

Réseaux de preuves booléens sous-logarithmiques

16^{èmes} Rencontres LAC

Clément Aubert



Institut Galilée - Université Paris-Nord
99, avenue Jean-Baptiste Clément
93430 Villetaneuse

16 et 17 novembre 2010

Deux modèles du calcul parallèle

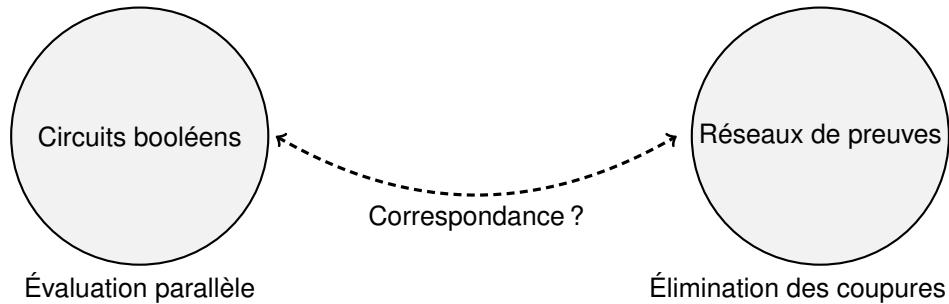
Circuits booléens

Évaluation parallèle

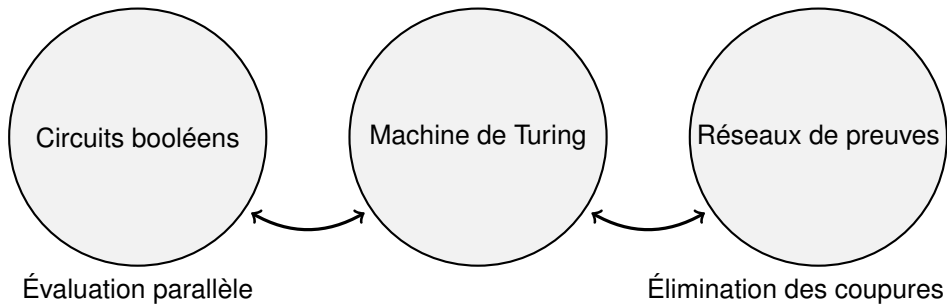
Correspondance ?

Réseaux de preuves

Élimination des coupures

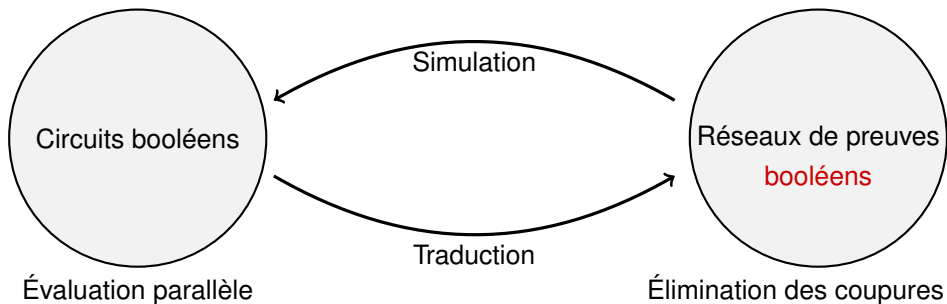


Deux modèles du calcul parallèle




Problème : linéarise le temps de calcul.

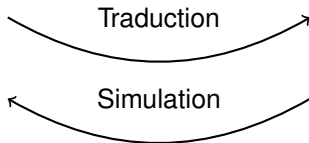
Deux modèles du calcul parallèle



- Profondeur
- Taille
- Uniformité
- Ressources allouées à la transformation

Tableau de correspondance

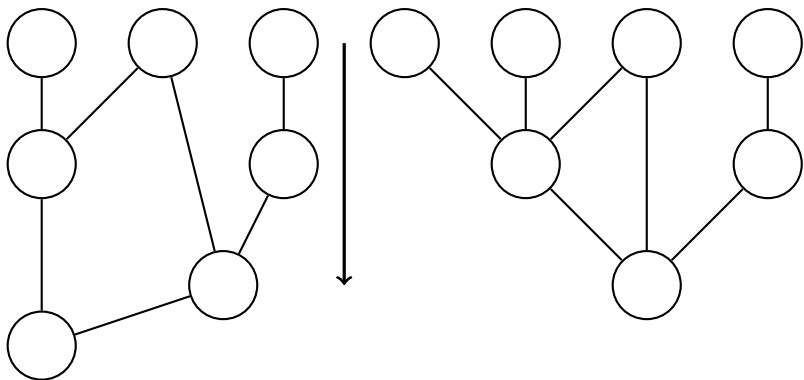
	Circuits booléens	Réseaux booléens
Entrées	Valeurs booléennes 0 et 1	Réseaux de preuve de type booléen 
Profondeur	Chemin maximal	Formule de coupure
Taille	Nombre de nœuds	Nombre de liens
Calcul	Évaluation parallèle	Élimination des coupures



- 1 **Circuits booléens**
- 2 Simulation
- 3 Réseaux booléens
- 4 Exemples et composition
- 5 Circuits de preuve
- 6 Résultats

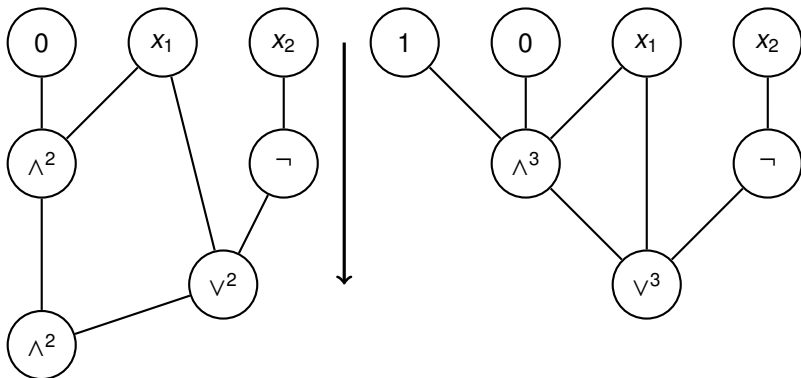
Circuits booléens, familles de circuits

Exemples (Circuits booléens)



Circuits booléens, familles de circuits

Exemples (Circuits booléens)



