Réseaux de preuves booléens sous-logarithmiques

Mémoire en vue de l'obtention du M2 L.M.F.I.
à l'Université Paris VII

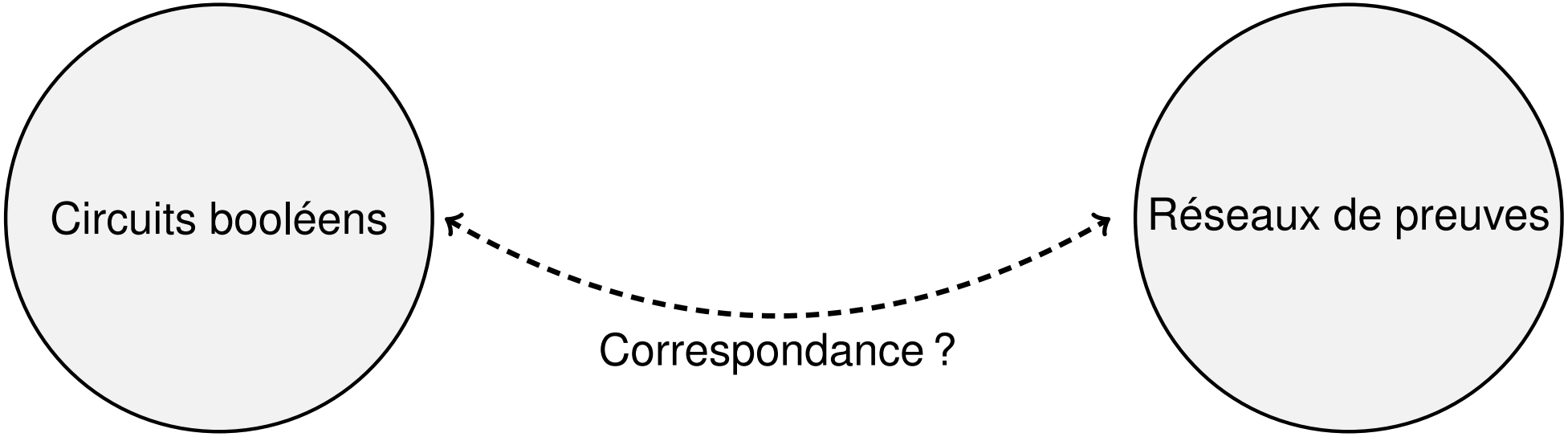
Encadrants :
V. Mogbil (L.I.P.N. - Université Paris XIII)
P. Jacobé de Naurois (L.I.P.N. - C.N.R.S.)

Clément Aubert

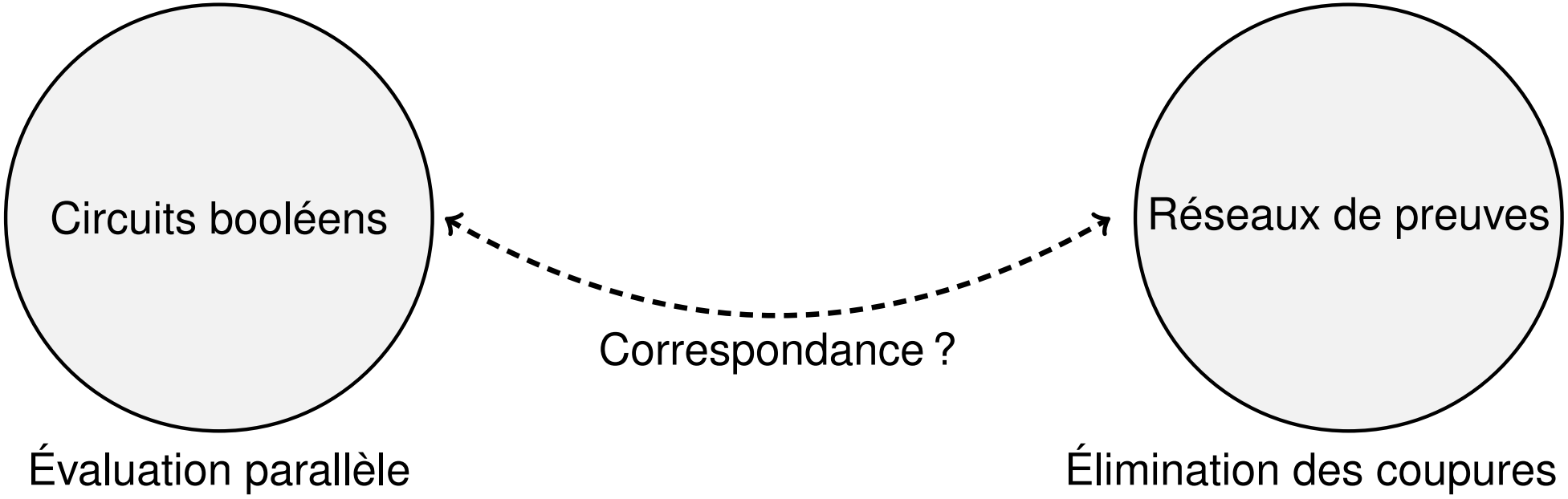
Institut Galilée - Université Paris-Nord
99, avenue Jean-Baptiste Clément
93430 Villetaneuse

23 septembre 2010

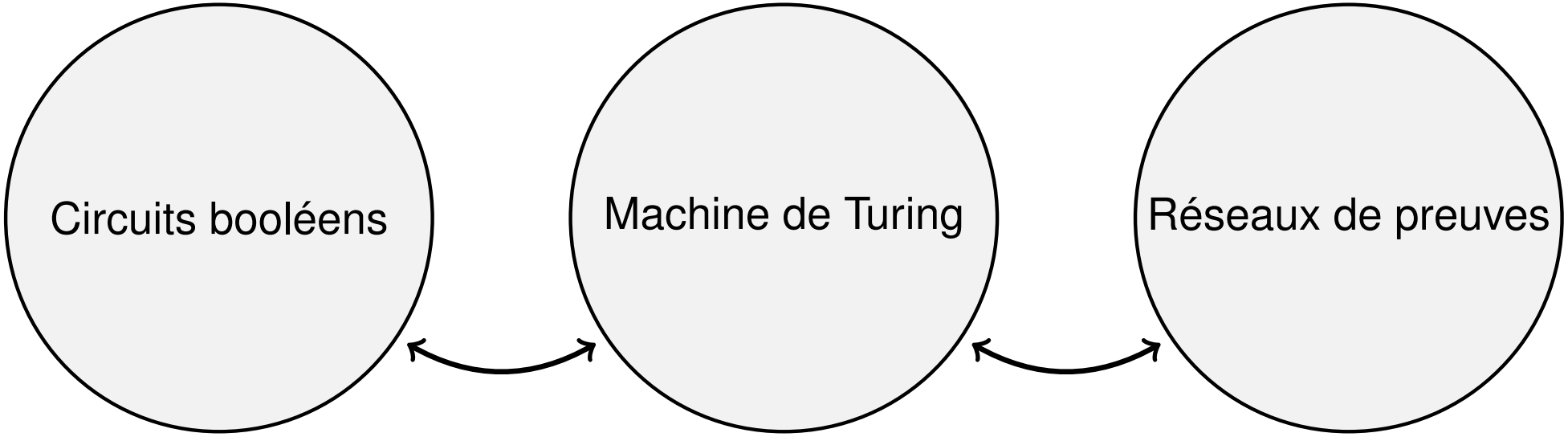
Deux modèles du calcul parallèle



Deux modèles du calcul parallèle



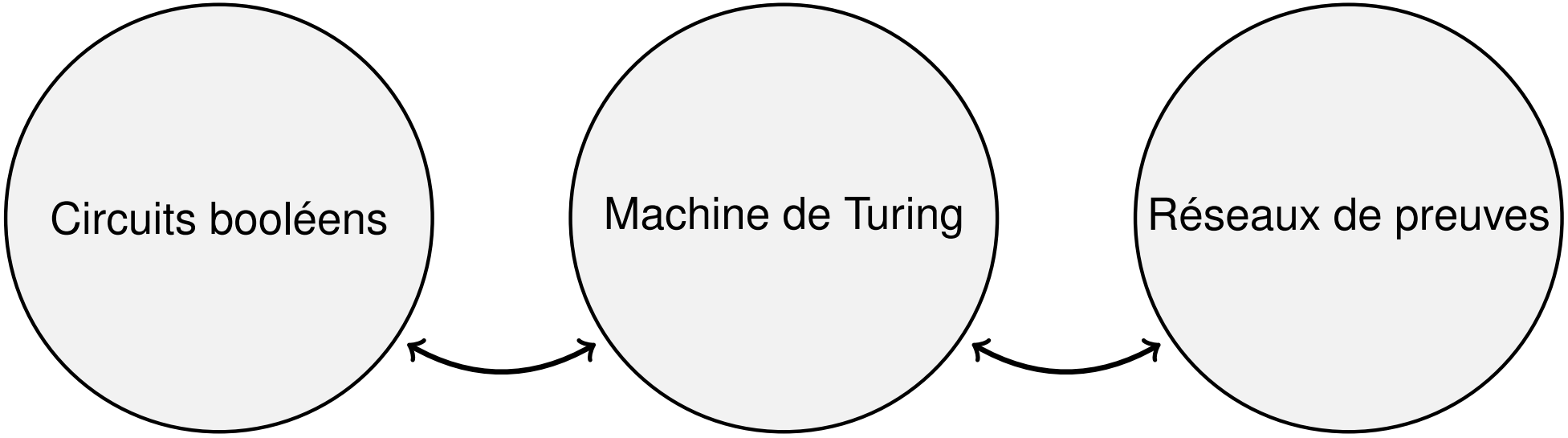
Deux modèles du calcul parallèle



Évaluation parallèle

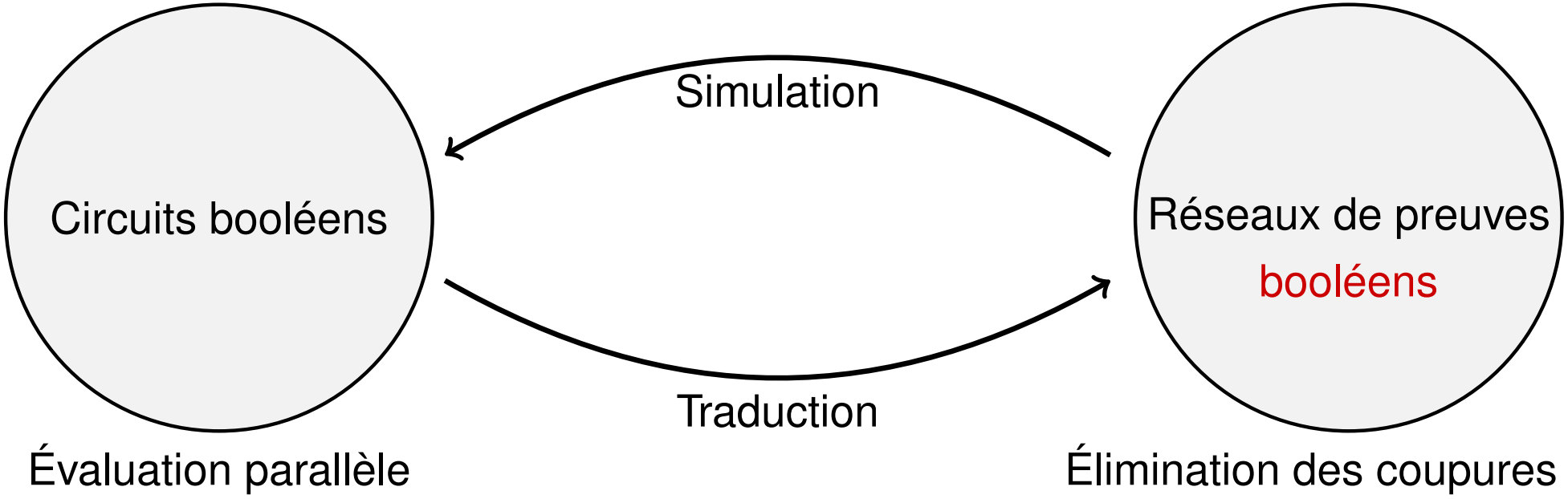
Élimination des coupures

Deux modèles du calcul parallèle

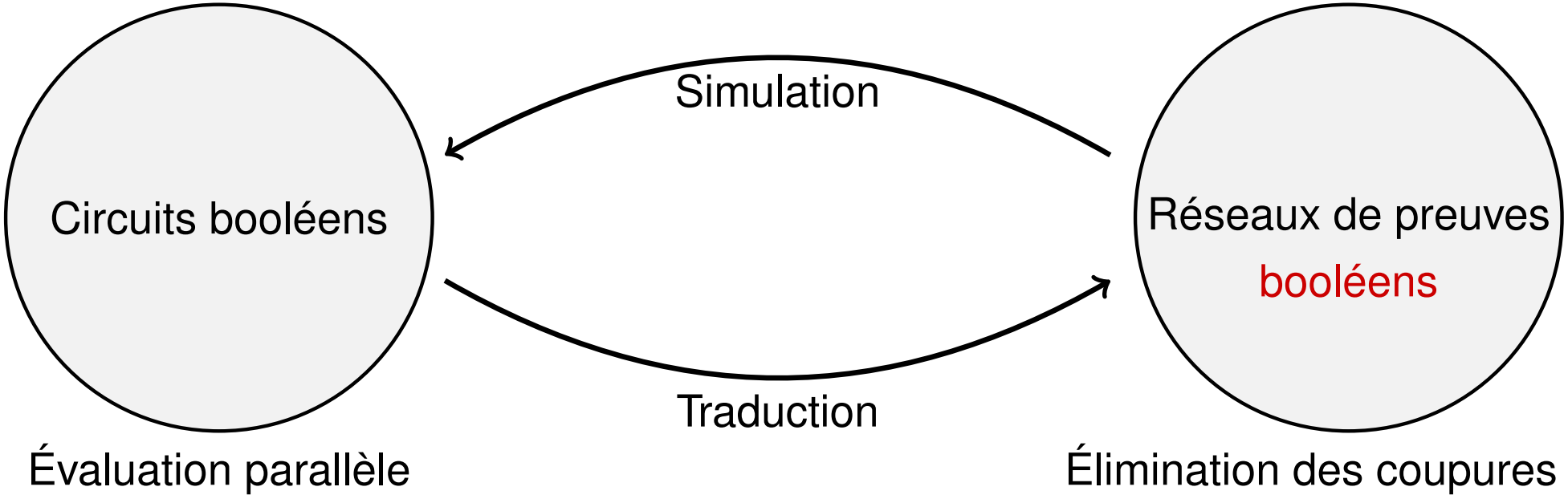


Problème : linéarise le temps de calcul.

Deux modèles du calcul parallèle

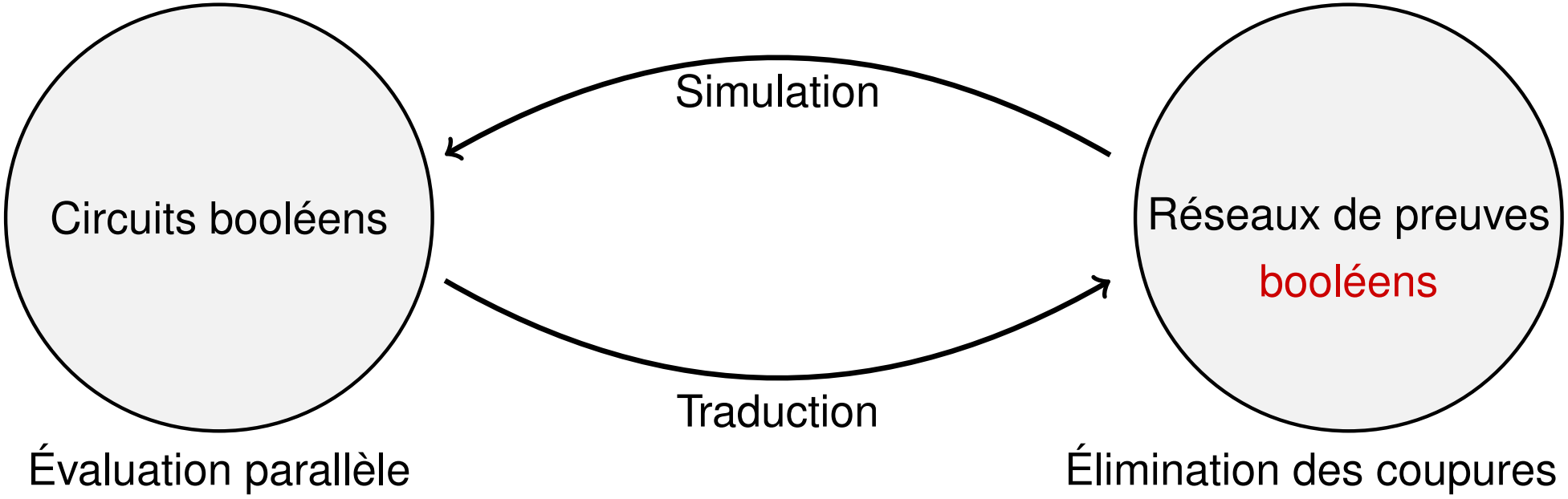


Deux modèles du calcul parallèle



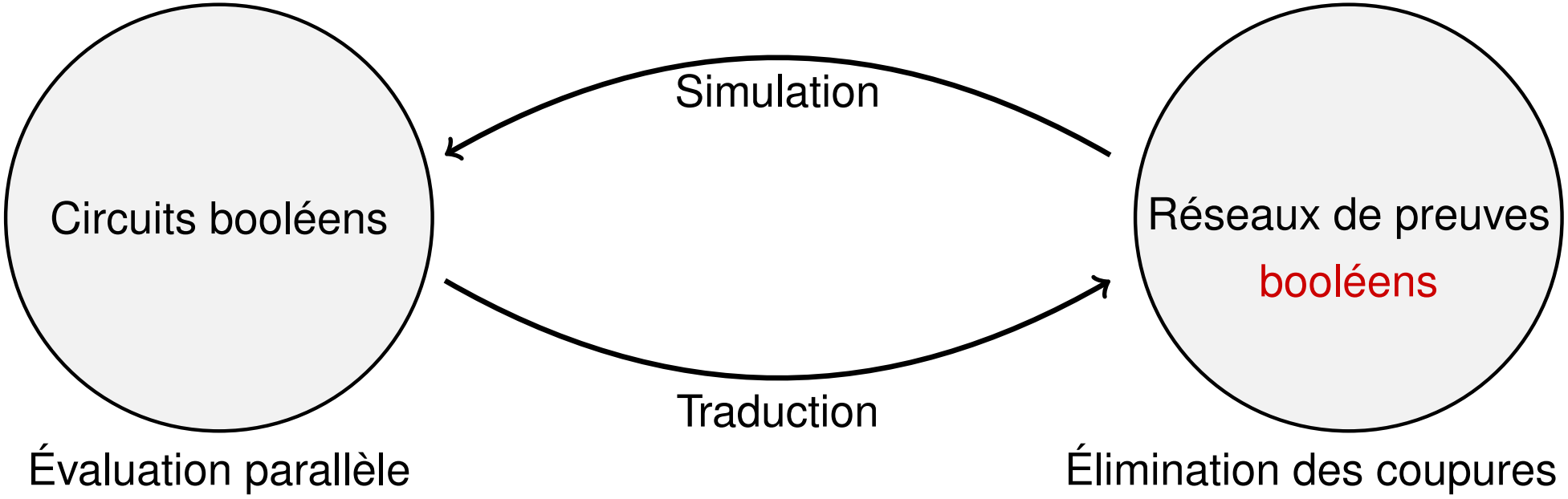
- Profondeur
- Taille

Deux modèles du calcul parallèle



- Profondeur
- Taille
- Uniformité

Deux modèles du calcul parallèle



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

Tableau de correspondance

	Circuits booléens	**Réseaux booléens**
Entrées	Valeurs booléennes	Réseaux de preuve de type booléen

