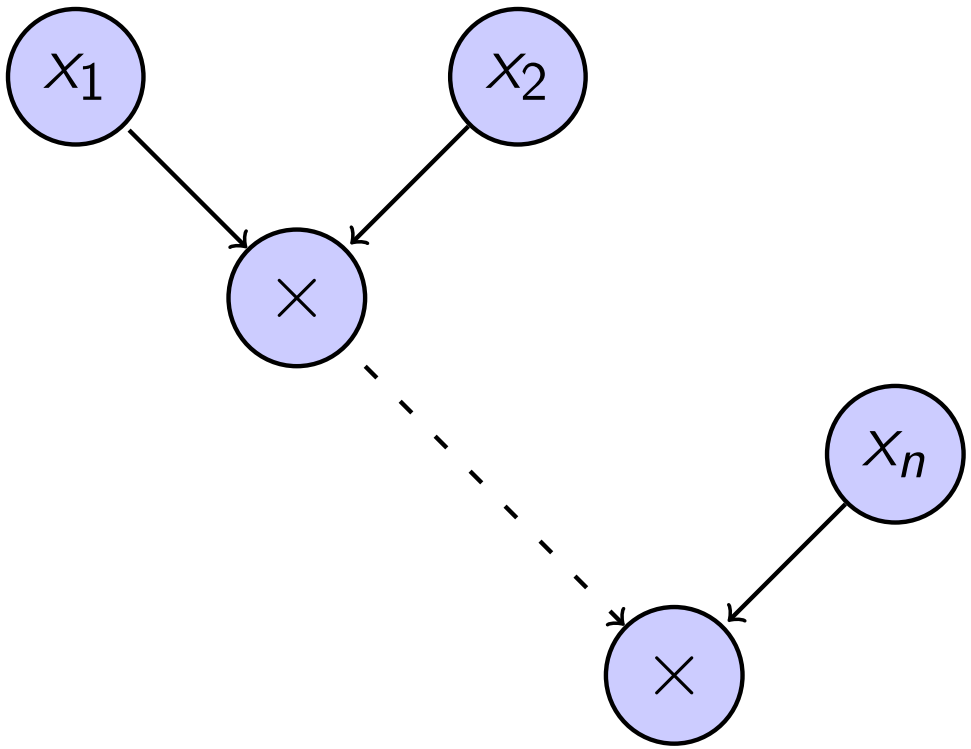
Complexité des circuits - Exemples

- Exemple:
  $P_n(x_1, \ldots, x_n) = x_1 \cdot x_2 \cdot \ldots \cdot x_n$



Complexité des circuits - Exemples

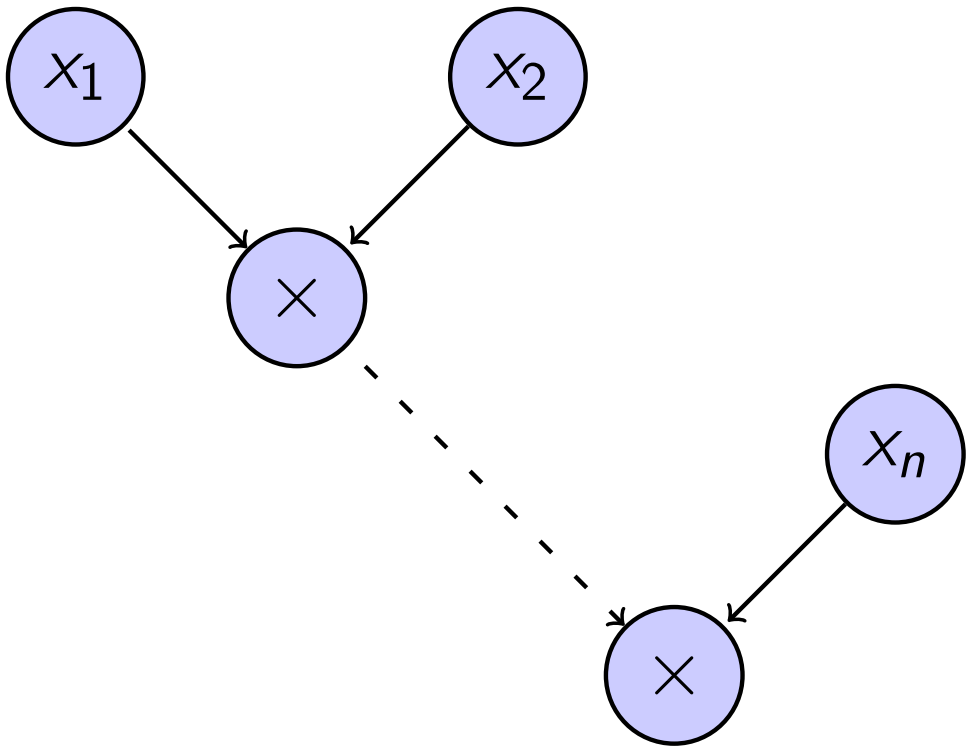
- Exemple:
  $P_n(x_1, \ldots, x_n) = x_1 \cdot x_2 \cdot \ldots \cdot x_n$