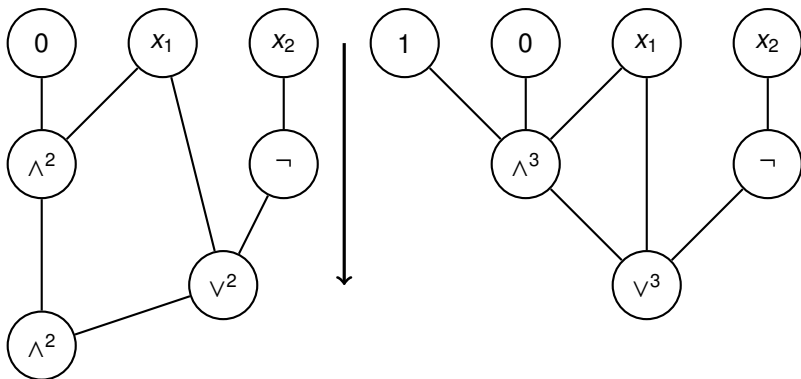
Définition (Bases)

$$\mathcal{B}_0 = \{\neg, \wedge^2, \vee^2\}$$

$$\mathcal{B}_1 = \{\neg, (\wedge^n)_{n \geq 2}, (\vee^n)_{n \geq 2}\}.$$

Circuits booléens, familles de circuits

Exemples (Circuits booléens)



Définition (Uniformité)

Une famille de circuits $C = (C_n)_{n \in \mathbb{N}}$ est *uniforme* s'il existe une machine de Turing déterministe qui étant donné n et le nom du nœud g peut déterminer toutes les informations sur le nœud g de C_n .

Définition (NC^i (resp. AC^i))

Pour $i \in \mathbb{N}$, ensemble des fonctions booléennes calculables par familles de circuits booléens uniformes, où pour chaque circuit ayant n entrées,

- sa profondeur est bornée par $\mathcal{O}(\log^i n)$,
- sa taille est polynomiale en n ,
- ses nœuds sont étiquetés par des fonctions de \mathfrak{B}_0 (resp. \mathfrak{B}_1).

$$NC = \bigcup_{i \in \mathbb{N}} NC^i \text{ et } AC = \bigcup_{i \in \mathbb{N}} AC^i.$$

Définition (NC^i (resp. AC^i))

Pour $i \in \mathbb{N}$, ensemble des fonctions booléennes calculables par familles de circuits booléens uniformes, où pour chaque circuit ayant n entrées,

- sa **profondeur est bornée par $\mathcal{O}(\log^i n)$** ,
- sa **taille est polynomiale en n** ,
- ses nœuds sont étiquetés par des fonctions de \mathfrak{B}_0 (resp. \mathfrak{B}_1).

$$NC = \bigcup_{i \in \mathbb{N}} NC^i \text{ et } AC = \bigcup_{i \in \mathbb{N}} AC^i.$$

Définition ($UstCONN_2$)

Étant donné le codage d'un graphe non-dirigé de degré 2 et les numéros de deux sommets, cette fonction détermine s'il existe un chemin entre ces deux sommets.

$$UstCONN_2 \in L$$

Définition (NC^i (resp. AC^i))

Pour $i \in \mathbb{N}$, ensemble des fonctions booléennes calculables par familles de circuits booléens uniformes, où pour chaque circuit ayant n entrées,

- sa **profondeur est bornée par $\mathcal{O}(\log^i n)$** ,
- sa **taille est polynomiale en n** ,
- ses nœuds sont étiquetés par des fonctions de \mathfrak{B}_0 (resp. \mathfrak{B}_1).

$$NC = \bigcup_{i \in \mathbb{N}} NC^i \text{ et } AC = \bigcup_{i \in \mathbb{N}} AC^i.$$

Théorème

Pour tout $k \geq 0$, $NC^k \subseteq AC^k \subseteq NC^{k+1}$.

$$AC^0 \subseteq NC^1 \subseteq L \subseteq NL \subseteq AC^1$$

$$AC^0(\text{UstCONN}_2) \subseteq AC^1$$

Théorème ([Terui, 2004])

Pour tout circuit booléen C de taille $|C|$ et de profondeur $p(C)$ sur la base $\mathfrak{B}_1(\text{UstCONN}_2)$, il existe un réseau de preuve booléen de taille $\mathcal{O}(|C|^4)$ et de profondeur $\mathcal{O}(p(C))$ qui accepte le même ensemble.

Problèmes :

- 1 $\text{UstCONN}_2 \in L$
- 2 Concernant \mathfrak{B}_0 ?

Théorème ([Aubert, 2010])

Pour tout circuit booléen C de taille $|C|$ et de profondeur $p(C)$ sur la base \mathfrak{B}_0 (resp. \mathfrak{B}_1), il existe un réseau de preuve booléen de taille $\mathcal{O}(|C|)$ (resp. $\mathcal{O}(|C|^2)$) et de profondeur $\mathcal{O}(p(C))$ qui accepte le même ensemble.

Problèmes :

- 1 $UstCONN_2 \in L$
- 2 Concernant \mathfrak{B}_0 ?

Théorème ([Aubert, 2010])

Pour tout circuit booléen C de taille $|C|$ et de profondeur $p(C)$ sur la base \mathfrak{B}_0 (resp. \mathfrak{B}_1), il existe un réseau de preuve booléen de taille $\mathcal{O}(|C|)$ (resp. $\mathcal{O}(|C|^2)$) et de profondeur $\mathcal{O}(p(C))$ qui accepte le même ensemble.

Problèmes :

- 1 $UstCONN_2 \in L$
- 2 Concernant \mathfrak{B}_0 ?

Théorème ([Mogbil et Rahli, 2007])

Pour tout $i \in \mathbb{N}$, la traduction d'une famille de circuits booléens appartenant à $AC^i(UstCONN_2)$ vers une famille de réseaux booléens de mBN^i est dans L .

Théorème ([Aubert, 2010])

Pour tout circuit booléen C de taille $|C|$ et de profondeur $p(C)$ sur la base \mathfrak{B}_0 (resp. \mathfrak{B}_1), il existe un réseau de preuve booléen de taille $\mathcal{O}(|C|)$ (resp. $\mathcal{O}(|C|^2)$) et de profondeur $\mathcal{O}(p(C))$ qui accepte le même ensemble.

Problèmes :

- 1 $\text{UstCONN}_2 \in L$
- 2 Concernant \mathfrak{B}_0 ?