Tableau de correspondance

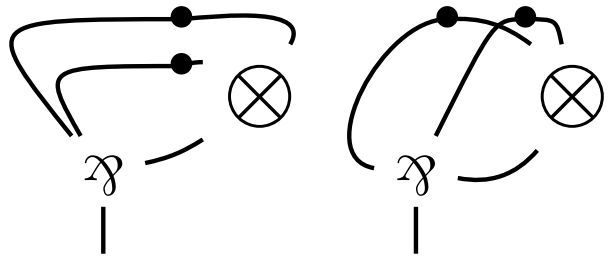
	Circuits booléens	**Réseaux booléens**
Entrées	Valeurs booléennes 0 et 1	Réseaux de preuve de type booléen 

Tableau de correspondance

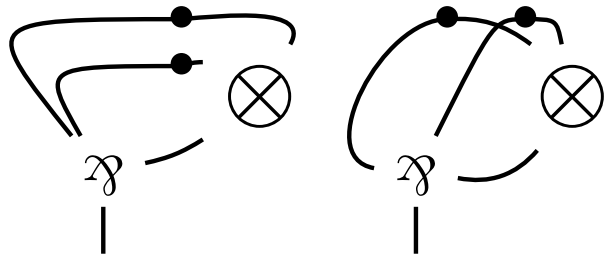
	Circuits booléens	**Réseaux booléens**
Entrées	Valeurs booléennes 0 et 1	Réseaux de preuve de type booléen 
Profondeur	Chemin maximal	Formule de coupure

Tableau de correspondance

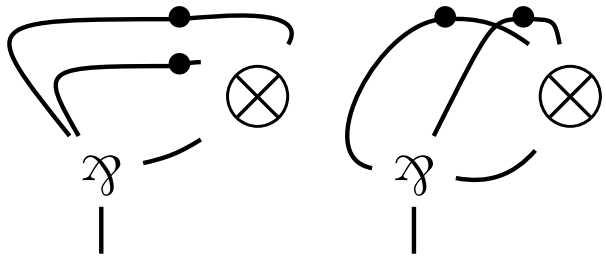
	Circuits booléens	**Réseaux booléens**
Entrées	Valeurs booléennes 0 et 1	Réseaux de preuve de type booléen 
Profondeur	Chemin maximal	Formule de coupure
Taille	Nombre de nœuds	Nombre de liens

Tableau de correspondance

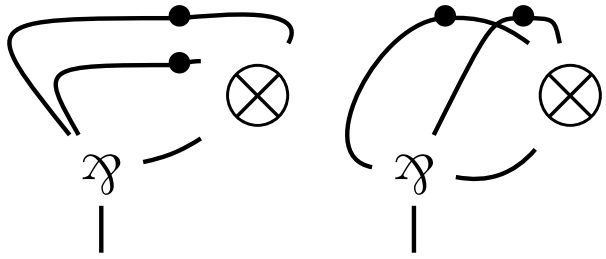
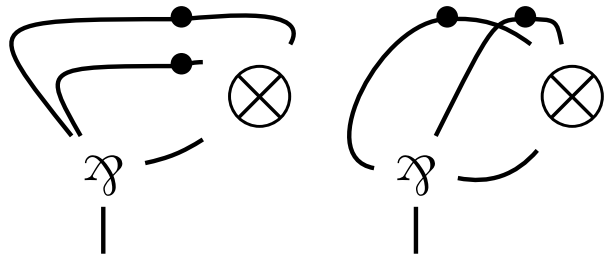
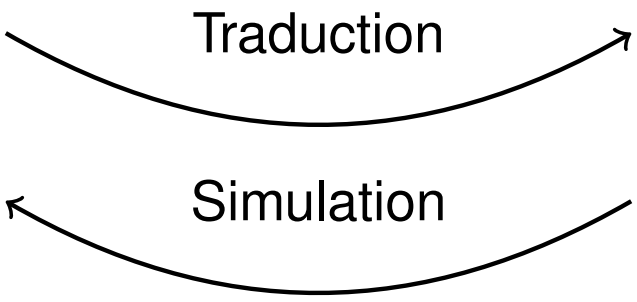
	Circuits booléens	**Réseaux booléens**
Entrées	Valeurs booléennes 0 et 1	Réseaux de preuve de type booléen 
Profondeur	Chemin maximal	Formule de coupure
Taille	Nombre de nœuds	Nombre de liens
Calcul	Évaluation parallèle	Élimination des coupures

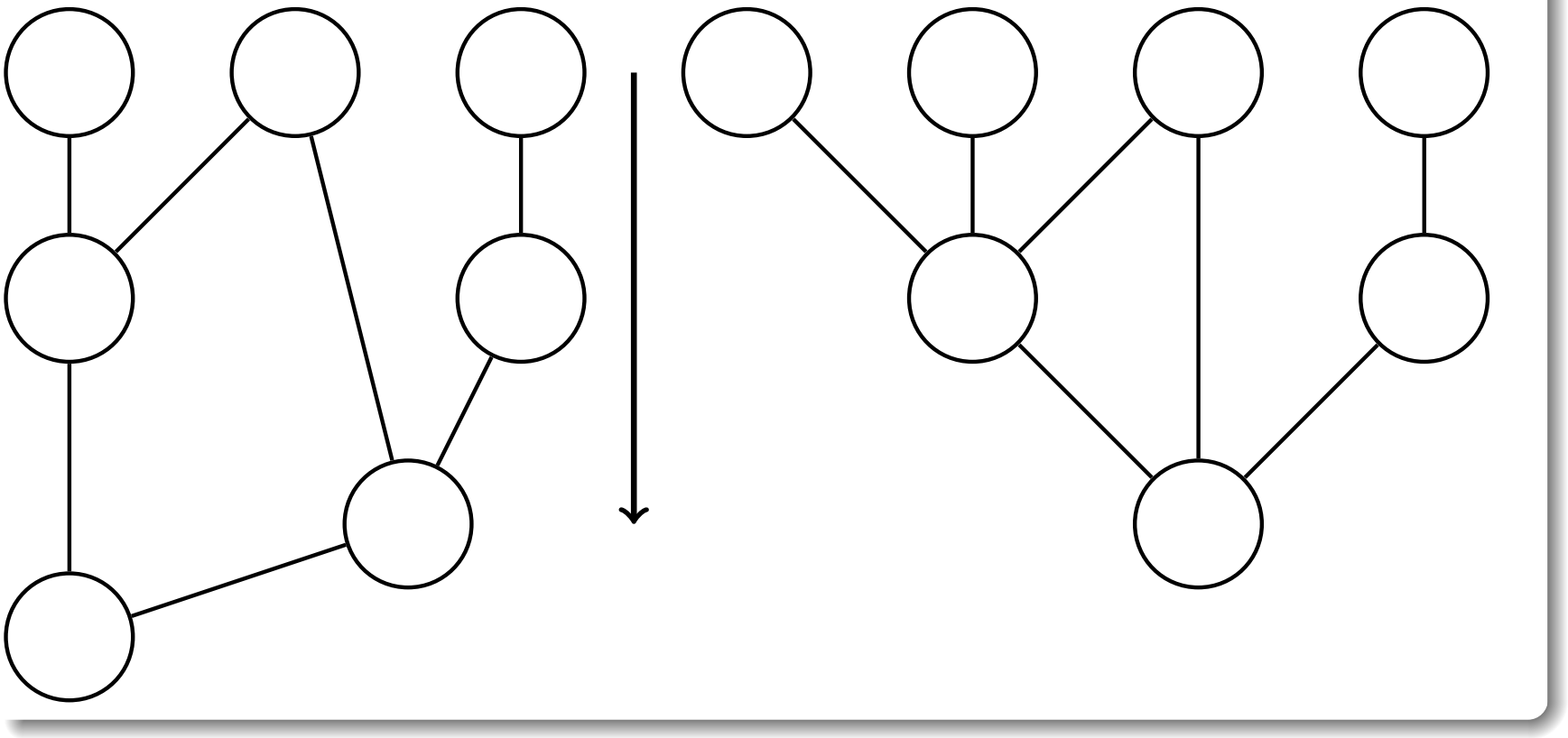
Tableau de correspondance

	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

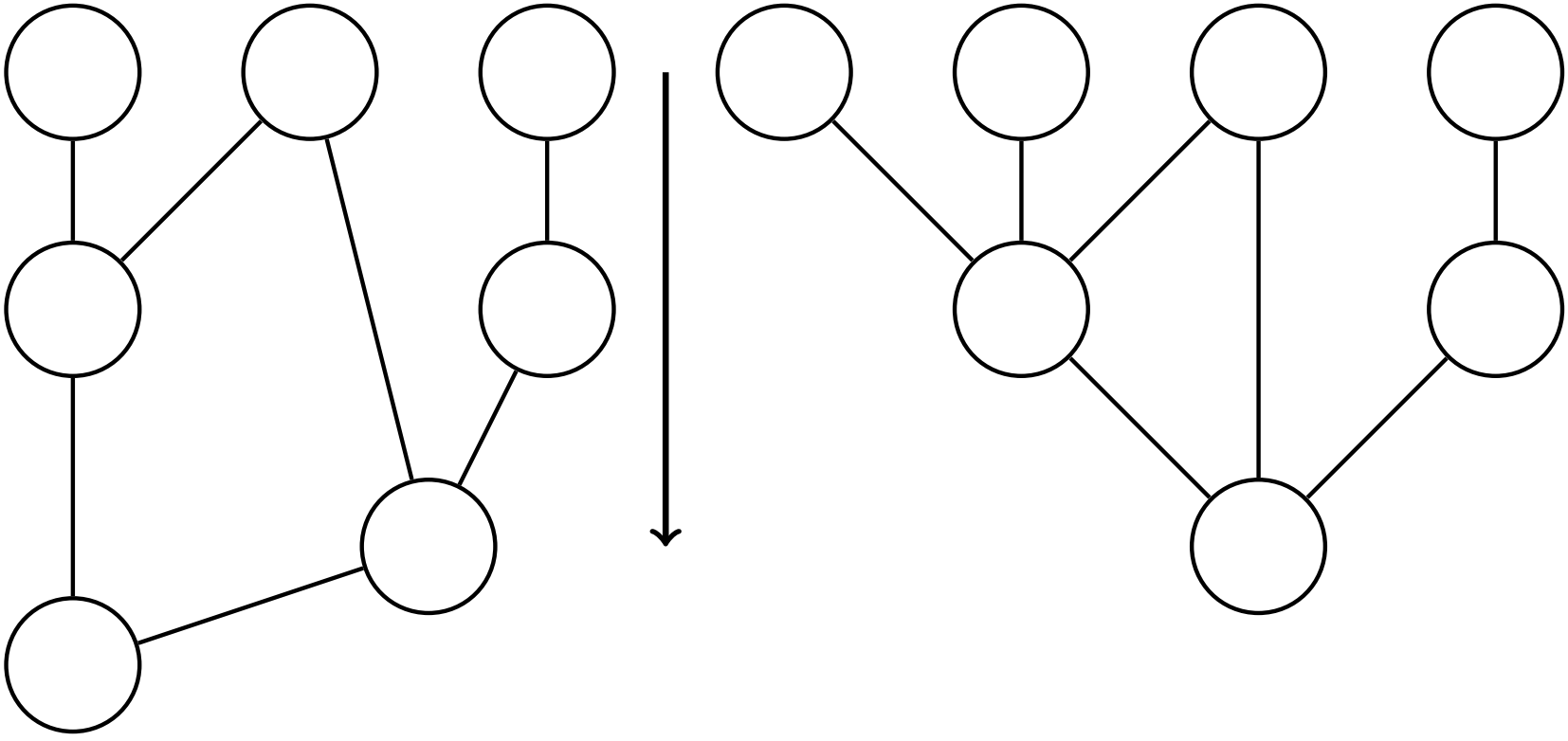


1. **Circuits booléens**
2. Réseaux booléens
3. Exemples et composition
4. Circuits de preuve
5. Simulation
6. Résultats

Exemples (Circuits booléens)



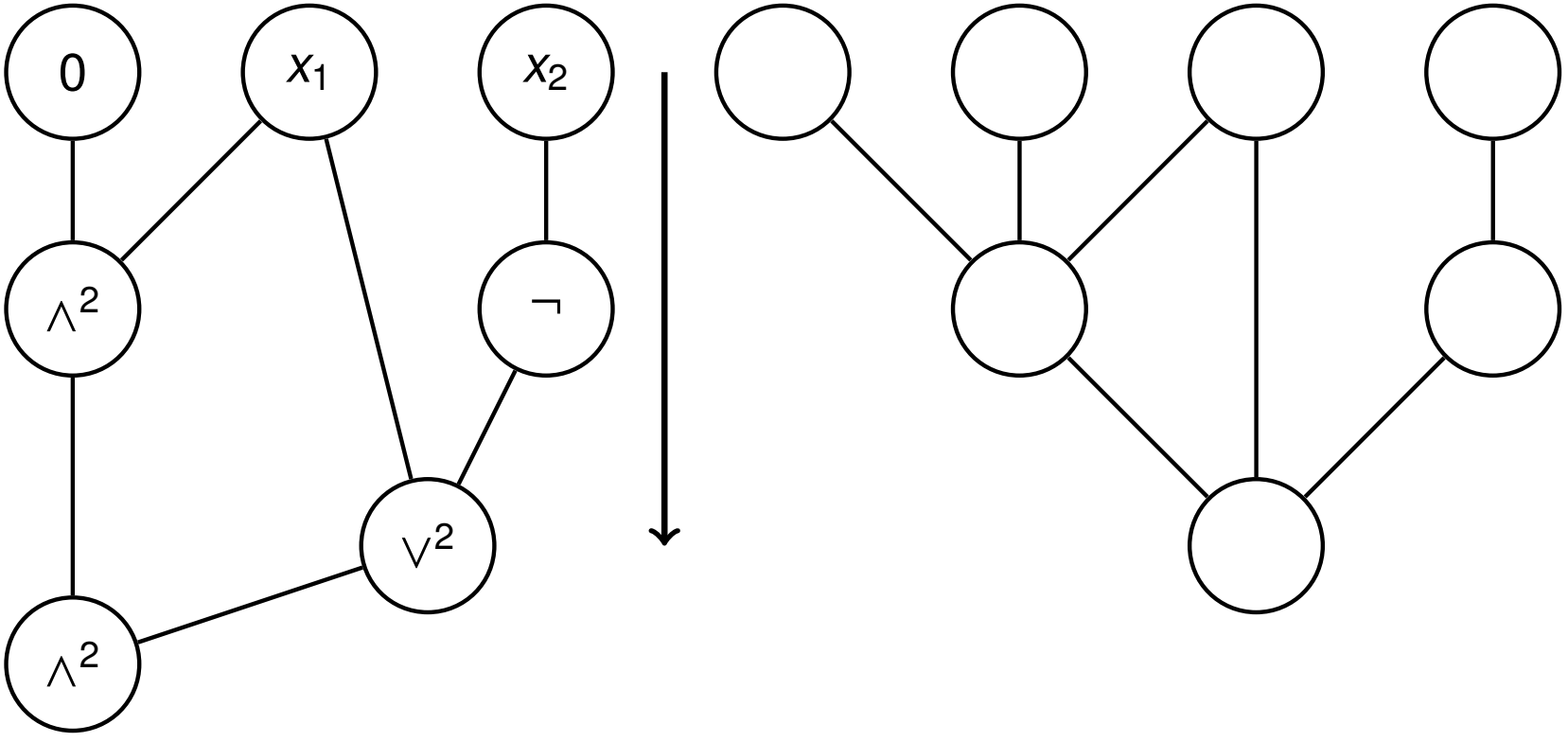
Exemples (Circuits booléens)



Définition (Bases)

$\mathfrak{B}_0 = \{\neg, \wedge^2, \vee^2\}$
$\mathfrak{B}_1 = \{\neg, (\wedge^n)_{n\geqslant 2}, (\vee^n)_{n\geqslant 2}\}$.