- Taille: $t = 2n - 1$.
- Profondeur: $p = n - 1$.

Complexité des circuits - Exemples

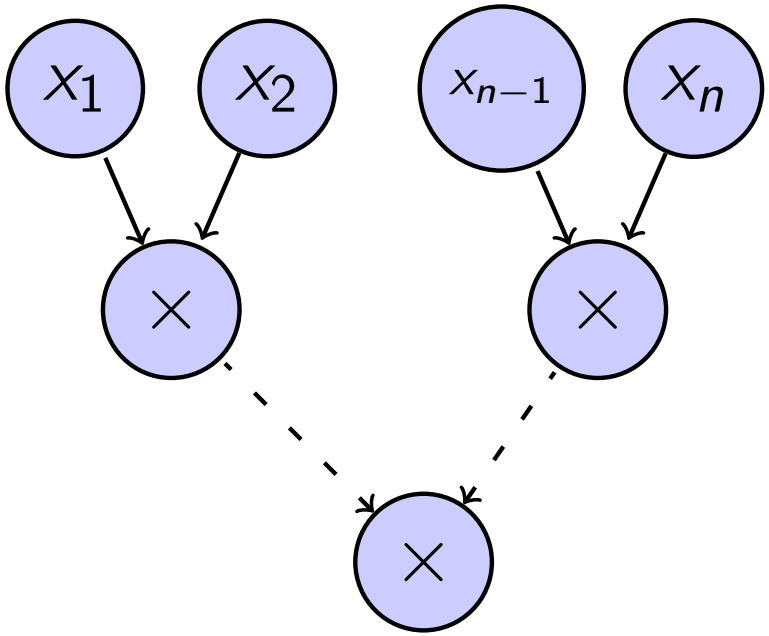
- Exemple:
  $P_n(x_1, \ldots, x_n) = x_1 \cdot x_2 \cdot \ldots \cdot x_n$



- Taille: $t = 2n - 1$.
- Profondeur: $p = n - 1$.
- Suite: polynômes homogènes.
- Circuit homogène: toutes les portes calculent des polynômes homogènes.