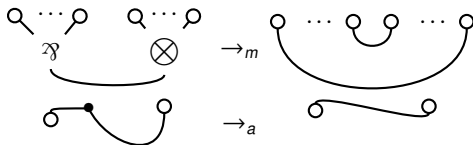
Théorème ([Aubert, 2010])

Pour tout $i \in \mathbb{N}$, la traduction d'une famille de circuits booléens appartenant à AC^i ou NC^i vers une famille de réseaux booléens de CCP^i est dans AC^0 .

- ① Circuits booléens
- ② **Simulation**
- ③ Réseaux booléens
- ④ Exemples et composition
- ⑤ Circuits de preuve
- ⑥ Résultats

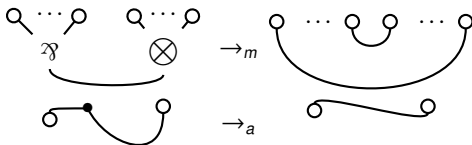
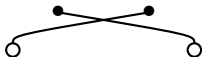
Définition (\rightarrow_m et \rightarrow_a)

Soit $\circ \in \{\bullet, (\mathcal{X}^n)_{n \geq 2}, (\otimes^n)_{n \geq 2}\}$.

Définition (t -réduction)

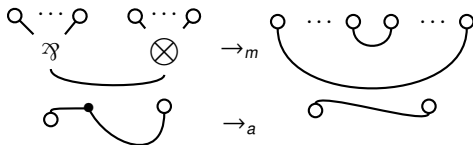
Définition (\rightarrow_m et \rightarrow_a)

Soit $\circ \in \{\bullet, (\mathcal{X}^n)_{n \geq 2}, (\otimes^n)_{n \geq 2}\}$.

Définition (t -réduction)

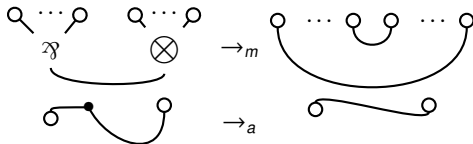
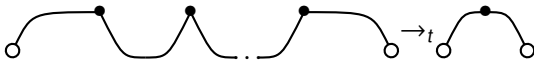
Définition (\rightarrow_m et \rightarrow_a)

Soit $\circ \in \{\bullet, (\mathcal{X}^n)_{n \geq 2}, (\otimes^n)_{n \geq 2}\}$.

Définition (t -réduction)

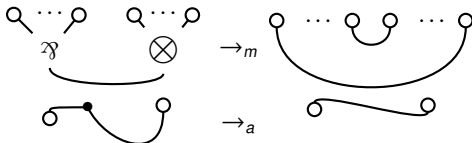
Définition (\rightarrow_m et \rightarrow_a)

Soit $\circ \in \{\bullet, (\otimes^n)_{n \geq 2}\}$.

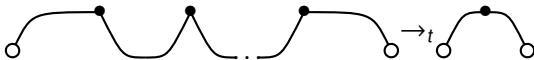
Définition (t -réduction)

Définition (\rightarrow_m et \rightarrow_a)

Soit $\circ \in \{\bullet, (\mathcal{X}^n)_{n \geq 2}, (\otimes^n)_{n \geq 2}\}$.



Définition (t -réduction)



Théorème ([Terui, 2004])

Pour tout réseau de preuve P de taille $|P|$ et de profondeur $d(P)$, il existe un circuit booléen C de taille $\mathcal{O}(|P|^4)$ et de profondeur $\mathcal{O}(d(P))$ sur la base $\mathfrak{B}_1(\text{UstCONN}_2)$ qui accepte le même ensemble que P .

- 1 Circuits booléens
- 2 Simulation
- 3 **Réseaux booléens**
- 4 Exemples et composition
- 5 Circuits de preuve
- 6 Résultats

Définition (Les règles de **MLLu**)

$$\frac{}{\vdash A, A^\perp} \text{ax.} \quad \frac{\vdash \Gamma_1, A_1 \quad \dots \quad \vdash \Gamma_n, A_n}{\vdash \Gamma_1, \dots, \Gamma_n, \otimes^n(A_1, \dots, A_n)} \otimes^n$$

$$\frac{\vdash \Gamma, A \quad \vdash \Delta, A^\perp}{\vdash \Gamma, \Delta} \text{cut} \quad \frac{\vdash \Gamma, A_n, \dots, A_1}{\vdash \Gamma, \wp^n(A_n, \dots, A_1)} \wp^n$$

Définition (Le type booléen, [Terui, 2004])

Le type booléen **B** est défini comme étant $\wp^3(\alpha^\perp, \alpha^\perp, \alpha \otimes \alpha)$.

$$\frac{\frac{\frac{}{\vdash \alpha^\perp, \alpha} \text{ax.} \quad \frac{}{\vdash \alpha^\perp, \alpha} \text{ax.}}{\vdash \alpha^\perp, \alpha^\perp, \alpha \otimes \alpha} \otimes^2}{\vdash \wp^3(\alpha^\perp, \alpha^\perp, \alpha \otimes \alpha)} \wp^3$$

Définition (Les règles de MLLu)

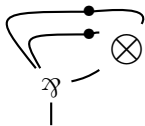
$$\frac{}{\vdash A, A^\perp} \text{ ax.} \qquad \frac{\vdash \Gamma_1, A_1 \quad \dots \quad \vdash \Gamma_n, A_n}{\vdash \Gamma_1, \dots, \Gamma_n, \otimes^n(A_1, \dots, A_n)} \otimes^n$$

$$\frac{\vdash \Gamma, A \quad \vdash \Delta, A^\perp}{\vdash \Gamma, \Delta} \text{ cut} \qquad \frac{\vdash \Gamma, A_n, \dots, A_1}{\vdash \Gamma, \wp^n(A_n, \dots, A_1)} \wp^n$$

Définition (Le type booléen, [Terui, 2004])

Le type booléen **B** est défini comme étant $\wp^3(\alpha^\perp, \alpha^\perp, \alpha \otimes \alpha)$.

$$\frac{\frac{\frac{}{\vdash \alpha^\perp, \alpha} \text{ ax.} \quad \frac{}{\vdash \alpha^\perp, \alpha} \text{ ax.}}{\vdash \alpha^\perp, \alpha^\perp, \alpha \otimes \alpha} \otimes^2}{\vdash \wp^3(\alpha^\perp, \alpha^\perp, \alpha \otimes \alpha)} \wp^3$$