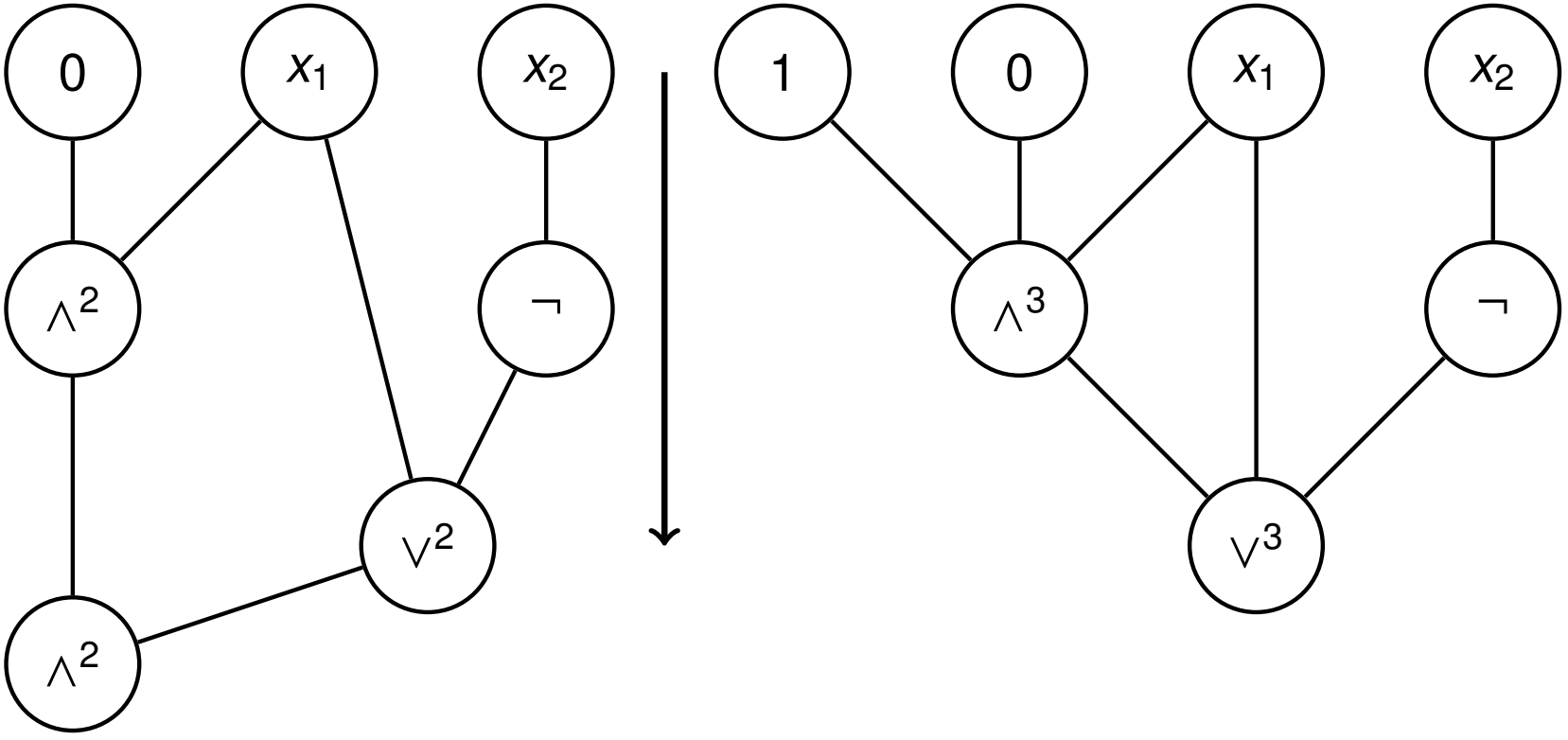
Exemples (Circuits booléens)



Définition (Bases)

$\mathfrak{B}_0 = \{\neg, \wedge^2, \vee^2\}$
$\mathfrak{B}_1 = \{\neg, (\wedge^n)_{n\geqslant 2}, (\vee^n)_{n\geqslant 2}\}$.

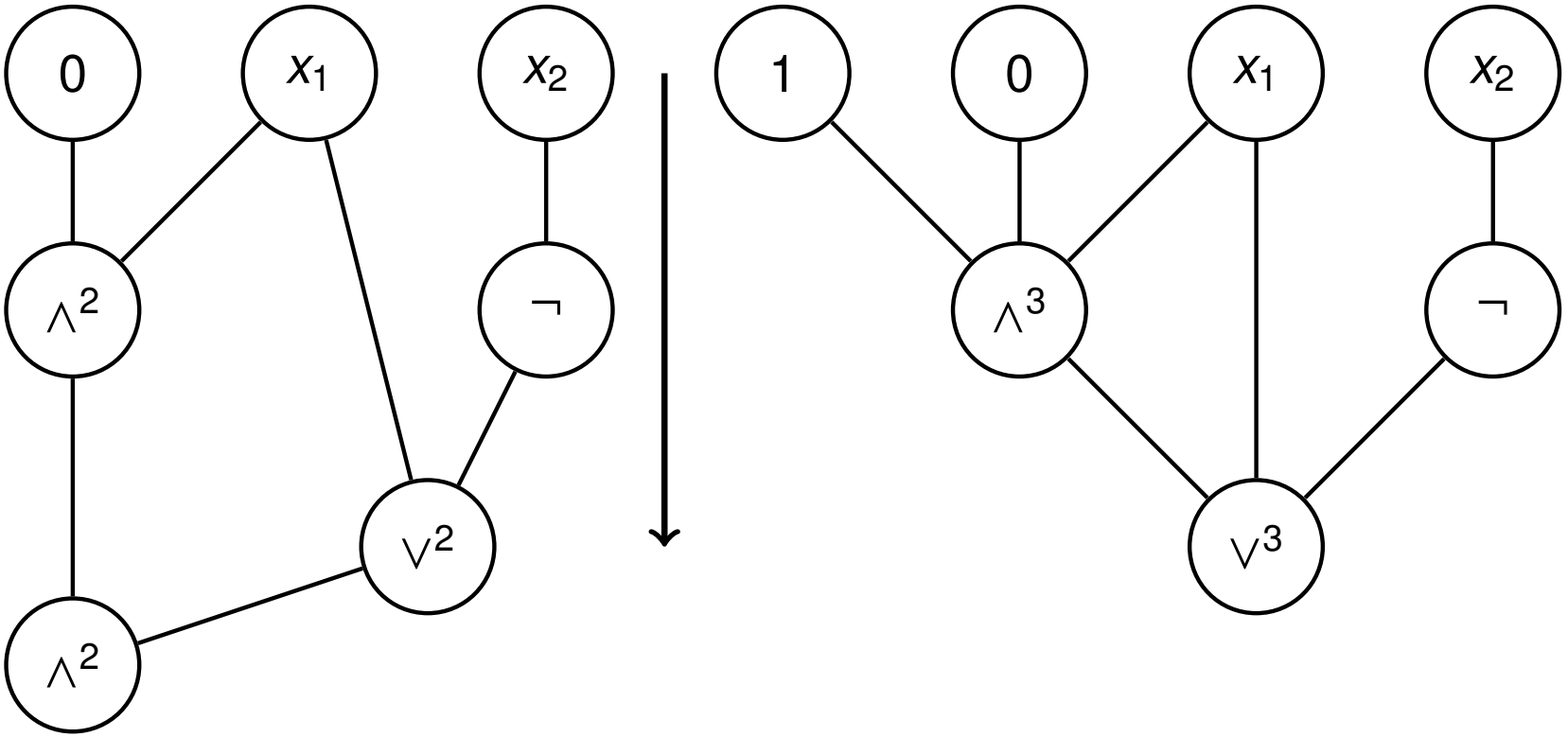
Exemples (Circuits booléens)



Définition (Bases)

$\mathfrak{B}_0 = \{\neg, \wedge^2, \vee^2\}$
$\mathfrak{B}_1 = \{\neg, (\wedge^n)_{n\geqslant 2}, (\vee^n)_{n\geqslant 2}\}$.

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. $\mathfrak{B}_1$).

$NC = \bigcup_{i \in \mathbb{N}} NC^i$ 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. $\mathfrak{B}_1$).

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

Définition ($UstCONN_2$)

Étant donnés 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.

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. $\mathfrak{B}_1$).

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

Définition ($UstCONN_2$)

Étant donnés 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. $\mathfrak{B}_1$).

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

Théorème

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

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

$$AC^0(UstCONN_2) \subseteq AC^1$$

Théorème ([Terui, 2004])

Pour tout circuit booléen C de taille $|C|$ et de profondeur $p(C)$ sur la base $\mathfrak{B}_1(UstCONN_2)$, il existe un réseau de preuve booléen de taille $\mathscr{O}(|C|^4)$ et de profondeur $\mathscr{O}(p(C))$ qui accepte le même ensemble.

Théorème ([Terui, 2004])

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

Problèmes :

1. $\mathit{UstCONN}_2 \in L$

Théorème ([Terui, 2004])

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

Problèmes :

1. $\mathit{UstCONN}_2 \in L$
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 $\mathscr{O}(|C|)$ (resp. $\mathscr{O}(|C^2|)$) et de profondeur $\mathscr{O}(p(C))$ qui accepte le même ensemble.

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 $\mathscr{O}(|C|)$ (resp. $\mathscr{O}(|C^2|)$) et de profondeur $\mathscr{O}(p(C))$ qui accepte le même ensemble.

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.

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. **Réseaux booléens**
3. Exemples et composition
4. Circuits de preuve
5. Simulation
6. Résultats

Définition (Les règles de **MLLu**)

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

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

Définition (Les règles de **MLLu**)

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

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

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

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

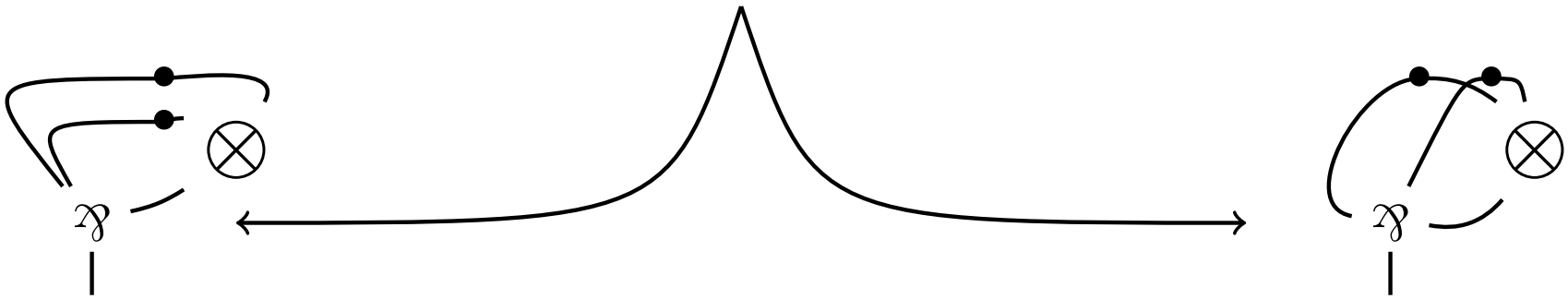
$$\dfrac{\dfrac{\dfrac{}{\vdash \alpha^{\perp}, \alpha}\ ax. \quad \dfrac{}{\vdash \alpha^{\perp}, \alpha}\ ax.}{\vdash \alpha^{\perp}, \alpha^{\perp}, \alpha \otimes \alpha}\ \otimes^2}{\vdash \parr^3(\alpha^{\perp}, \alpha^{\perp}, \alpha \otimes \alpha)}\ \parr^3$$

Définition (Les règles de **MLLu**)

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

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

$$\dfrac{\dfrac{\dfrac{}{\vdash \alpha^{\perp}, \alpha}\ ax. \quad \dfrac{}{\vdash \alpha^{\perp}, \alpha}\ ax.}{\vdash \alpha^{\perp}, \alpha^{\perp}, \alpha \otimes \alpha}\ \otimes^2}{\vdash \parr^3(\alpha^{\perp}, \alpha^{\perp}, \alpha \otimes \alpha)}\ \parr^3$$

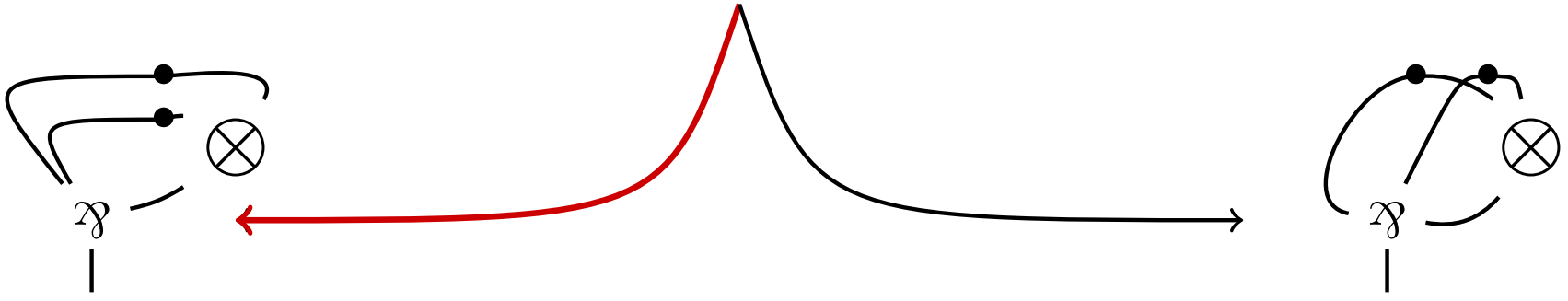


Définition (Les règles de **MLLu**)

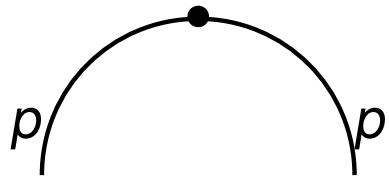
$$\frac{}{\vdash A, A^{\perp}}\ ax. \qquad \frac{\vdash \Gamma_1, A_1 \quad \dots \quad \vdash \Gamma_n, A_n}{\vdash \Gamma_1, \dots, \Gamma_n, \otimes^n(A_1, \dots, A_n)}\ \otimes^n$$

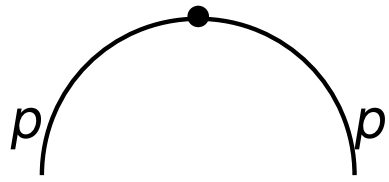
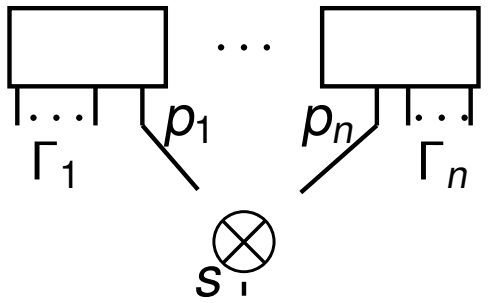
$$\frac{\vdash \Gamma, A \qquad \vdash \Delta, A^{\perp}}{\vdash \Gamma, \Delta}\ cut \qquad \frac{\vdash \Gamma, A_n, \dots, A_1}{\vdash \Gamma, \parr^n(A_n, \dots, A_1)}\ \parr^n$$

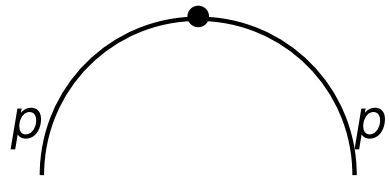
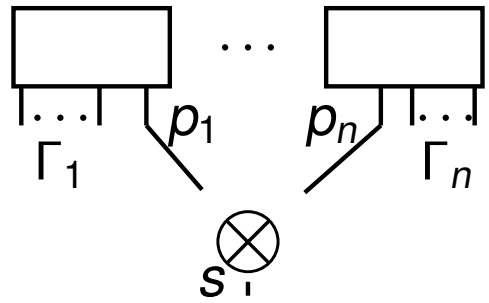
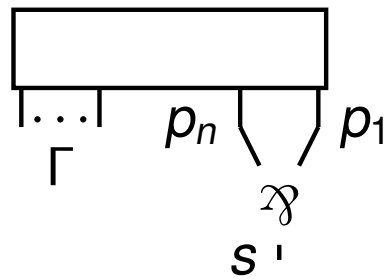
$$\dfrac{\dfrac{\dfrac{}{\vdash p : \alpha^{\perp}, p : \alpha \rhd ax_p}\ ax. \quad \dfrac{}{\vdash q : \alpha^{\perp}, q : \alpha \rhd ax_q}\ ax.}{\vdash p : \alpha^{\perp}, q : \alpha^{\perp}, r : \alpha \otimes \alpha \rhd tenseur_r^{p,q}(ax_p, ax_q)}\ \otimes^2}{\vdash s : \parr^3(\alpha^{\perp},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