Complexité des circuits - Exemples

- Exemple:
  $P_n(x_1, \ldots, x_n) = x_1 \cdot x_2 \cdot \ldots \cdot x_n$

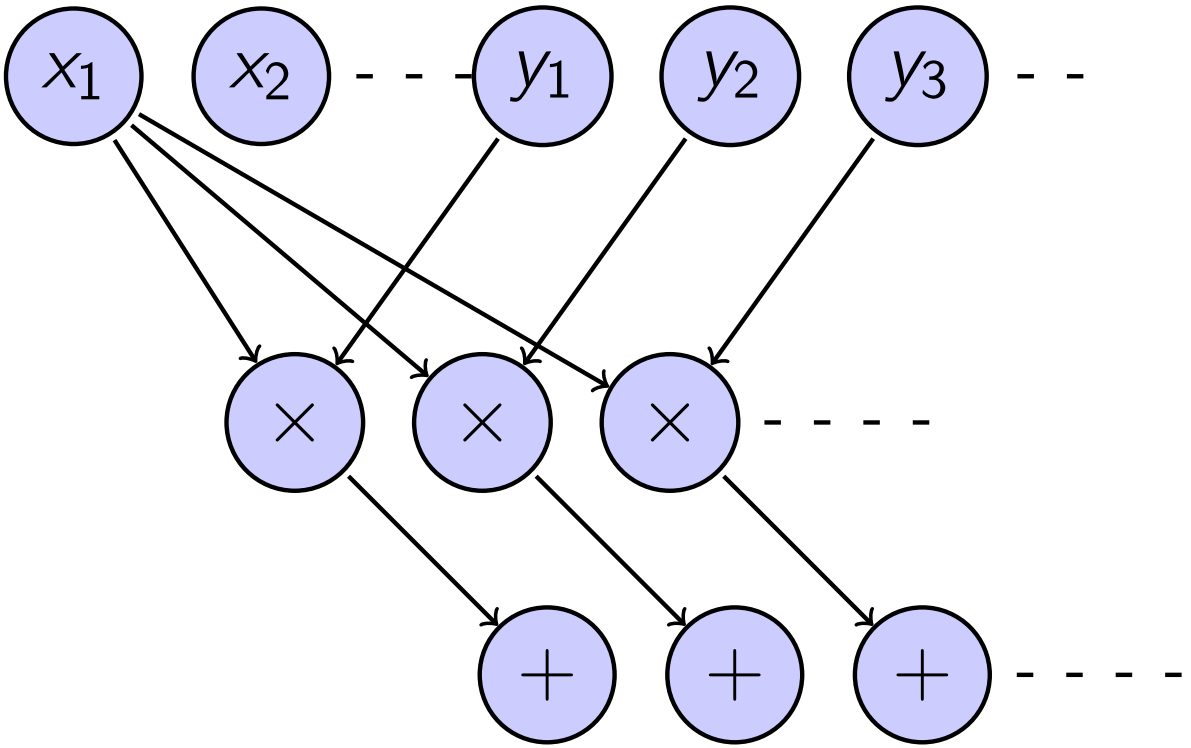


- Taille: $t = 2n - 1$.
- Profondeur: $p = \log n$.

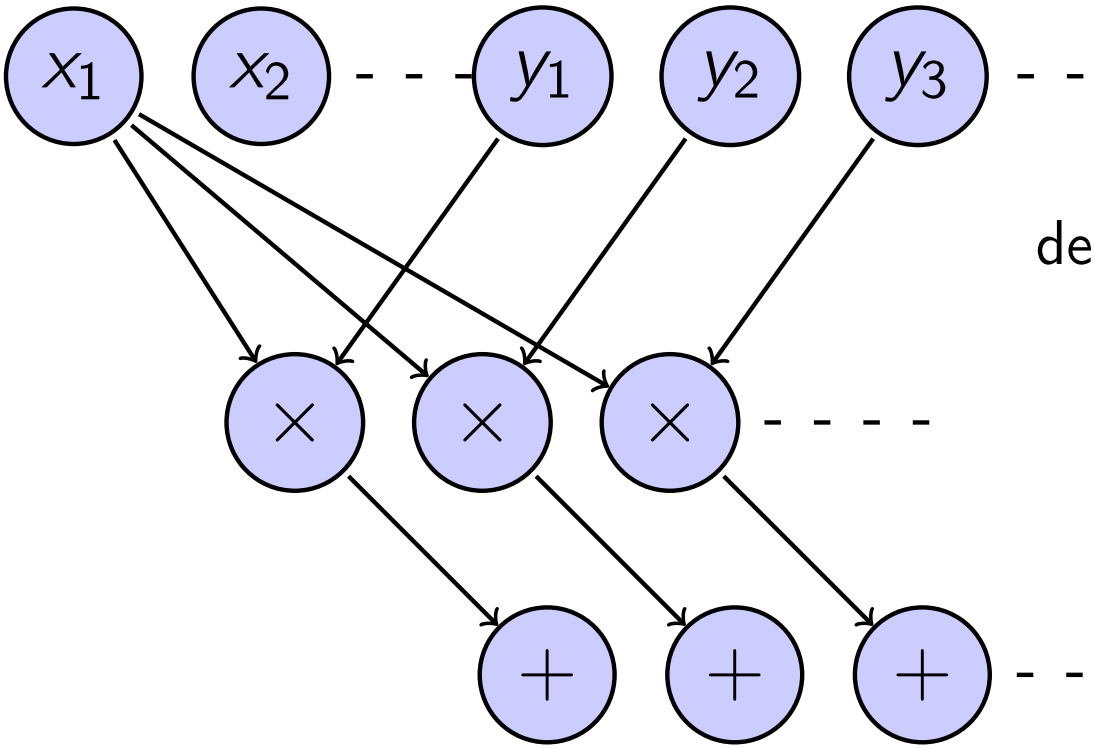
Complexité des circuits - Exemples

- $X = \begin{pmatrix} x_1 & x_2 & x_3 \\ x_4 & x_5 & x_6 \\ x_7 & x_8 & x_9 \end{pmatrix}$
- $Y = \begin{pmatrix} y_1 & y_2 & y_3 \\ y_4 & y_5 & y_6 \\ y_7 & y_8 & y_9 \end{pmatrix}$
- Produit matriciel: $X \cdot Y$.