Définition (Les règles de MLLu)

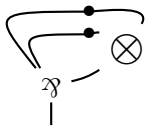
$$\frac{}{\vdash A, A^\perp} ax. \quad \frac{\vdash \Gamma_1, A_1 \quad \dots \quad \vdash \Gamma_n, A_n}{\vdash \Gamma_1, \dots, \Gamma_n, \otimes^n(A_1, \dots, A_n)} \otimes^n$$

$$\frac{\vdash \Gamma, A \quad \vdash \Delta, A^\perp}{\vdash \Gamma, \Delta} cut \quad \frac{\vdash \Gamma, A_n, \dots, A_1}{\vdash \Gamma, \wp^n(A_n, \dots, A_1)} \wp^n$$

Définition (Le type booléen, [Terui, 2004])

Le type booléen **B** est défini comme étant $\wp^3(\alpha^\perp, \alpha^\perp, \alpha \otimes \alpha)$.

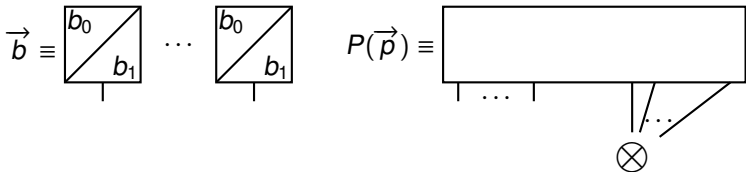
$$\frac{\frac{\frac{}{\vdash p : \alpha^\perp, p : \alpha \triangleright ax_p} ax. \quad \frac{}{\vdash q : \alpha^\perp, q : \alpha \triangleright ax_q} ax.}{\vdash p : \alpha^\perp, q : \alpha^\perp, r : \alpha \otimes \alpha \triangleright tenseur_r^{p,q}(ax_p, ax_q)} \otimes^2}{\vdash s : \wp^3(\alpha^\perp, \alpha^\perp, \alpha \otimes \alpha) \triangleright par_s^{q,p,r}(tenseur_r^{p,q}(ax_p, ax_q))} \wp^3$$



Définition (Réseau de preuve booléen, [Terui, 2004])

Un réseau de preuve booléen à n entrées est un réseau de preuve $P(\vec{p})$ de type

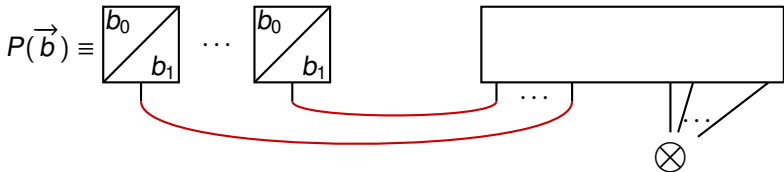
$$\vdash p_1 : \mathbf{B}^\perp[A_1], \dots, p_n : \mathbf{B}^\perp[A_n], s : \otimes^{1+m}(\mathbf{B}[A], C_1, \dots, C_m)$$

Définition ($P(\vec{b})$)

Définition (Réseau de preuve booléen, [Terui, 2004])

Un réseau de preuve booléen à n entrées est un réseau de preuve $P(\vec{p})$ de type

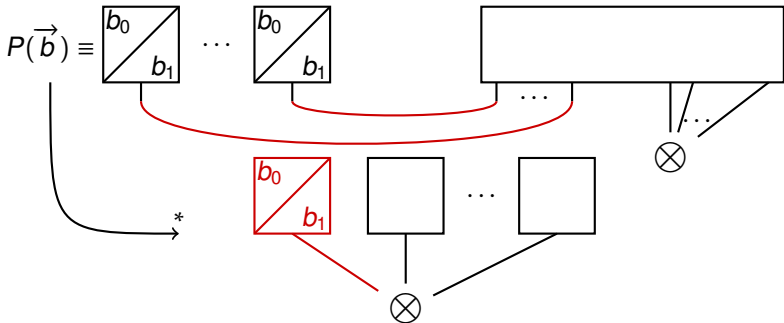
$$\vdash p_1 : \mathbf{B}^\perp[A_1], \dots, p_n : \mathbf{B}^\perp[A_n], s : \otimes^{1+m}(\mathbf{B}[A], C_1, \dots, C_m)$$

Définition ($P(\vec{b})$)

Définition (Réseau de preuve booléen, [Terui, 2004])

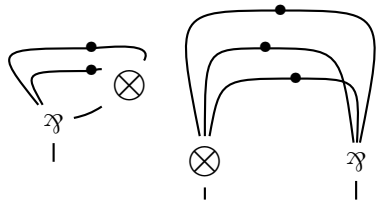
Un réseau de preuve booléen à n entrées est un réseau de preuve $P(\vec{p})$ de type

$$\vdash p_1 : \mathbf{B}^\perp[A_1], \dots, p_n : \mathbf{B}^\perp[A_n], s : \otimes^{1+m}(\mathbf{B}[A], C_1, \dots, C_m)$$

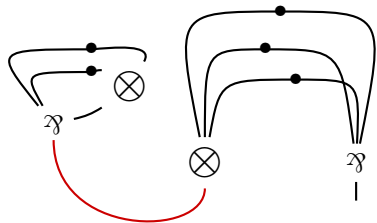
Définition ($P(\vec{b})$)

- ① Circuits booléens
- ② Simulation
- ③ Réseaux booléens
- ④ **Exemples et composition**
- ⑤ Circuits de preuve
- ⑥ Résultats