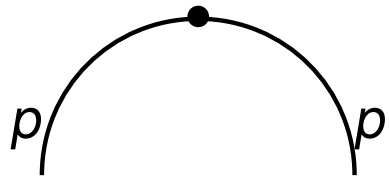
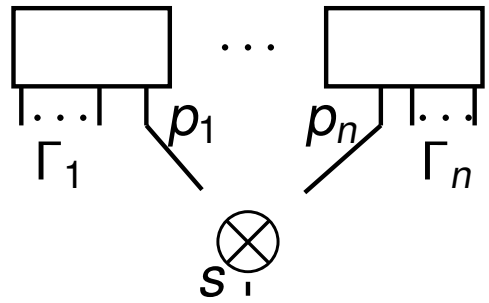
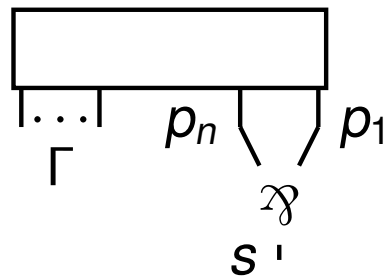
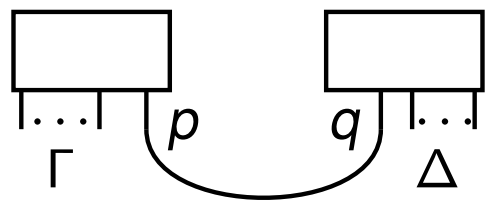


Règles	
$\dfrac{}{\vdash A,\ A^{\perp}}\ ax.$	
$\dfrac{\vdash \Gamma_1, A_1 \quad \ldots \quad \vdash \Gamma_n, : A_n}{\vdash \Gamma_1, \ldots, \Gamma_n, \otimes^n (A_1, \ldots, A_n)}\ \otimes^n$	
$\dfrac{\vdash \Gamma, A_n, \ldots, A_1}{\vdash \Gamma, \parr^n (A_n, \ldots, A_1)}\ \parr^n$	
$\dfrac{\vdash \Gamma, A \qquad \vdash \Delta, A^{\perp}}{\vdash \Gamma, \Delta}\ cut$	

Typage	Réseau
$\dfrac{}{\vdash p : A, p : A^{\perp} \triangleright ax_p}\ ax.$	
$\dfrac{\vdash \Gamma_1, \quad A_1 \qquad \ldots \qquad \vdash \Gamma_n, \quad : A_n}{\vdash \Gamma_1, \ldots, \Gamma_n, \quad \otimes^n (A_1, \ldots, A_n)}\ \otimes^n$	
$\dfrac{\vdash \Gamma, \quad A_n, \ldots, \quad A_1}{\vdash \Gamma, \quad \parr^n (A_n, \ldots, A_1)}\ \parr^n$	
$\dfrac{\vdash \Gamma, \quad A \qquad \vdash \Delta, \quad A^{\perp}}{\vdash \Gamma, \Delta}\ cut$	

Typage	Réseau
$\dfrac{}{\vdash p : A, p : A^{\perp} \triangleright ax_p}\ ax.$	
$\dfrac{\vdash \Gamma_1, p_1 : A_1 \triangleright P_1 \quad \ldots \quad \vdash \Gamma_n, p_n : A_n \triangleright P_n}{\vdash \Gamma_1, \ldots, \Gamma_n, s : \otimes^n (A_1, \ldots, A_n) \triangleright tenseur_s^{\vec{p}} (\vec{P})}\ \otimes^n$	
$\dfrac{\vdash \Gamma, A_n, \ldots, A_1}{\vdash \Gamma, \parr^n (A_n, \ldots, A_1)}\ \parr^n$	
$\dfrac{\vdash \Gamma, A \qquad \vdash \Delta, A^{\perp}}{\vdash \Gamma, \Delta}\ cut$	

Typage	Réseau
$\dfrac{}{\vdash p : A, p : A^{\perp} \triangleright ax_p}\ ax.$	
$\dfrac{\vdash \Gamma_1, p_1 : A_1 \triangleright P_1 \quad \ldots \quad \vdash \Gamma_n, p_n : A_n \triangleright P_n}{\vdash \Gamma_1, \ldots, \Gamma_n, s : \otimes^n (A_1, \ldots, A_n) \triangleright tenseur_s^{\vec{p}} (\vec{P})}\ \otimes^n$	
$\dfrac{\vdash \Gamma, p_n : A_n, \ldots, p_1 : A_1 \triangleright P}{\vdash \Gamma, s : \parr^n (A_n, \ldots, A_1) \triangleright par_s^{p_n,\ldots,p_1} (P)}\ \parr^n$	
$\dfrac{\vdash \Gamma, \quad A \qquad \vdash \Delta, \quad A^{\perp}}{\vdash \Gamma, \Delta}\ cut$	

Typage	Réseau
$\dfrac{}{\vdash p : A, p : A^{\perp} \triangleright ax_p}\ ax.$	
$\dfrac{\vdash \Gamma_1, p_1 : A_1 \triangleright P_1 \quad \ldots \quad \vdash \Gamma_n, p_n : A_n \triangleright P_n}{\vdash \Gamma_1, \ldots, \Gamma_n, s : \otimes^n (A_1, \ldots, A_n) \triangleright tenseur_s^{\vec{p}}(\vec{P})}\ \otimes^n$	
$\dfrac{\vdash \Gamma, p_n : A_n, \ldots, p_1 : A_1 \triangleright P}{\vdash \Gamma, s : \parr^n (A_n, \ldots, A_1) \triangleright par_s^{p_n,\ldots,p_1}(P)}\ \parr^n$	
$\dfrac{\vdash \Gamma, p : A \triangleright P \quad \vdash \Delta, q : A^{\perp} \triangleright Q}{\vdash \Gamma, \Delta \triangleright cut^{p,q}(P, Q)}\ cut$	

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

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

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

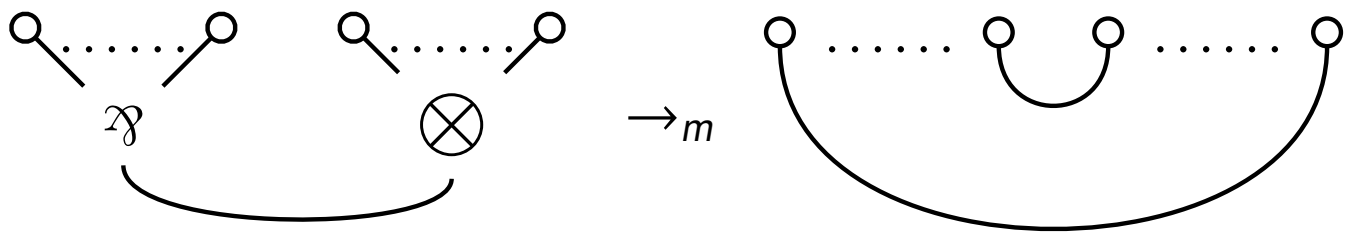
Définition (Réseau de preuve booléen, [Terui, 2004])

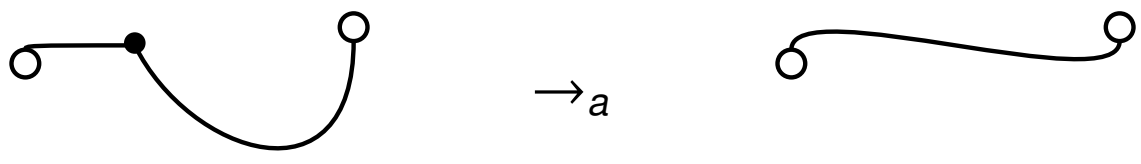
Un réseau de preuve booléen à n entrées est un réseau de preuve $P(\overrightarrow{p})$ de type

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

Définition ($\rightarrow_m$ et $\rightarrow_a$)

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



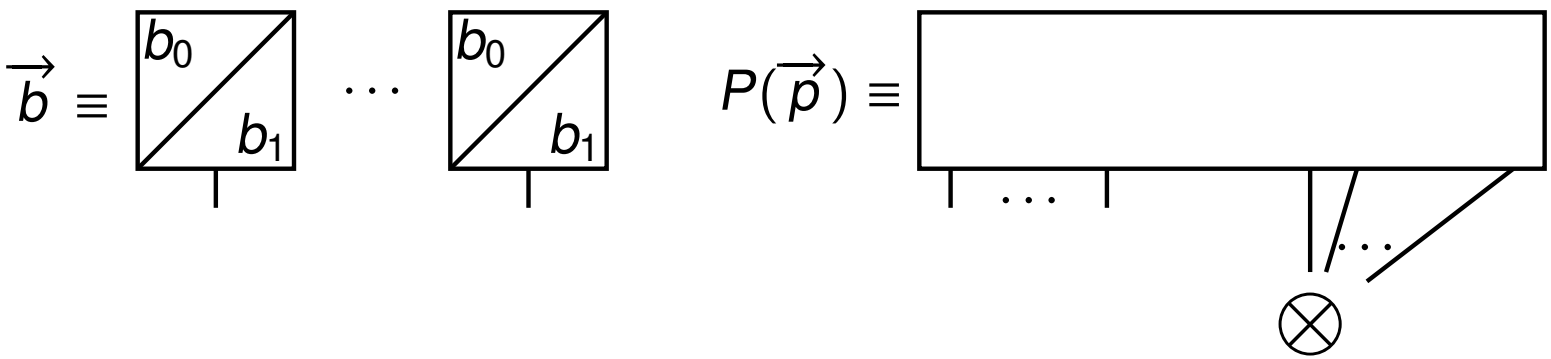


Définition (Réseau de preuve booléen, [Terui, 2004])

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

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

Définition

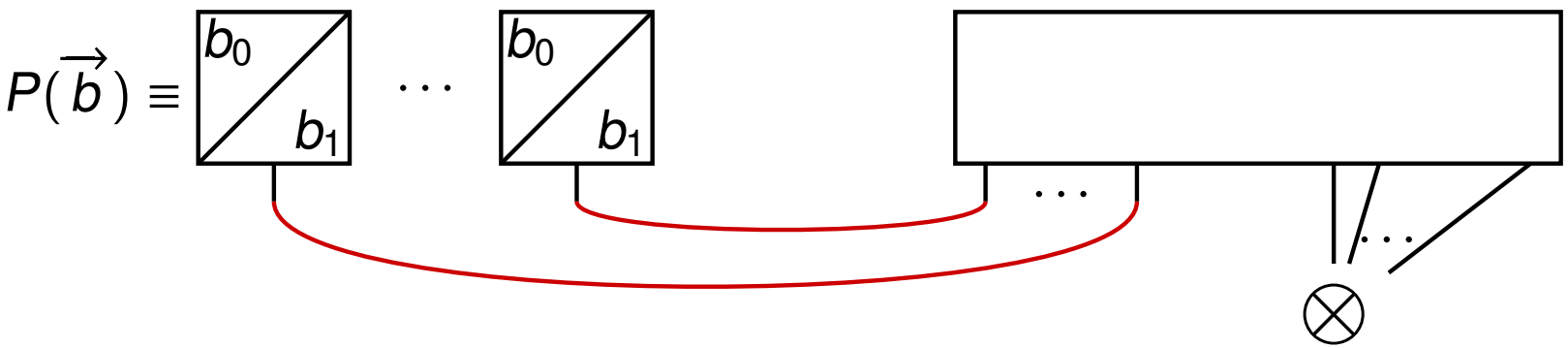


Définition (Réseau de preuve booléen, [Terui, 2004])

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

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

Définition

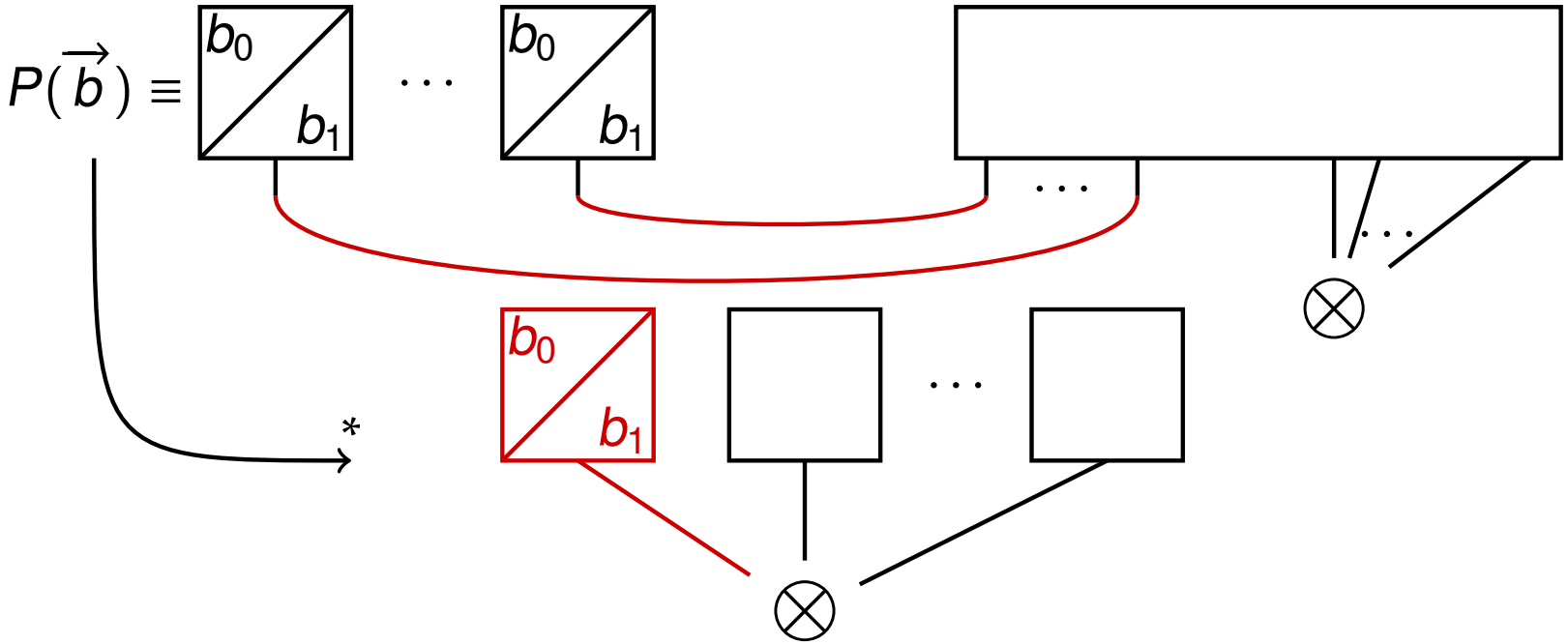


Définition (Réseau de preuve booléen, [Terui, 2004])

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

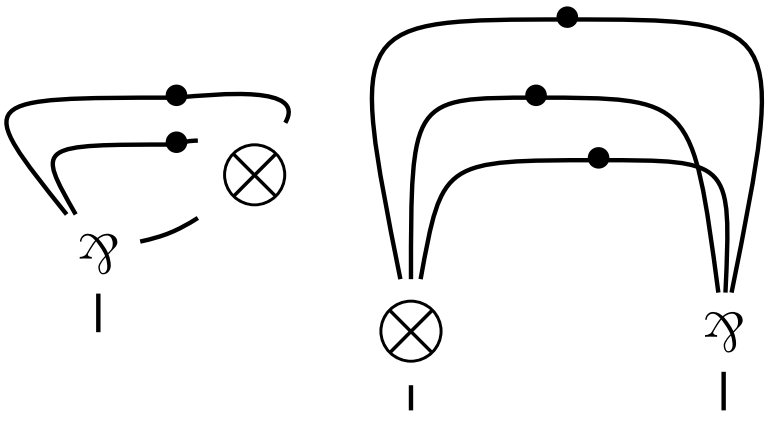
$$\vdash p_1 : \mathbf{B}^{\perp}[A_1], \ldots, p_n : \mathbf{B}^{\perp}[A_n], s : \otimes^{1+m}(\mathbf{B}[A], C_1, \ldots, C_m)$$