Complexité des circuits - Exemples



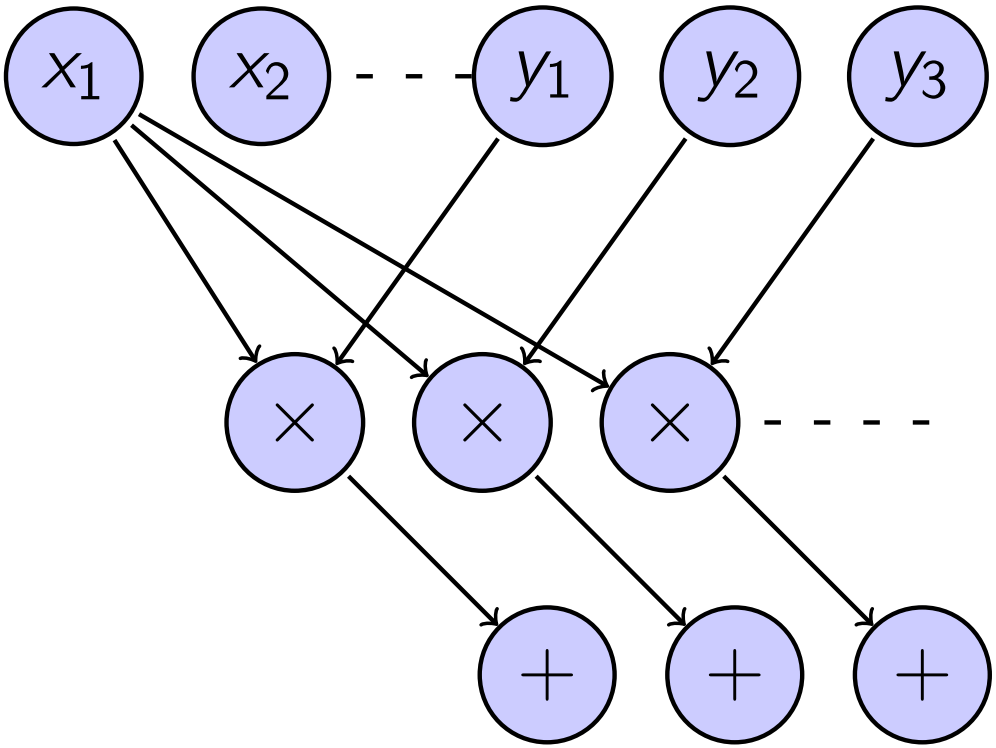
Complexité des circuits - Exemples



Produit de deux matrices de taille n:

- Taille: $t = O(n^3)$.
- Profondeur: $p = 2$.

Complexité des circuits - Exemples



Produit de deux matrices:

- Taille: $t = O(n^3)$.
- Profondeur: $p = 2$.

Produit n matrices de taille n:

- Taille: $t = O(n^4)$.
- Profondeur: $p = \log n$.

Conjecture de Valiant

Classe VP

(f_n) : il existe c pour tout $n \geq 2$

- au plus n^c inconnues
- f_n calculés par des circuits de taille $\leq n^c$
- degré borné par n^c.

$$\mathrm{Det}_n((x_{i,j})_{i,j\leq n}) = \sum_{\sigma\in\mathfrak{S}_n} (-1)^{\epsilon(\sigma)} \prod_{i=1}^{n} x_{i,\sigma(i)}$$

Conjecture de Valiant

Classe VP

(f_n) : il existe c pour tout $n \geq 2$

- au plus n^c inconnues
- f_n calculés par des circuits de taille $\leq n^c$
- degré borné par n^c.

Classe VNP

(g_n) : il existe $(f_n) \in$ VP pour tout n

- $g_n(x) = \sum_{\epsilon \in \{0,1\}^{n^c}} f_n(x, \epsilon)$.

$$\mathrm{Per}_n((x_{i,j})_{i,j \leq n}) = \sum_{\sigma \in \mathfrak{S}_n} \prod_{i=1}^{n} x_{i,\sigma(i)}$$

Conjecture de Valiant

Classe VP

(f_n) : il existe c pour tout $n \geq 2$

- au plus n^c inconnues
- f_n calculés par des circuits de taille $\leq n^c$
- degré borné par n^c.