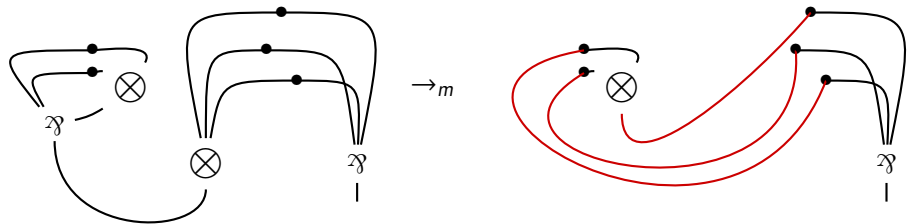
Un premier exemple : la négation



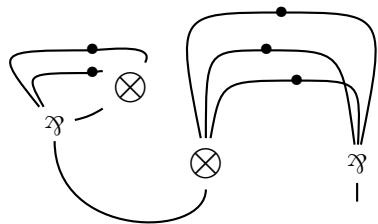
Un premier exemple : la négation



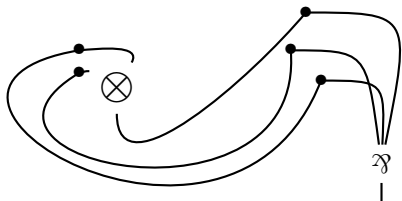
Un premier exemple : la négation



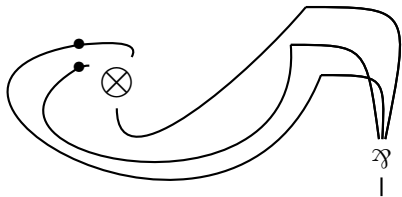
Un premier exemple : la négation



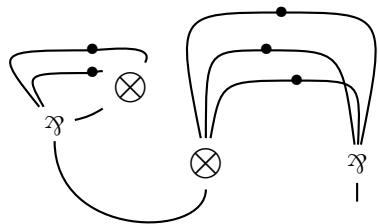
$\rightarrow m$



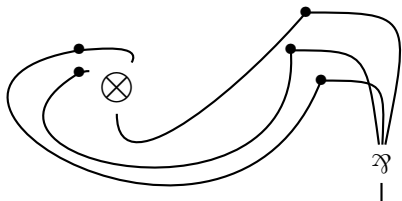
$\downarrow a$



Un premier exemple : la négation



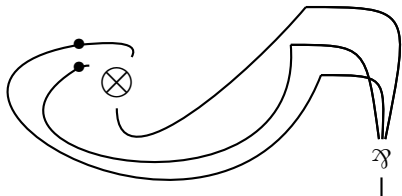
$\rightarrow m$



$\downarrow ev$

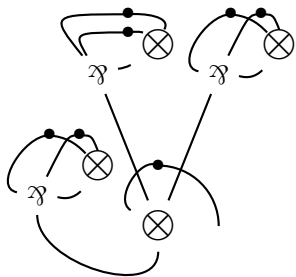


$\downarrow a$

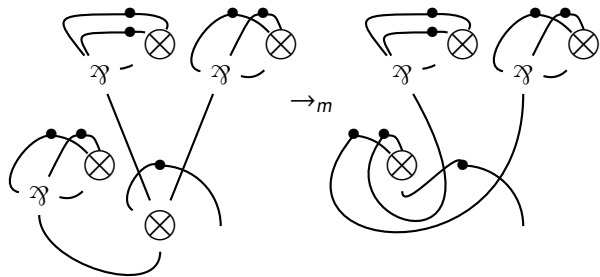


\equiv

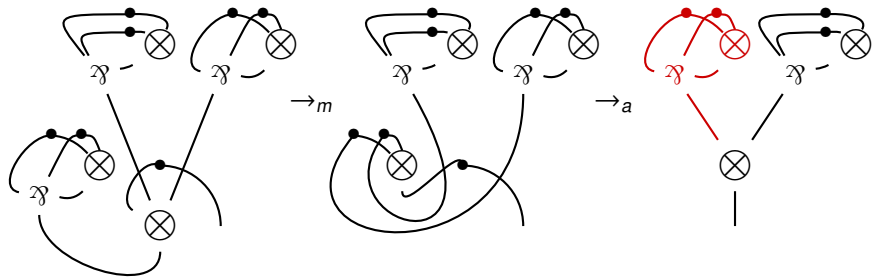
Second exemple : le conditionnel



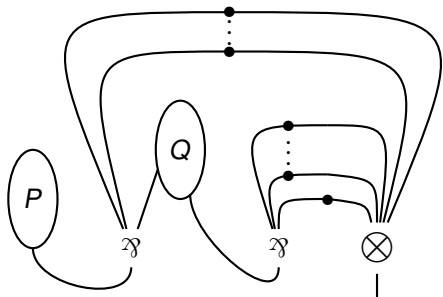
Second exemple : le conditionnel



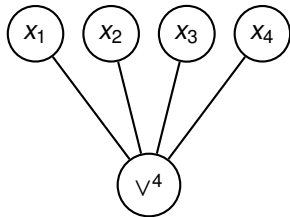
Second exemple : le conditionnel



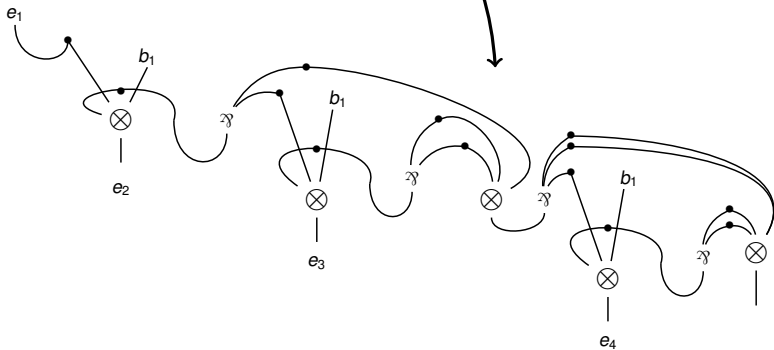
Nécessite de composer :



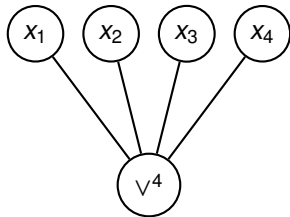
Un exemple de traduction



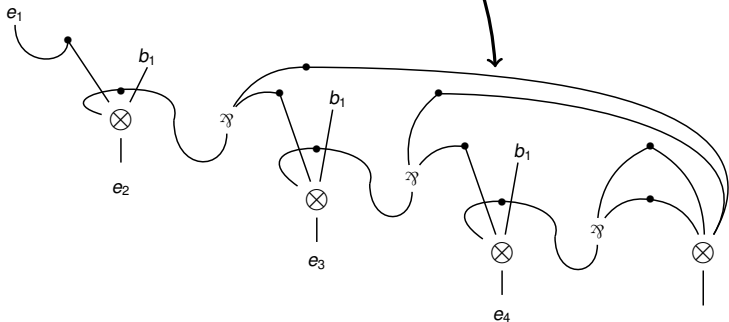
Traduction de [Terui, 2004]