Définition

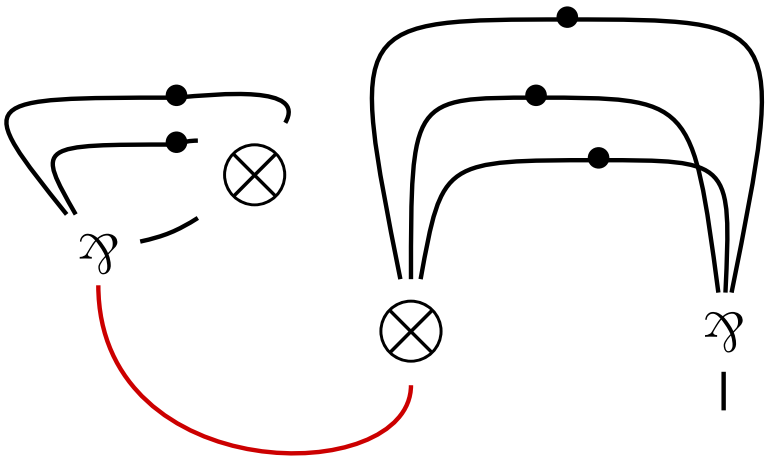


1. Circuits booléens
2. Réseaux booléens
3. **Exemples et composition**
4. Circuits de preuve
5. Simulation
6. Résultats

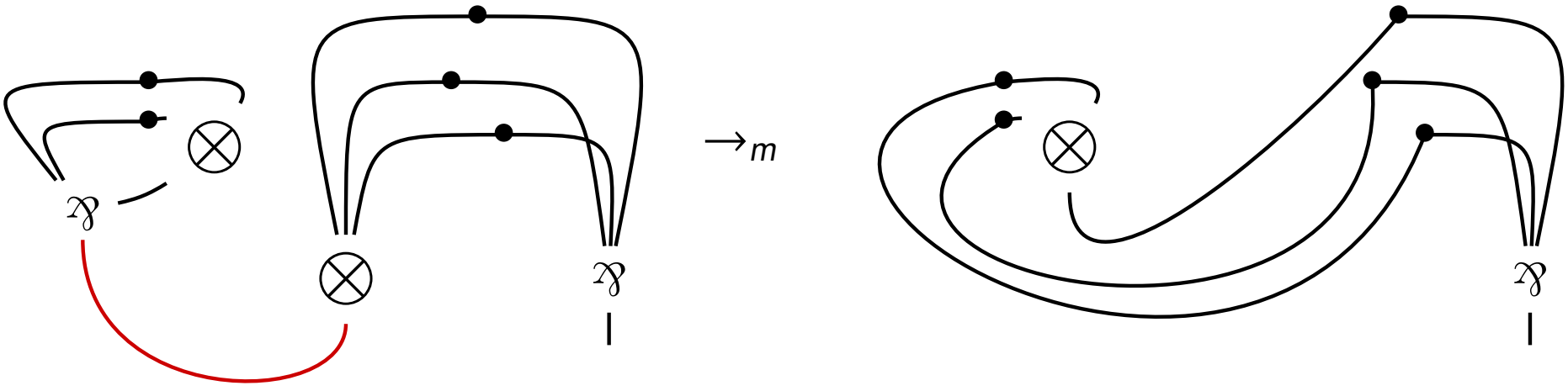
Un premier exemple : la négation



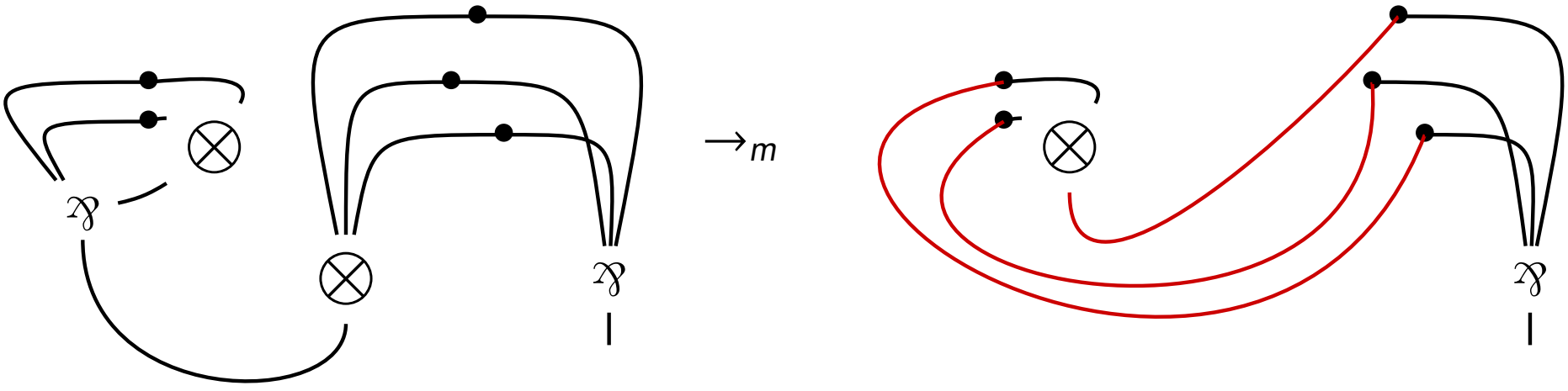
Un premier exemple : la négation



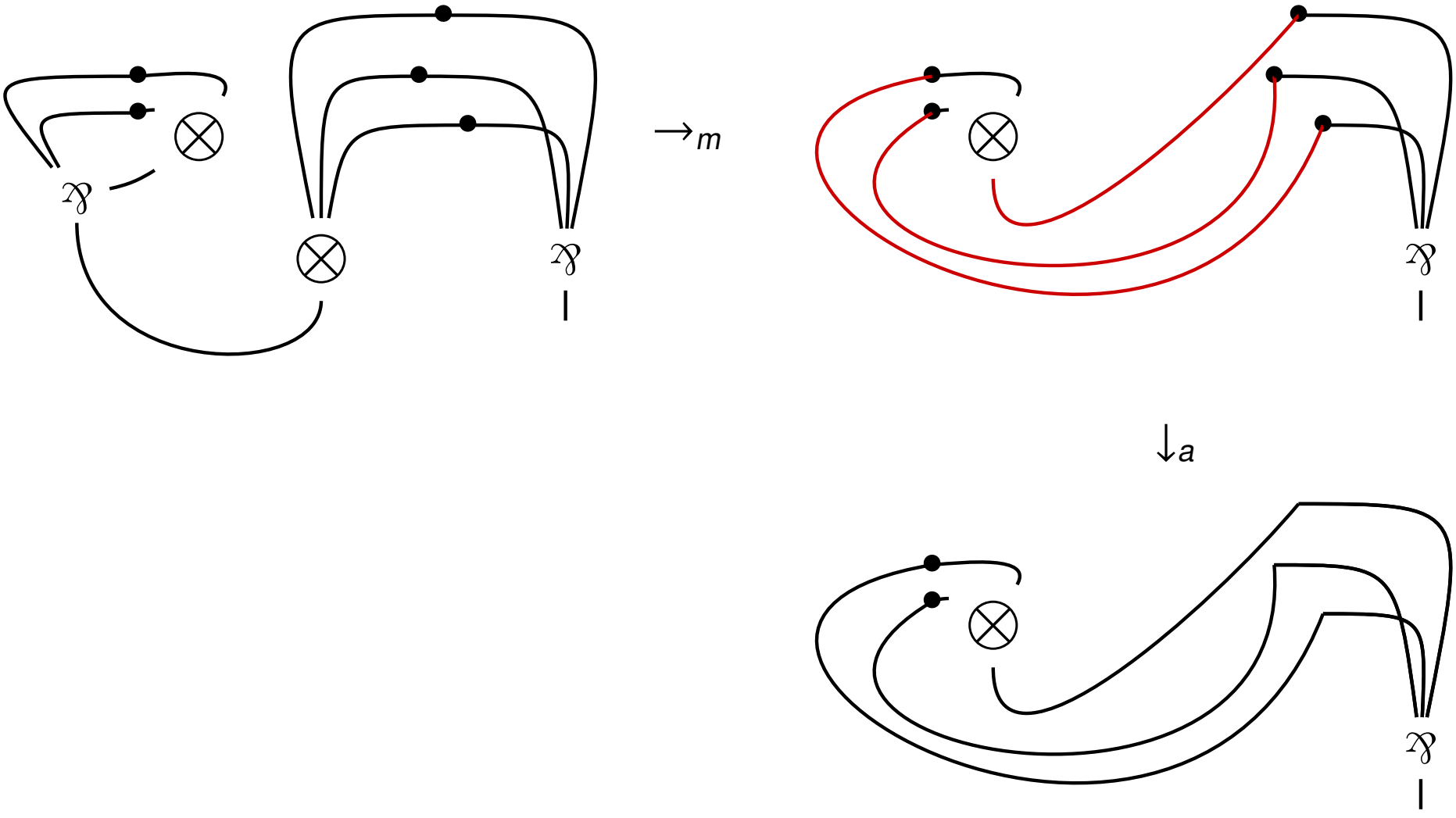
Un premier exemple : la négation



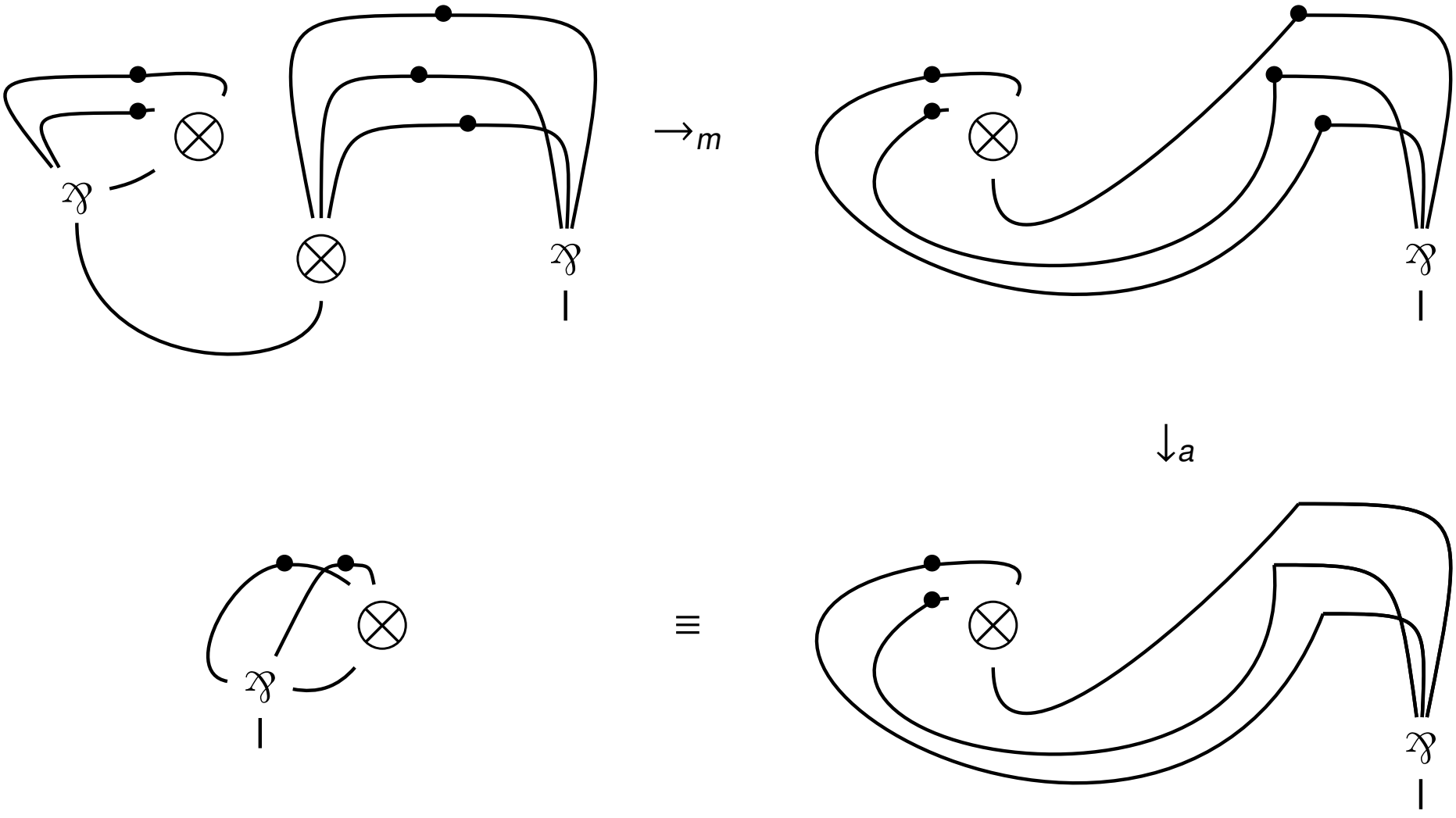
Un premier exemple : la négation



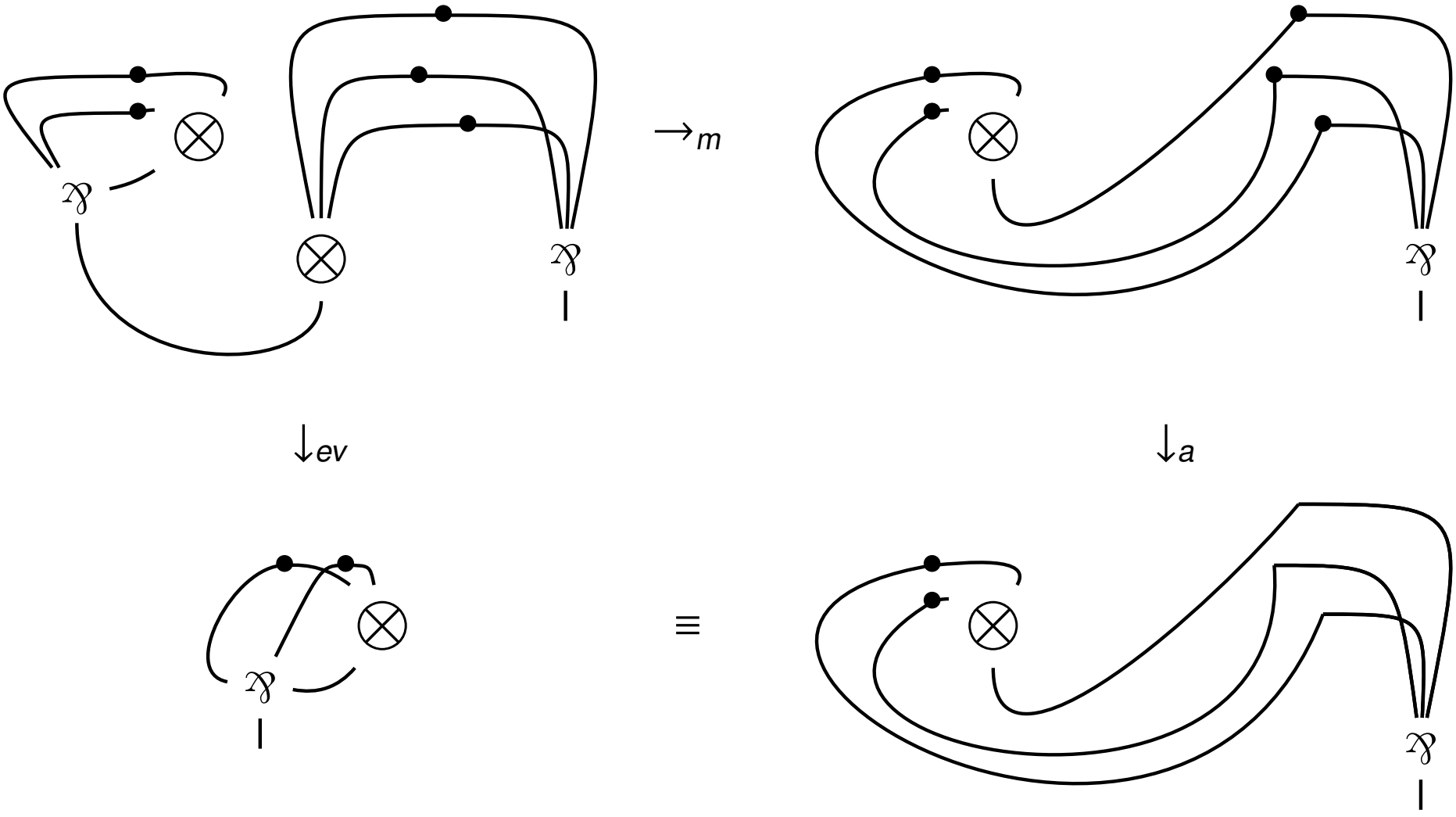
Un premier exemple : la négation



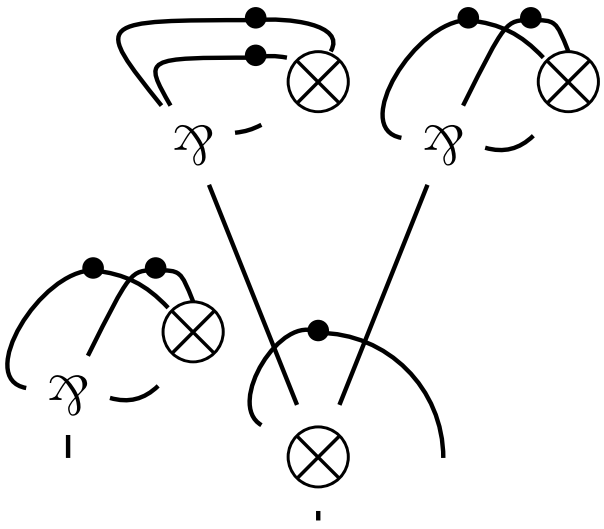
Un premier exemple : la négation



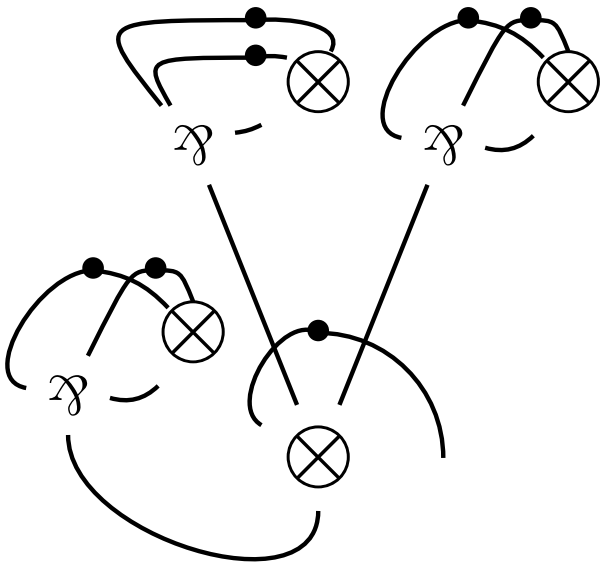
Un premier exemple : la négation



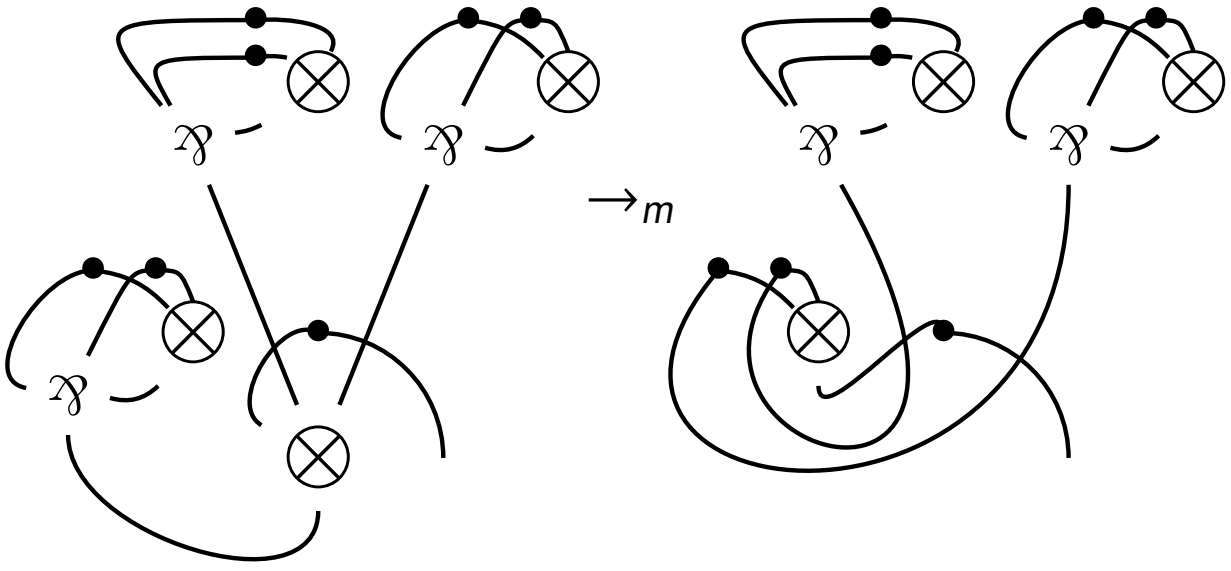