Classe VNP

(g_n) : il existe $(f_n) \in \mathrm{VP}$ pour tout n

- $g_n(x) = \sum_{\epsilon \in \{0,1\}^{n^c}} f_n(x, \epsilon)$.

Conjecture de Valiant

$\mathrm{VP} \neq \mathrm{VNP}$.

Réduction de la profondeur

Théorème (Valiant,Skyum,Berkowitz,Rackoff/Agrawal,Vinay)

f_n de degrés d_n
circuits de taille $n^{O(1)}$.
Alors f_n calculée par des circuits de taille $n^{O(1)}$
et de profondeur $O(\log n \log d_n)$.
De plus, les circuits sont "équilibrés".

Réduction de la profondeur

Théorème (Valiant,Skyum,Berkowitz,Rackoff/Agrawal,Vinay)

f_n de degrés d_n
circuits de taille $n^{O(1)}$.
Alors f_n calculée par des circuits de taille $n^{O(1)}$
et de profondeur $O(\log n \log d_n)$.
De plus, les circuits sont "équilibrés".

Dans la suite, $d_n = n^{O(1)}$.

Réduction de la profondeur

Théorème (Valiant,Skyum,Berkowitz,Rackoff/Agrawal,Vinay)

f_n de degrés d_n
circuits de taille $n^{O(1)}$.
Alors f_n calculée par des circuits de taille $n^{O(1)}$
et de profondeur $O(\log n \log d_n)$.
De plus, les circuits sont "équilibrés".

Dans la suite, $d_n = n^{O(1)}$.
Peut-on réduire encore la profondeur?

Réduction à la profondeur 4

Portes d'arité non bornée.

Réduction à la profondeur 4

Portes d'arité non bornée.

Théorème (Agrawal,Vinay)

Si f_n a circuits de taille sous-exponentielle.
Alors f_n a des circuits de profondeur 4 de taille sous-exponentielle.

Réduction à la profondeur 4

Portes d'arité non bornée.

Théorème (Agrawal,Vinay)

Si f_n a circuits de taille sous-exponentielle.
Alors f_n a des circuits de profondeur 4 de taille sous-exponentielle.

Remarques:

- Profondeur 2 $\rightarrow$ forme développée du polynôme.

Réduction à la profondeur 4

Portes d'arité non bornée.

Théorème (Agrawal,Vinay)

Si f_n a circuits de taille sous-exponentielle.
Alors f_n a des circuits de profondeur 4 de taille sous-exponentielle.

Remarques:

- Profondeur 2 $\rightarrow$ forme développée du polynôme.
- Profondeur 3 $\rightarrow$???

Réduction à la profondeur 4

Théorème (Koiran)

Si f_n a circuits (homogènes) de taille polynomiale.
Alors f_n a des circuits (homogènes) de profondeur 4 de taille $2^{O(\sqrt{d}\log^2 n)}$.

Idée:

$$\underset{t,d}{\mathcal{C}} \longrightarrow \underset{2^{O(\log d \log t)}}{\text{Produit matriciel itéré}} \longrightarrow \underset{2^{O(\sqrt{d}\log^2 t)}}{\text{Circuit de profondeur } 4}$$

Réduction à la profondeur 4

Théorème (Koiran)

Si f_n a circuits (homogènes) de taille polynomiale.
Alors f_n a des circuits (homogènes) de profondeur 4 de taille $2^{O(\sqrt{d}\log^2 n)}$.

Idée:

$$\underset{t,d}{\mathcal{C}} \longrightarrow \underset{2^{O(\log d \log t)}}{\text{Produit matriciel itéré}} \longrightarrow \underset{2^{O(\sqrt{d}\log^2 t)}}{\text{Circuit de profondeur 4}}$$

Théorème (T.)

Si f_n a circuits (homogènes) de taille polynomiale.
Alors f_n a des circuits (homogènes) de profondeur 4 de taille $2^{O(\sqrt{d}\log n)}$.