Un exemple de traduction



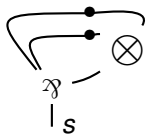
Traduction de [Aubert, 2010]



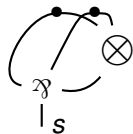
- ① Circuits booléens
- ② Simulation
- ③ Réseaux booléens
- ④ Exemples et composition
- ⑤ **Circuits de preuve**
- ⑥ Résultats

Pièces de circuits de preuves

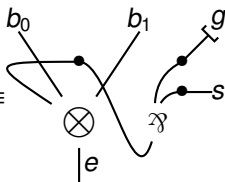
$b_0 \equiv$



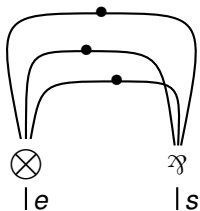
$b_1 \equiv$



$DUPL^1 \equiv$

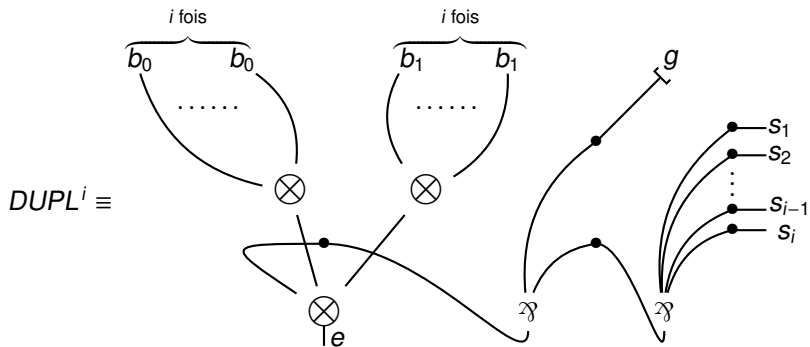


$NEG \equiv$



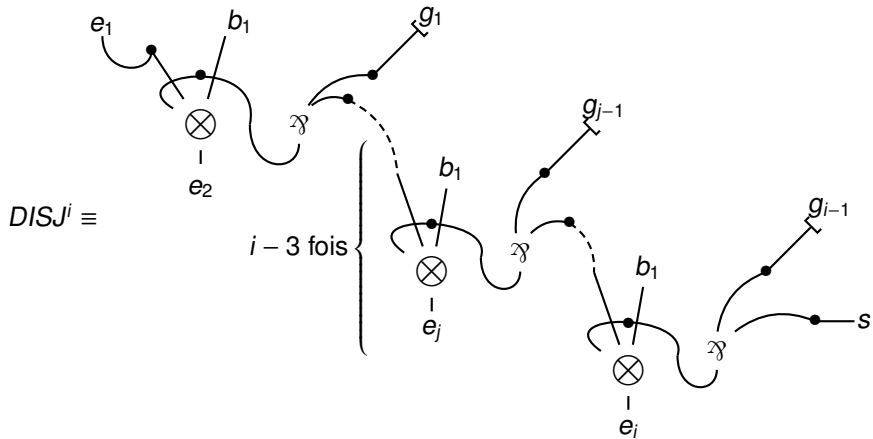
Pièces de circuits de preuves

On pose $2 \leq j \leq i$.



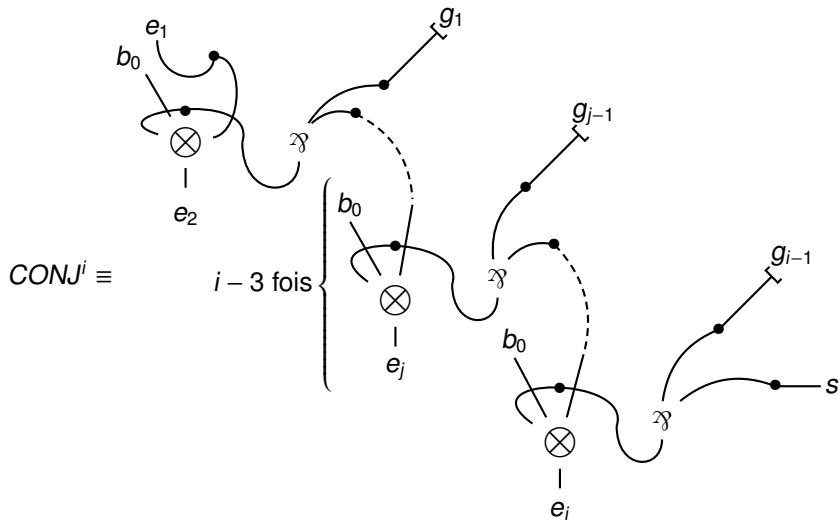
Pièces de circuits de preuves

On pose $2 \leq j \leq i$.



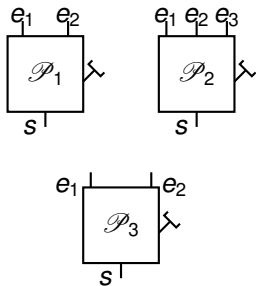
Pièces de circuits de preuves

On pose $2 \leq j \leq i$.



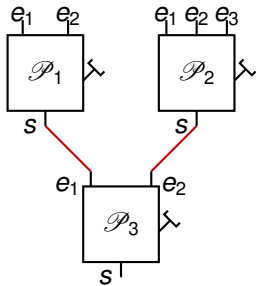
Composition de pièces et de circuits de preuves

Définition (Circuit de preuve)



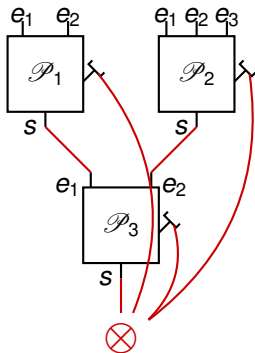
Composition de pièces et de circuits de preuves

Définition (Circuit de preuve)



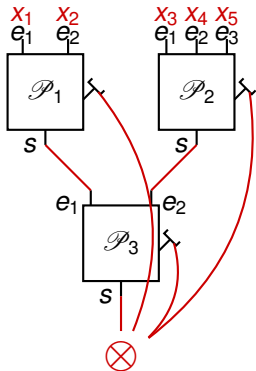
Composition de pièces et de circuits de preuves

Définition (Circuit de preuve)