Second exemple : le conditionnel



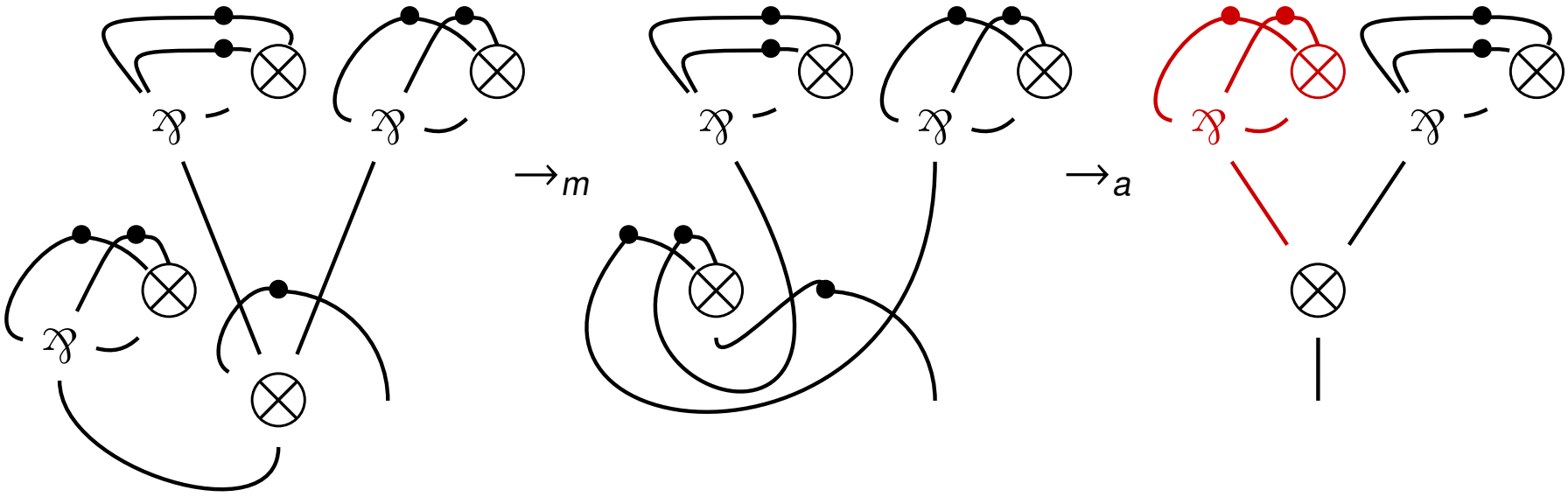
Second exemple : le conditionnel



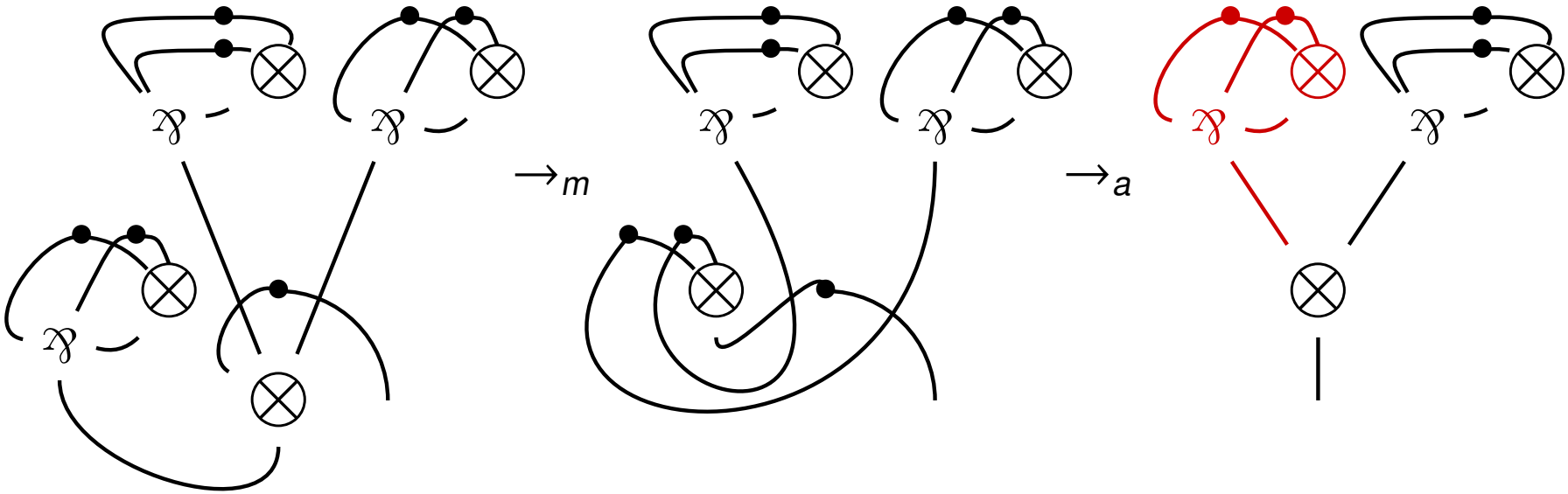
Second exemple : le conditionnel



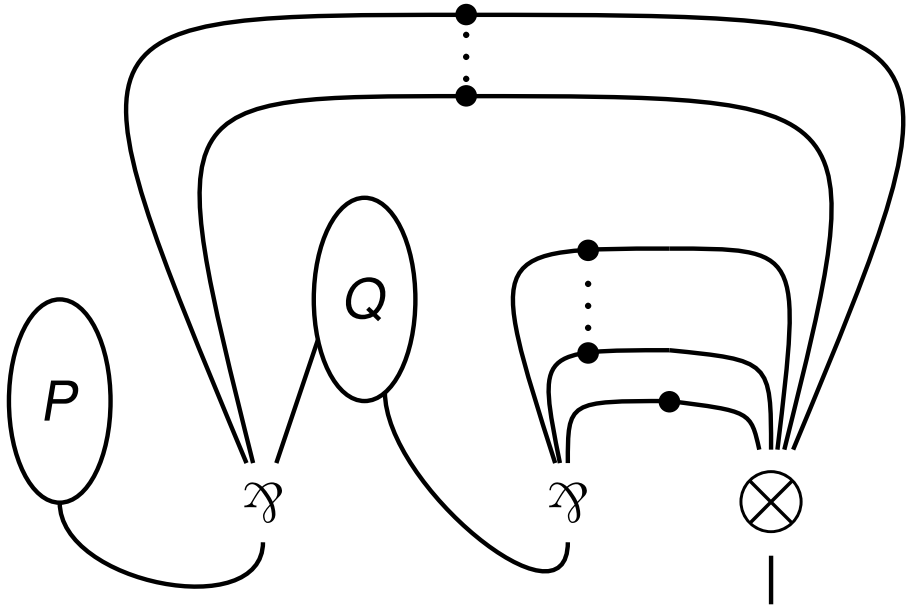
Second exemple : le conditionnel



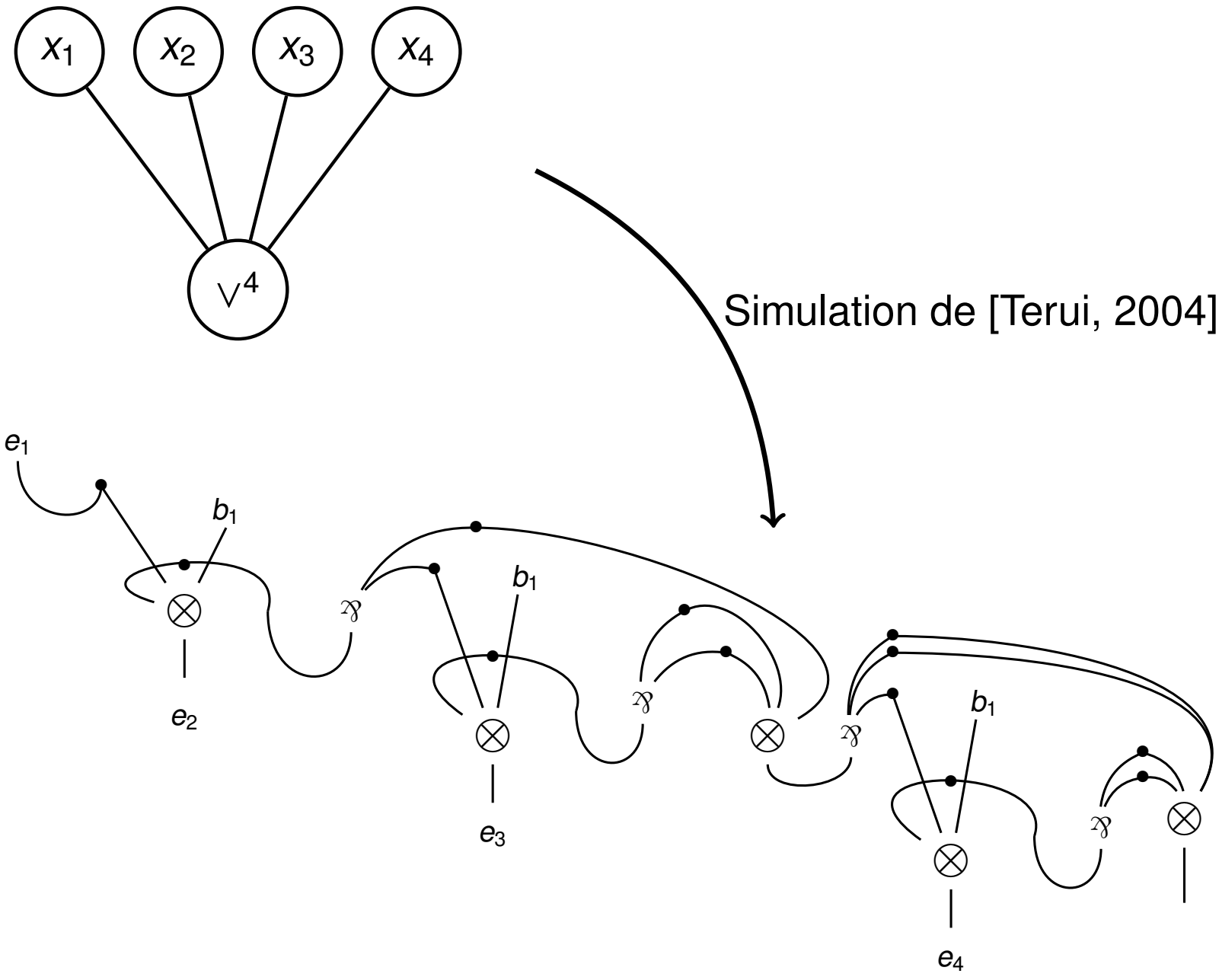
Second exemple : le conditionnel



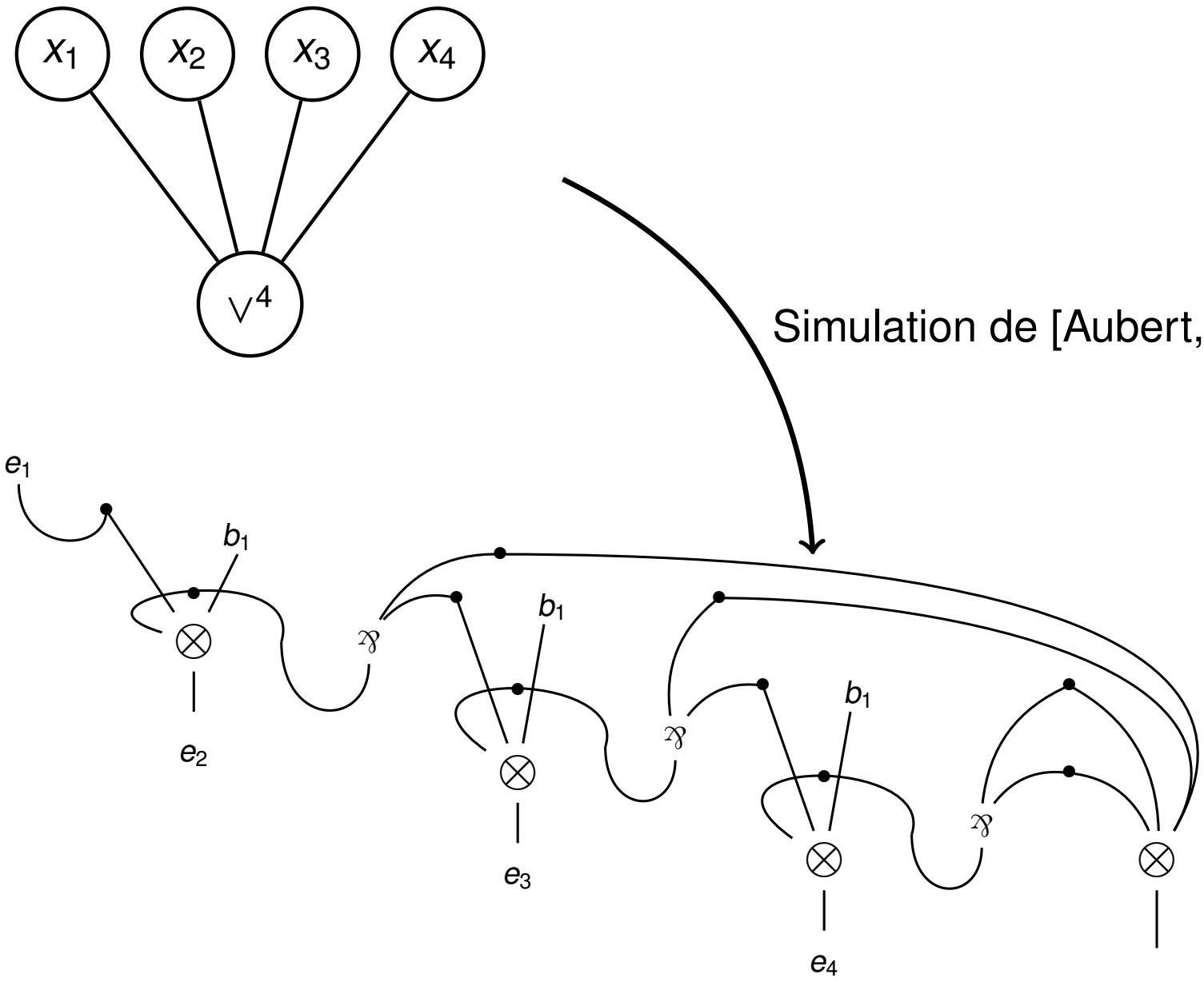
Nécessite de composer :



Un exemple de simulation

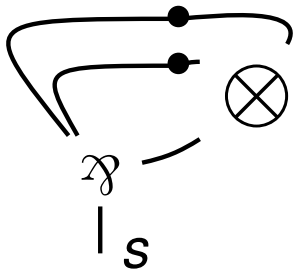


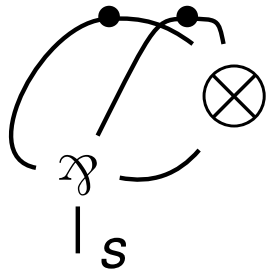
Un exemple de simulation

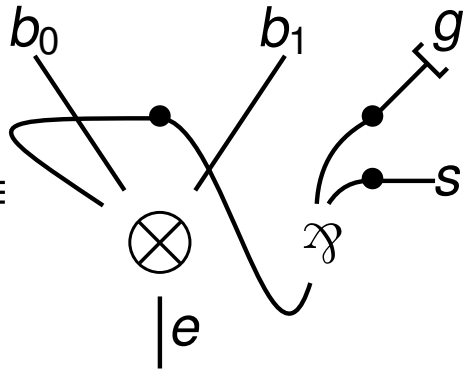


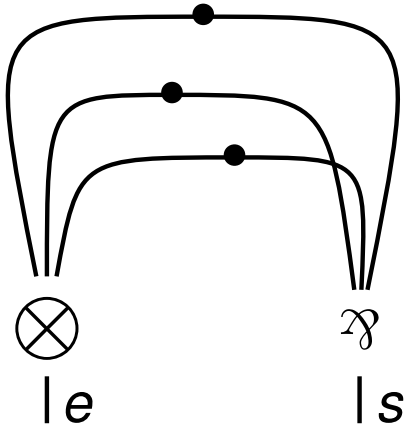
1. Circuits booléens
2. Réseaux booléens
3. Exemples et composition
4. **Circuits de preuve**
5. Simulation
6. Résultats