Cas du Permanent

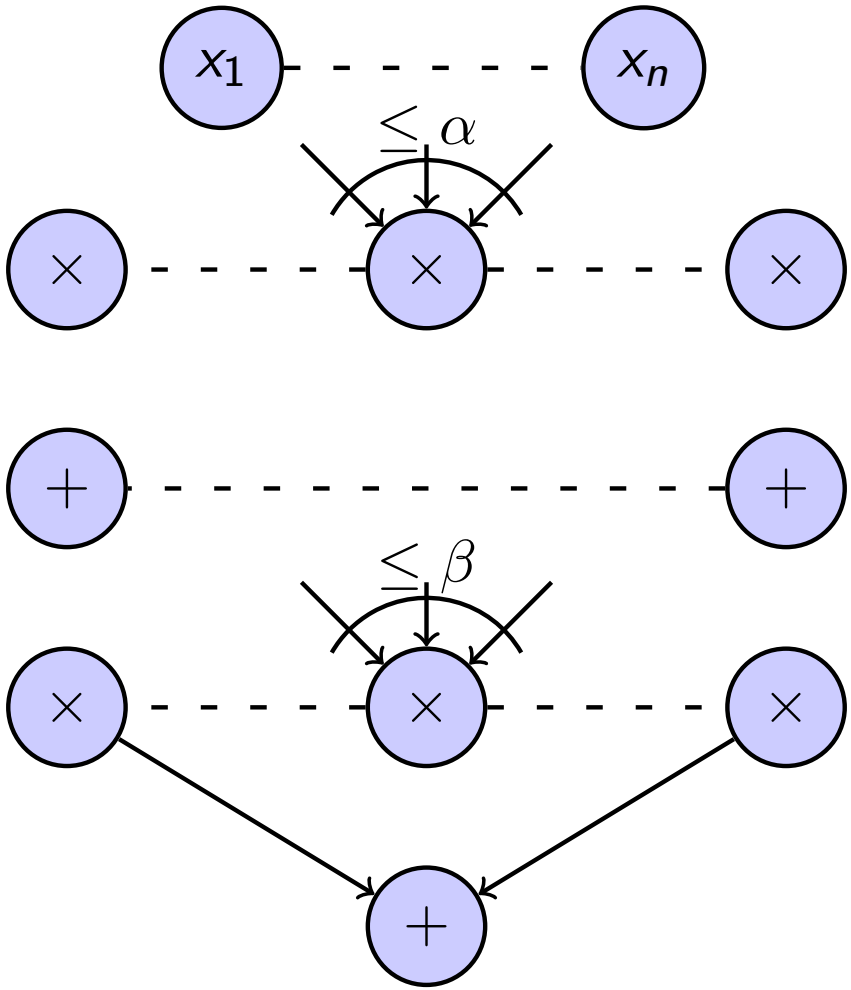
Corollaire

Si Perm_n *n'a pas de circuits homogènes de profondeur* 4 *de taille* $2^{O(\sqrt{n}\log n)}$.

Alors $\mathrm{VP} \neq \mathrm{VNP}$.

Bornes inférieures pour le permanent en profondeur 4

Circuits homogènes:



Bornes inférieures pour le permanent en profondeur 4

Théorème (Gupta,Kamath,Kayal,Saptharishi)

Si C est un circuit homogène de profondeur 4 avec $\alpha \leq O(\sqrt{n})$ calculant Perm_n.
Alors, $taille(C) \geq 2^{\Omega(\sqrt{n})}$.

Bornes inférieures pour le permanent en profondeur 4

Théorème (Gupta,Kamath,Kayal,Saptharishi)

Si C est un circuit homogène de profondeur 4 avec $\alpha \leq O(\sqrt{n})$ calculant Perm_n.
Alors, $taille(C) \geq 2^{\Omega(\sqrt{n})}$.

Proposition

Si C est un circuit homogène de profondeur 4 avec $\beta \leq O(\sqrt{n})$ calculant Perm_n.
Alors, $taille(C) \geq 2^{\Omega(\sqrt{n}\log n)}$.

Bornes inférieures pour le permanent en profondeur 4

Théorème (Gupta,Kamath,Kayal,Saptharishi)

Si C est un circuit homogène de profondeur 4 avec $\alpha \leq O(\sqrt{n})$ calculant Perm_n.
Alors, $taille(C) \geq 2^{\Omega(\sqrt{n})}$.

Proposition

Si C est un circuit homogène de profondeur 4 avec $\beta \leq O(\sqrt{n})$ calculant Perm_n.
Alors, $taille(C) \geq 2^{\Omega(\sqrt{n}\log n)}$.

Corollaire

Si C circuit minimal homogène de profondeur 4 avec $\alpha, \beta \leq O(\sqrt{n})$ calculant Det_n.
Alors, $taille(C) \geq 2^{\Theta(\sqrt{n}\log n)}$.