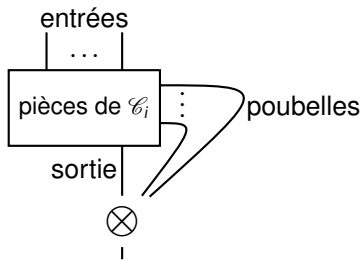
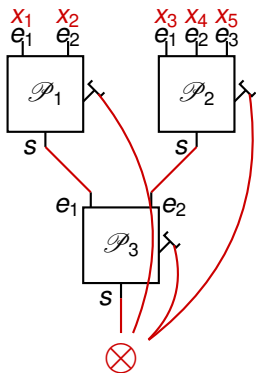
Composition de pièces et de circuits de preuves

Définition (Circuit de preuve)



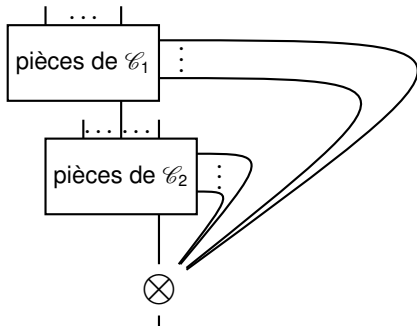
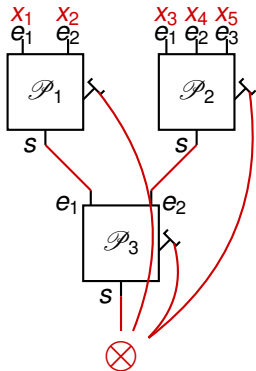
Composition de pièces et de circuits de preuves

Définition (Circuit de preuve)



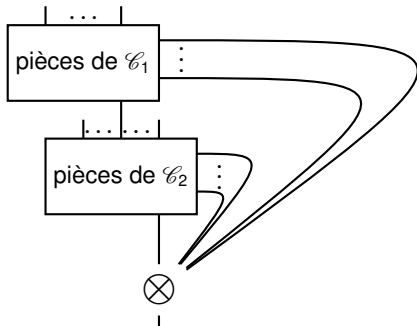
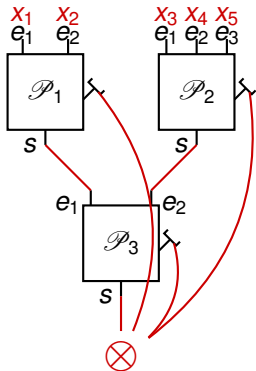
Composition de pièces et de circuits de preuves

Définition (Circuit de preuve)



Composition de pièces et de circuits de preuves

Définition (Circuit de preuve)

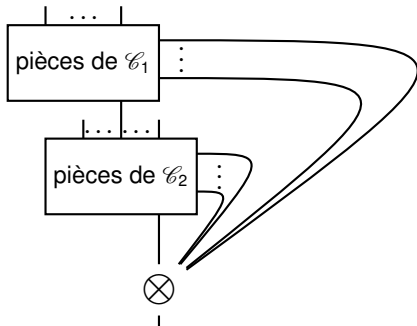
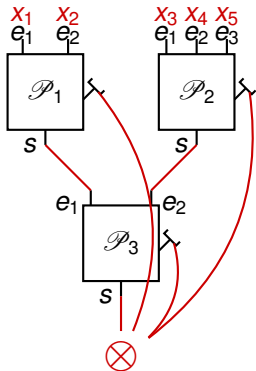


Théorème ([Aubert, 2010])

Tout circuit de preuve est un réseau de preuve booléen de **MLLu**.

Composition de pièces et de circuits de preuves

Définition (Circuit de preuve)



Lemme (Traduction)

Il est possible d'associer à tout circuit booléen C_n un circuit de preuve $\mathcal{T}(C_n)$ tel que si C_n s'évalue en i , $\mathcal{T}(C_n) \rightarrow_{ev} b_i$.

Soient C_n un circuit booléen, $p(C_n)$ sa profondeur, $|C_n|$ sa taille, et $\mathcal{T}(C_n)$ son traduit en circuit de preuve, de profondeur $d(\mathcal{T}(C_n))$ et de taille $|\mathcal{T}(C_n)|$.

Théorème (Profondeur de $\mathcal{T}(C_n)$, [Aubert, 2010])

$$d(\mathcal{T}(C_n)) = \mathcal{O}(p(C_n)).$$

Soient C_n un circuit booléen, $p(C_n)$ sa profondeur, $|C_n|$ sa taille, et $\mathcal{T}(C_n)$ son traduit en circuit de preuve, de profondeur $d(\mathcal{T}(C_n))$ et de taille $|\mathcal{T}(C_n)|$.

Théorème (Profondeur de $\mathcal{T}(C_n)$, [Aubert, 2010])

$$d(\mathcal{T}(C_n)) = \mathcal{O}(p(C_n)).$$

Démonstration

- Soit x_i l'entrée de $\mathcal{T}(C_n)$ où la formule de coupure est la plus profonde,
- le chemin de la sortie à x_i passe par au plus $p(C_n) \times 2$ pièces,
- on a donc $d(\mathcal{T}(C_n)) \leq p(C_n) \times 2 \times d(\mathbf{B})$.

Soient C_n un circuit booléen, $p(C_n)$ sa profondeur, $|C_n|$ sa taille, et $\mathcal{T}(C_n)$ son traduit en circuit de preuve, de profondeur $d(\mathcal{T}(C_n))$ et de taille $|\mathcal{T}(C_n)|$.

Théorème (Profondeur de $\mathcal{T}(C_n)$, [Aubert, 2010])

$$d(\mathcal{T}(C_n)) = \mathcal{O}(p(C_n)).$$

Théorème (Taille de $\mathcal{T}(C_n)$, [Aubert, 2010])

Si C_n appartient à une famille de circuits booléens comprise dans NC^i (resp. AC^i), $|\mathcal{T}(C_n)| = \mathcal{O}(|C_n|)$ (resp. $|\mathcal{T}(C_n)| = \mathcal{O}(|C_n|^2)$).

Soient C_n un circuit booléen, $p(C_n)$ sa profondeur, $|C_n|$ sa taille, et $\mathcal{T}(C_n)$ son traduit en circuit de preuve, de profondeur $d(\mathcal{T}(C_n))$ et de taille $|\mathcal{T}(C_n)|$.