Pièces de circuits de preuves

$b_0 \equiv$ 

$b_1 \equiv$ 

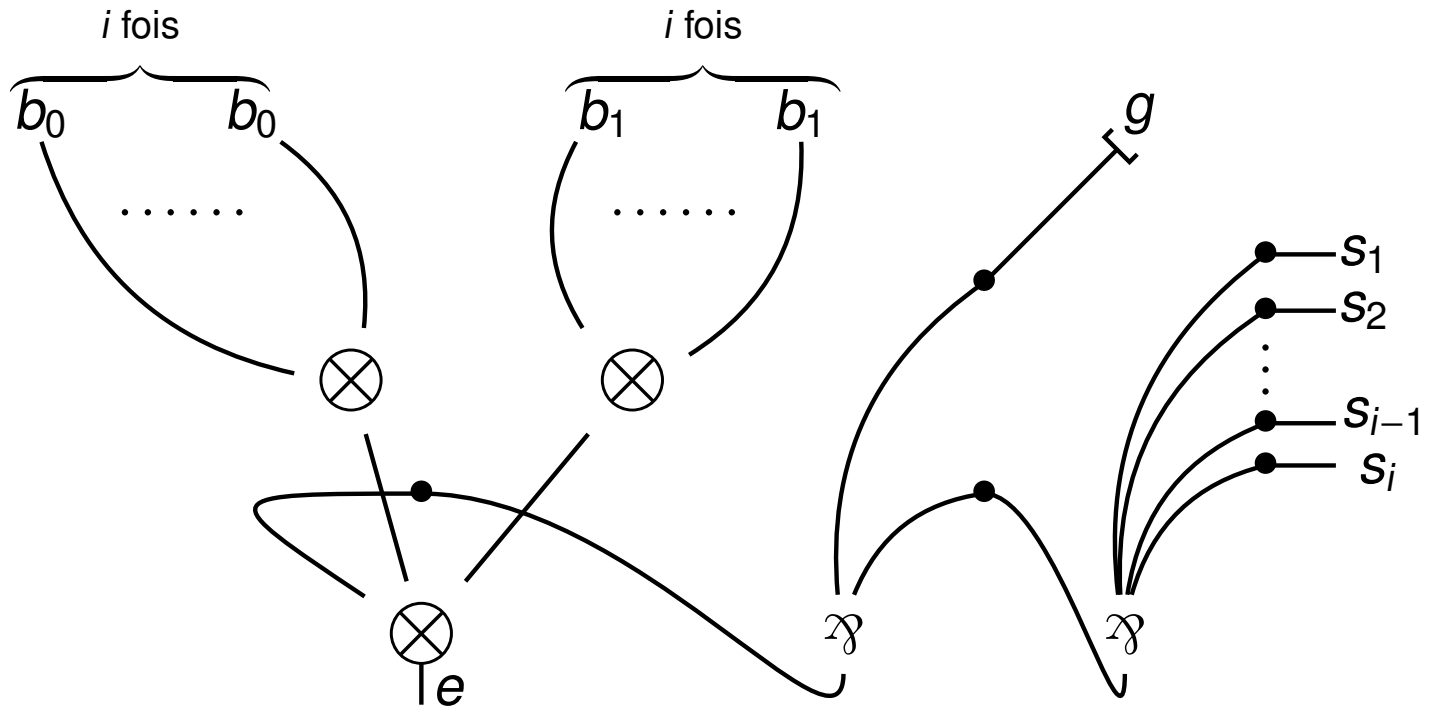
$DUPL^1 \equiv$ 

$NEG \equiv$ 

Pièces de circuits de preuves

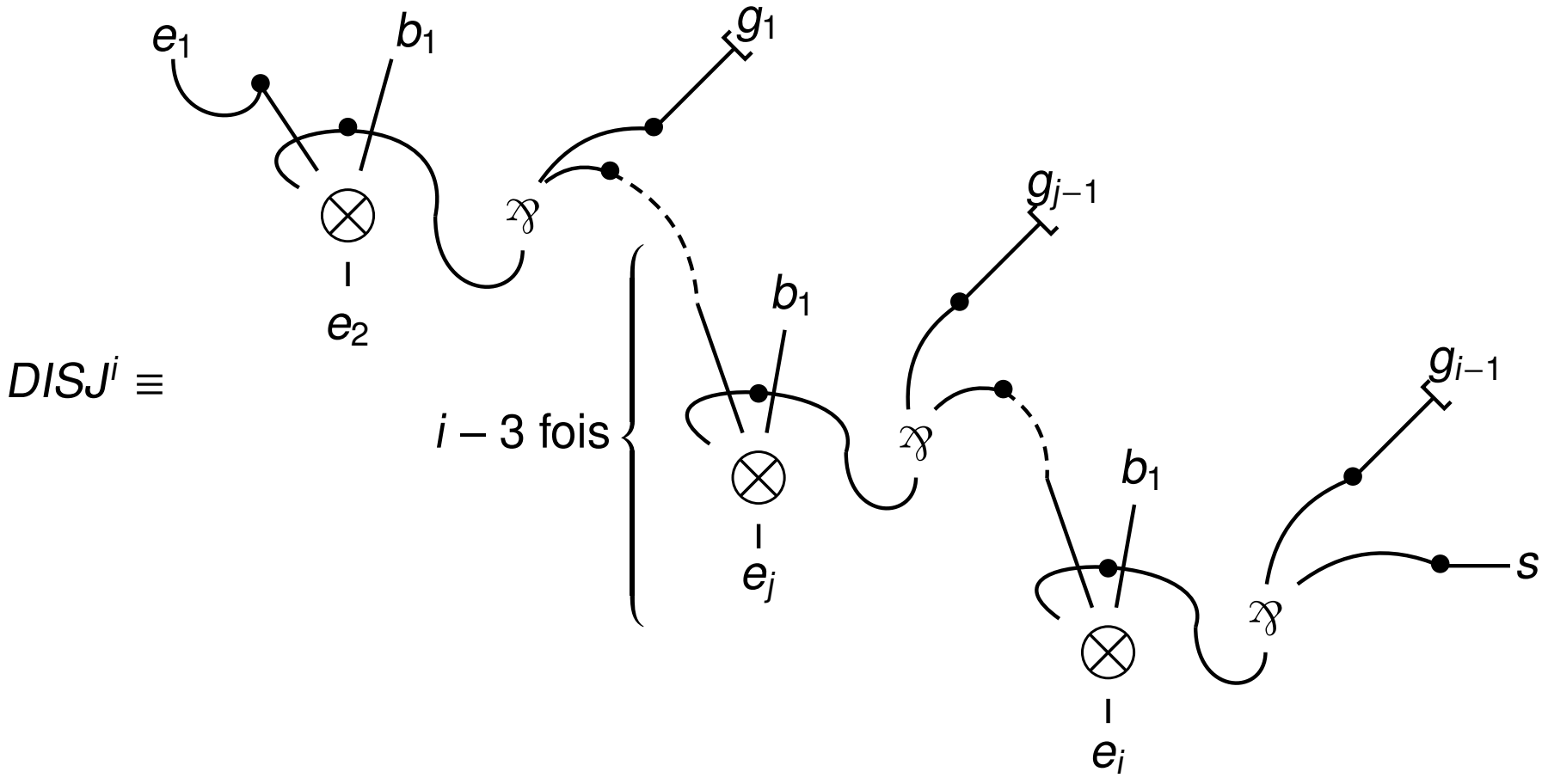
On pose $2 \leqslant j \leqslant i$.

$DUPL^i \equiv$



Pièces de circuits de preuves

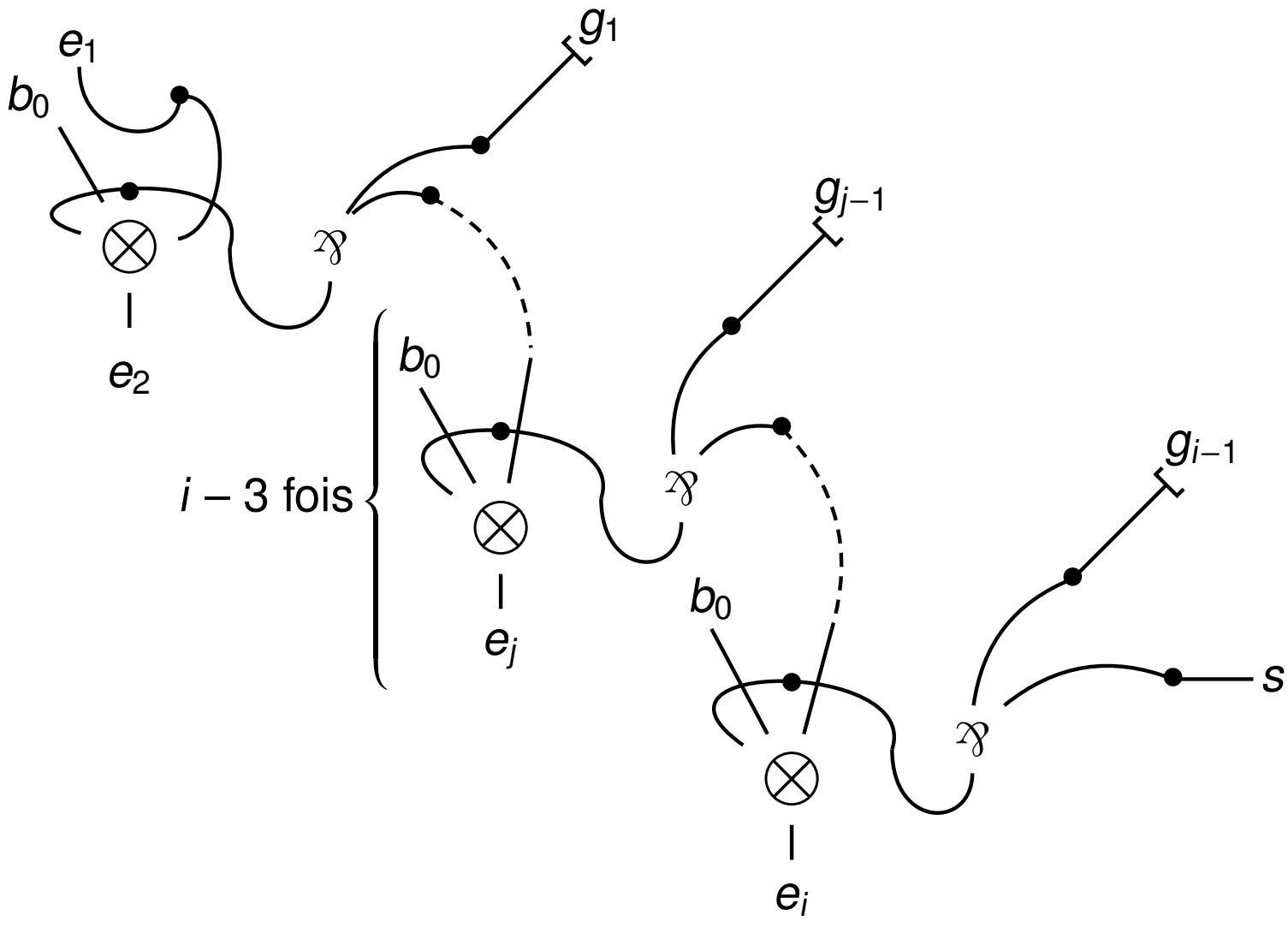
On pose $2 \leqslant j \leqslant i$.



Pièces de circuits de preuves

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

$CONJ^i \equiv$



Composition de pièces et de circuits de preuves

Définition (Circuit de preuve)

1. On compose des pièces (identifie une sortie d'une pièce avec une entrée d'une autre pièce), sans boucler,
2. on étiquette les entrées des pièces restées libres,
3. on ajoute un tenseur conclusion qui collecte la sortie de la dernière pièce et les poubelles générées.

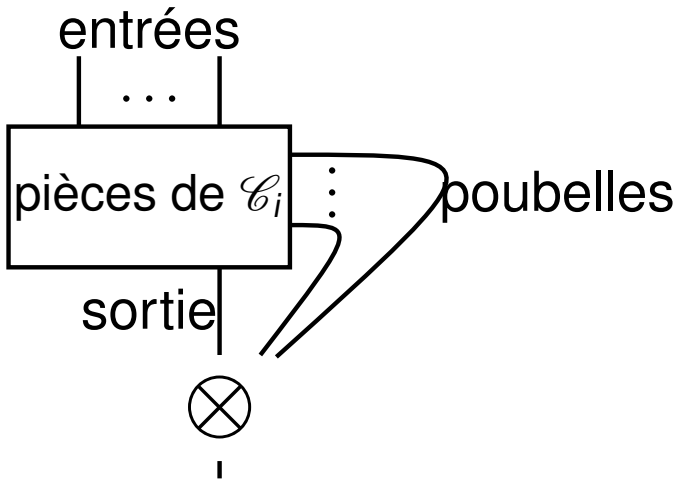
Composition de pièces et de circuits de preuves

Définition (Circuit de preuve)

1. On compose des pièces (identifie une sortie d'une pièce avec une entrée d'une autre pièce), sans boucler,
2. on étiquette les entrées des pièces restées libres,
3. on ajoute un tenseur conclusion qui collecte la sortie de la dernière pièce et les poubelles générées.

Définition (Composition de circuits de preuves)

Soient $\mathscr{C}_1$ et $\mathscr{C}_2$ deux circuits de preuves. On les représente ainsi :

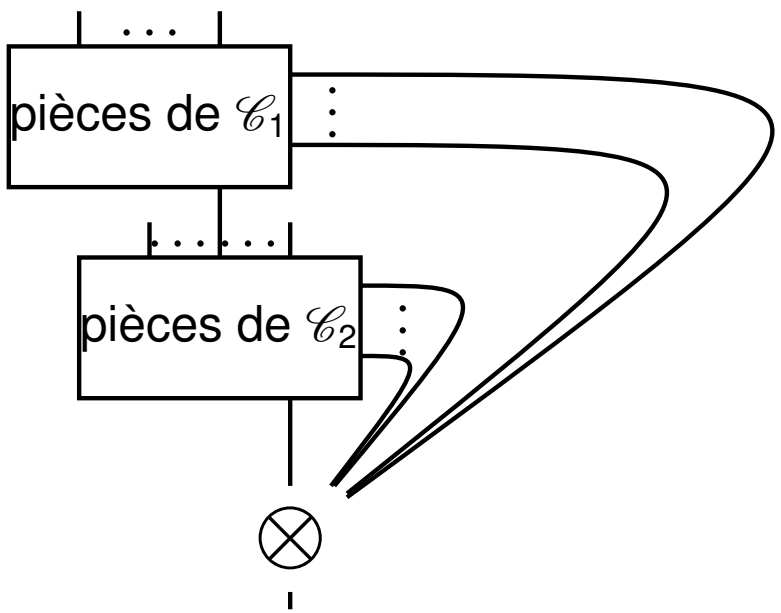


Composition de pièces et de circuits de preuves

Définition (Circuit de preuve)

1. On compose des pièces (identifie une sortie d'une pièce avec une entrée d'une autre pièce), sans boucler,
2. on étiquette les entrées des pièces restées libres,
3. on ajoute un tenseur conclusion qui collecte la sortie de la dernière pièce et les poubelles générées.

Définition (Composition de circuits de preuves)



Composition de pièces et de circuits de preuves

Définition (Circuit de preuve)

1. On compose des pièces (identifie une sortie d'une pièce avec une entrée d'une autre pièce), sans boucler,
2. on étiquette les entrées des pièces restées libres,
3. on ajoute un tenseur conclusion qui collecte la sortie de la dernière pièce et les poubelles générées.

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)

1. On compose des pièces (identifie une sortie d'une pièce avec une entrée d'une autre pièce), sans boucler,
2. on étiquette les entrées des pièces restées libres,
3. on ajoute un tenseur conclusion qui collecte la sortie de la dernière pièce et les poubelles générées.

Théorème ([Aubert, 2010])

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

Lemme (Traduction)

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

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

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

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

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

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

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

Lemme

Soit $\mathscr{P}$ une pièce d'un circuit de preuve à $n \geqslant 1$ entrées et $m \geqslant 1$ sorties. Soient $A_{s_1}, \ldots, A_{s_m}$ les formules à sa sortie et $A_{e_1}, \ldots, A_{e_n}$ les formules à son entrée. On a pour $j \in \{1, \ldots, n\}$

$$d(A_{e_j}) \leqslant d(\boldsymbol{B}) + max(d(A_{s_1}), \ldots, d(A_{s_m}))$$

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

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

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

Lemme

Soit $\mathscr{P}$ une pièce d'un circuit de preuve à $n \geqslant 1$ entrées et $m \geqslant 1$ sorties. Soient $A_{s_1}, \ldots, A_{s_m}$ les formules à sa sortie et $A_{e_1}, \ldots, A_{e_n}$ les formules à son entrée. On a pour $j \in \{1, \ldots, n\}$

$$d(A_{e_j}) \leqslant d(\boldsymbol{B}) + max(d(A_{s_1}), \ldots, d(A_{s_m}))$$

Démonstration

- Soit x_i l'entrée de $\mathscr{T}(C_n)$ 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 $d(\mathscr{T}(C_n)) \leqslant p(C_n) \times 2 \times d(\mathbf{B})$.

Principaux théorèmes

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

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

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

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

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

Principaux théorèmes

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

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

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

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

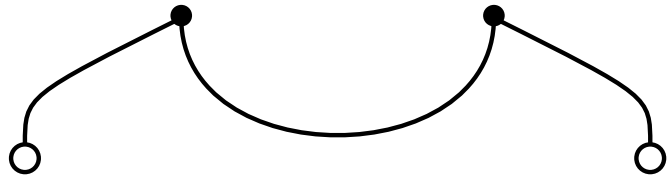
Si C_n appartient à une famille de circuits booléens comprise dans NC^i (resp. AC^i), $|\mathscr{T}(C_n)| = \mathscr{O}(|C_n|)$ (resp. $|\mathscr{T}(C_n)| = \mathscr{O}(|C_n|^2)$).

Démonstration

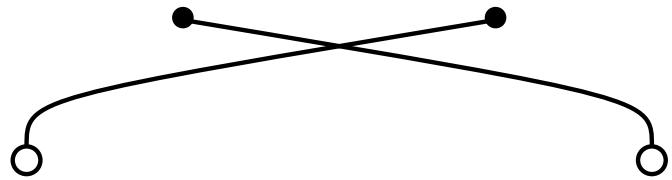
- Soit k le nombre d'arrêtes de C_n, $k \leqslant 2 \times |C_n|$ (resp. $k \leqslant |C_n|^2$),
- un nœud de C_n d'arité entrante n et sortante m est représenté par un réseau de preuve de taille au plus $9(n+m)$,
- la somme des arités entrantes et sortantes de l'ensemble des nœuds de C_n ne peut dépasser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

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

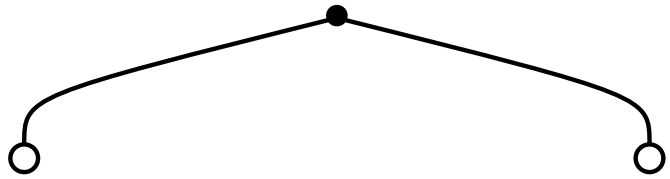
Définition (t-réduction)



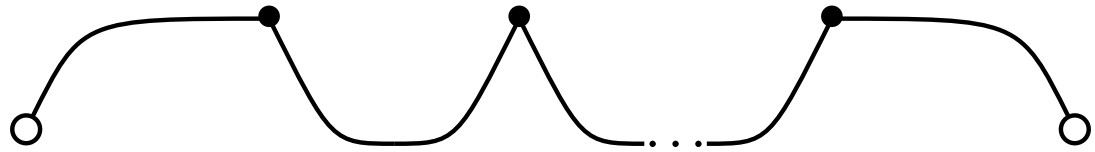
Définition (t-réduction)



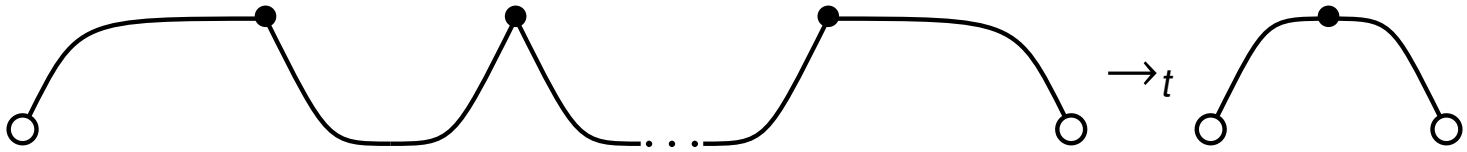
Définition (t-réduction)



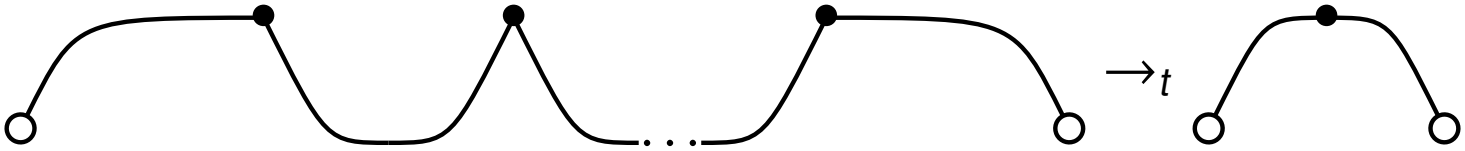
Définition (t-réduction)



Définition (t-réduction)



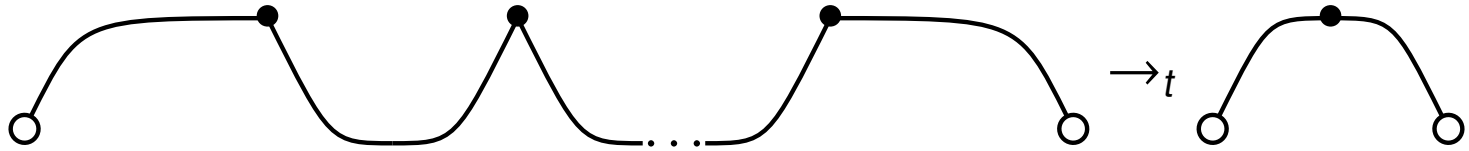
Définition (t-réduction)



Définition ($\Rightarrow$)

On écrit $P \Rightarrow Q$ si Q peut être obtenu depuis P en éliminant toutes les a-, m- ou t- coupures en parallèle.

Définition (t-réduction)



Définition ($\Rightarrow$)

On écrit $P \Rightarrow Q$ si Q peut être obtenu depuis P en éliminant toutes les a-, m- ou t- coupures en parallèle.

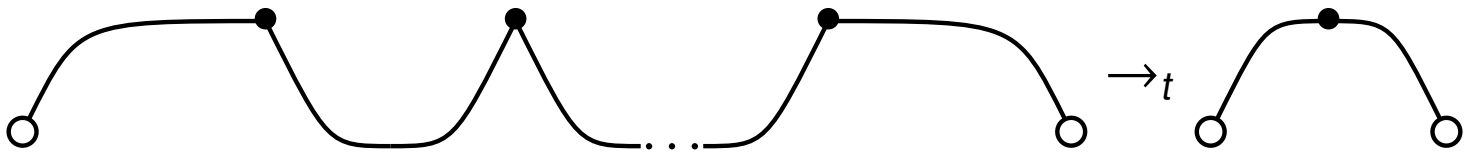
Théorème ([Terui, 2004])

Il existe une séquence de réductions parallèles

$$P \Rightarrow P_1 \Rightarrow \ldots \Rightarrow P_n$$

telle que P_n est sans coupures et $n \leqslant 3 \times d(P)$.

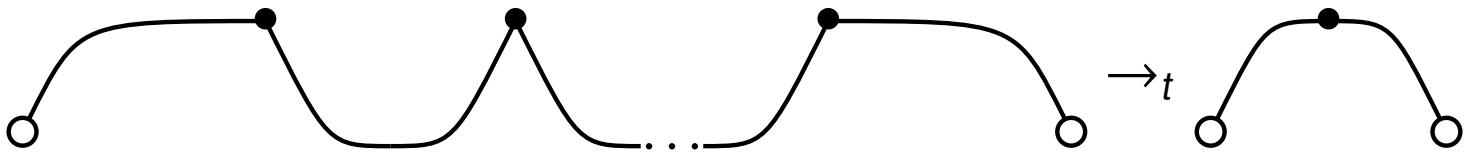
Définition (t-réduction)



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 $\mathfrak{B}_1(\mathit{UstCONN}_2)$ qui accepte le même ensemble que P.

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 $\mathscr{O}(|P|^4)$ et de profondeur $\mathscr{O}(d(P))$ sur la base $\mathfrak{B}_1(UstCONN_2)$ qui accepte le même ensemble que P.

Démonstration

C est composé de cinq sous-circuits :

1. transforme le code de P en fonction des entrées,
2. simule les $\rightarrow_t$-réduction en parallèle,
3. simule les $\rightarrow_a$-réduction en parallèle,
4. simule les $\rightarrow_m$-réduction en parallèle,
5. identifie si le résultat de l'évaluation est b_0 ou b_1.

1. Circuits booléens
2. Réseaux booléens
3. Exemples et composition
4. Circuits de preuve
5. Simulation
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. $\mathfrak{B}_1$).

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

$APN = \bigcup_{i \in \mathbb{N}} APN^i$ (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.

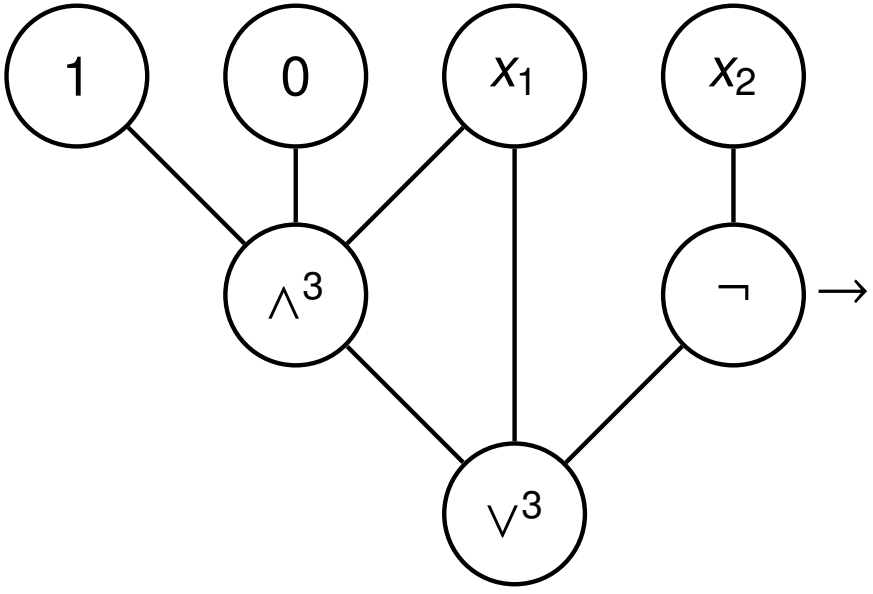
Sortie : Une description d'une famille de circuits de preuves appartenant à CCP^i tels que le résultat de l'évaluation *via* élimination des coupures de chaque circuit de preuve coïncide avec le résultat de l'évaluation du circuit booléen correspondant.

Théorème

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

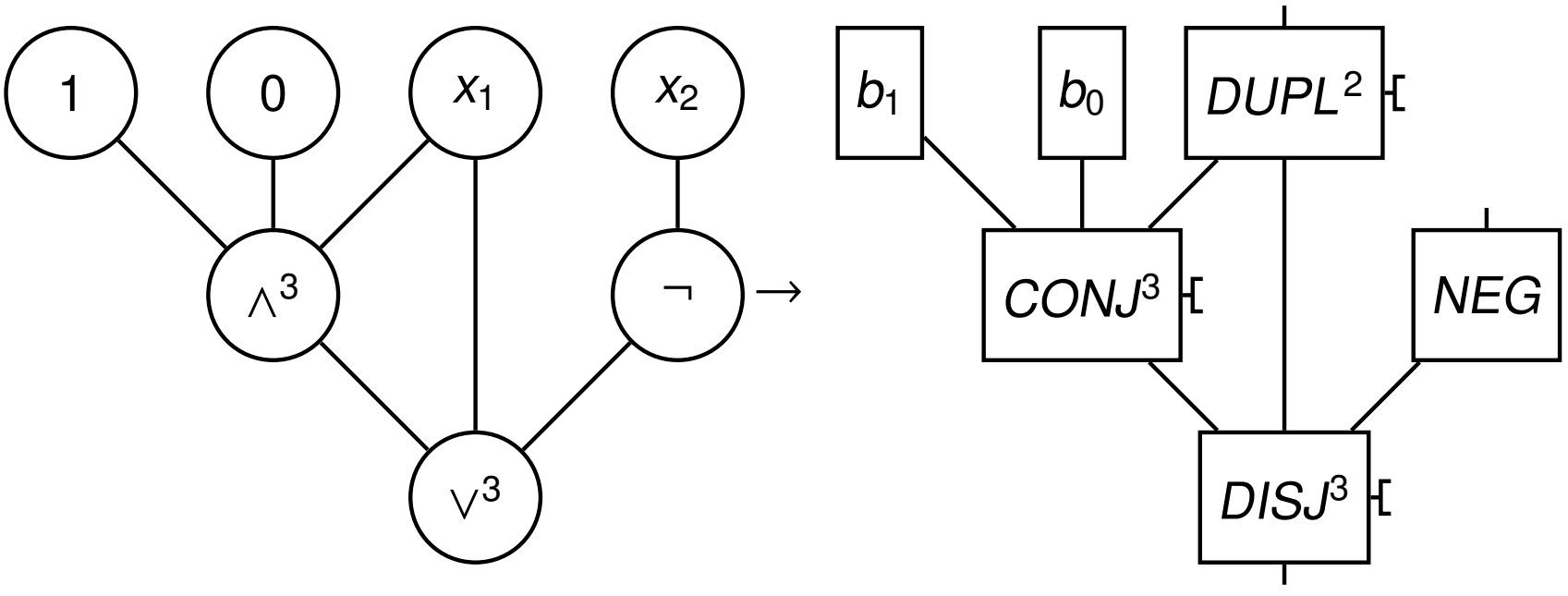
Théorème

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



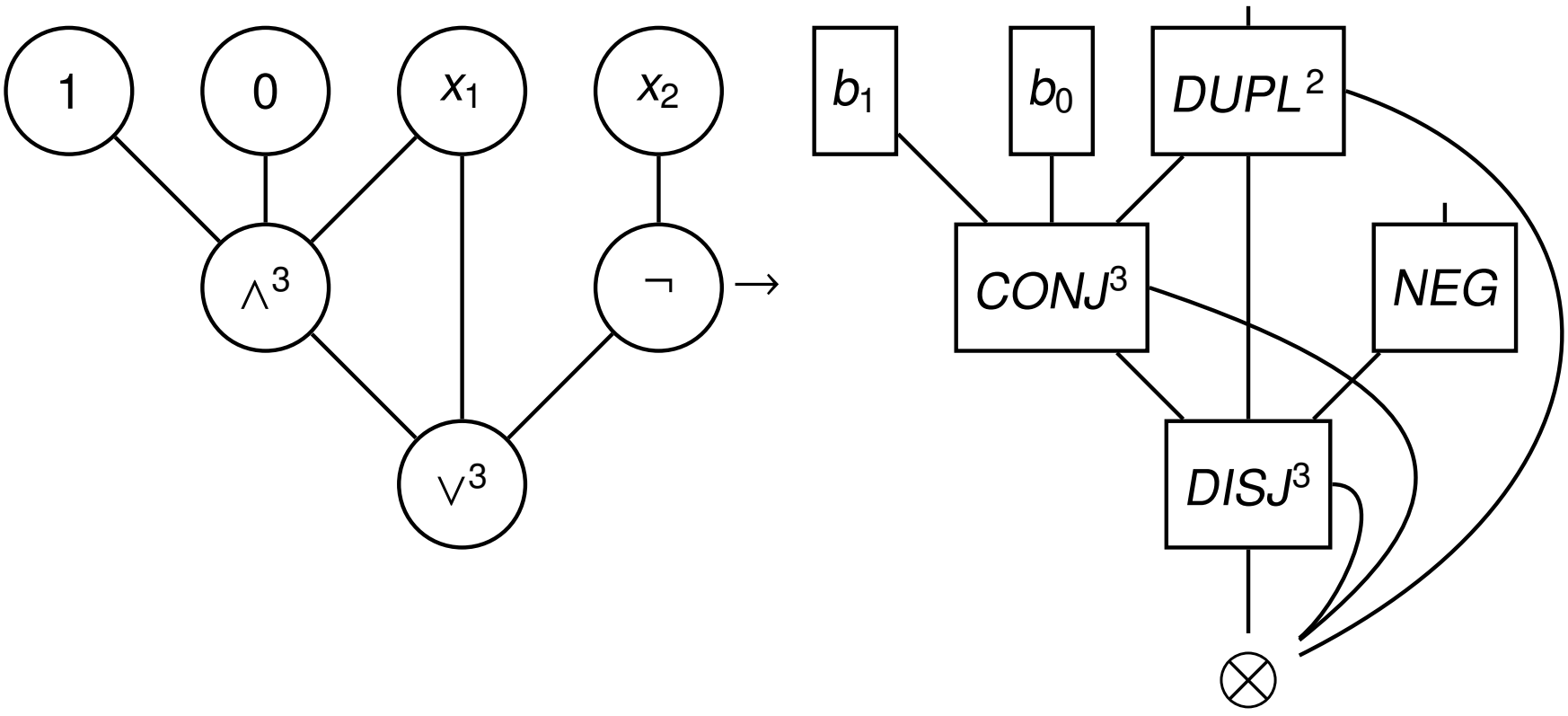
Théorème

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



Théorème

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



Inclusion des classes de complexité

Théorème

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

Inclusion des classes de complexité

Théorème

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

Remarque

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

Inclusion des classes de complexité

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.