Théorème (Profondeur de $\mathcal{T}(C_n)$, [Aubert, 2010])

$$d(\mathcal{T}(C_n)) = \mathcal{O}(p(C_n)).$$

Théorème (Taille de $\mathcal{T}(C_n)$, [Aubert, 2010])

Si C_n appartient à une famille de circuits booléens comprise dans NC^i (resp. AC^i), $|\mathcal{T}(C_n)| = \mathcal{O}(|C_n|)$ (resp. $|\mathcal{T}(C_n)| = \mathcal{O}(|C_n|^2)$).

Démonstration

- Soit k le nombre d'arrêtes de C_n , $k \leq 2 \times |C_n|$ (resp. $k \leq |C_n|^2$),
- un nœud de C_n d'arité entrante n et sortante m est représenté par un réseau de preuve de taille au plus $9(n + m)$,
- la somme des arités entrantes et sortantes de l'ensemble des nœuds de C_n ne peut dépasser k .

- ① Circuits booléens
- ② Simulation
- ③ Réseaux booléens
- ④ Exemples et composition
- ⑤ Circuits de preuve
- ⑥ **Résultats**

Définition (NC^i (resp. AC^i))

Pour $i \in \mathbb{N}$, ensemble des fonctions booléennes calculables par familles de circuits booléens uniformes, où pour chaque circuit ayant n entrées,

- sa profondeur est bornée par $\mathcal{O}(\log^i n)$,
- sa taille est polynomiale en n ,
- ses nœuds sont étiquetés par des fonctions de \mathfrak{B}_0 (resp. \mathfrak{B}_1).

$$NC = \bigcup_{i \in \mathbb{N}} NC^i \text{ et } AC = \bigcup_{i \in \mathbb{N}} AC^i$$

Définition (APN^i , [Terui, 2004] (resp. mBN^i , [Mogbil et Rahli, 2007]))

Pour $i \in \mathbb{N}$, ensemble des fonctions booléennes calculables par familles de réseaux booléens non-uniformes (resp. uniformes), où pour chaque circuit ayant n entrées,

- sa profondeur est bornée par $\mathcal{O}(\log^i n)$,
- sa taille est polynomiale en n .

$$APN = \bigcup_{i \in \mathbb{N}} APN^i \quad (\text{resp. } mBN = \bigcup_{i \in \mathbb{N}} mBN^i)$$

Définition (CCP^i [Aubert, 2010])

Pour $i \in \mathbb{N}$, ensemble des fonctions booléennes calculables par familles de circuits de preuves *uniformes*, où pour chaque circuit ayant n entrées,

- sa profondeur est bornée par $\mathcal{O}(\log^i n)$,
- sa taille est polynomiale en n .

$$CCP = \bigcup_{i \in \mathbb{N}} CCP^i$$

Définition (Traduction de AC^i vers CCP^i)

On pose le problème suivant :

Entrée : Une description d'une famille de circuits booléens appartenant à AC^i .

Sortie : Une description d'une famille de circuits de preuves appartenant à CCP^i tels que le résultat de l'évaluation *via* élimination des coupures de chaque circuit de preuve coïncide avec le résultat de l'évaluation du circuit booléen correspondant.

Définition (Traduction de AC^i vers CCP^i)

On pose le problème suivant :

Entrée : Une description d'une famille de circuits booléens appartenant à AC^i .

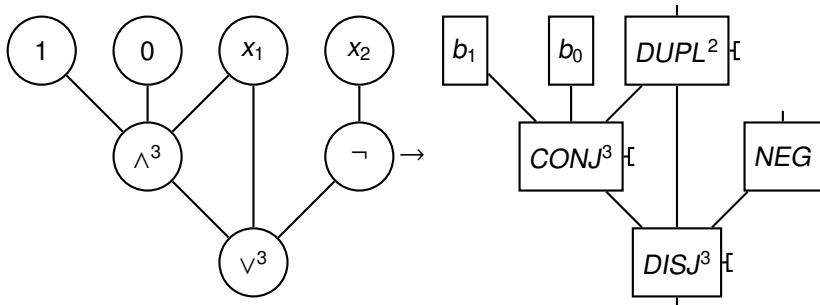
Sortie : Une description d'une famille de circuits de preuves appartenant à CCP^i tels que le résultat de l'évaluation *via* élimination des coupures de chaque circuit de preuve coïncide avec le résultat de l'évaluation du circuit booléen correspondant.

Théorème

Traduction de AC^i vers CCP^i appartient à AC^0 .

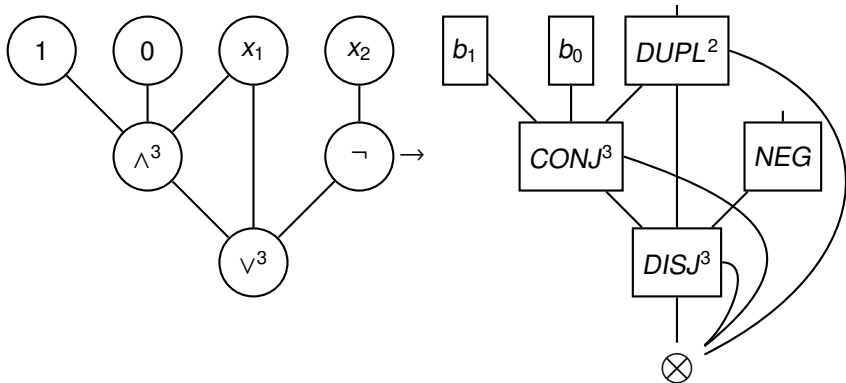
Théorème

Traduction de AC^i vers CCP^i appartient à AC^0 .



Théorème

Traduction de AC^i vers CCP^i appartient à AC^0 .



Théorème

Pour $i \in \mathbb{N}$, $AC^i \subseteq CCP^i$.

Remarque

Pour $i \in \mathbb{N}$, $CCP^i \subseteq mBN^i$.

Remarque

$AC^0 \subseteq CCP^0 \subseteq AC^0(UstCONN_2)$.



AUBERT, C. (2010).

Réseaux de preuves booléens sous-logarithmiques.
Mémoire de M2 L.M.F.I., Paris VII, L.I.P.N.



MOGBIL, V. et RAHLI, V. (2007).

Uniform circuits, & Boolean proof nets.
In Proceedings of L.F.C.S., pages 401–421. Springer.



TERUI, K. (2004).

Proof Nets and Boolean Circuits.
In Proceedings of LICS'04, pages 182–191.