

Théorie de Valiant

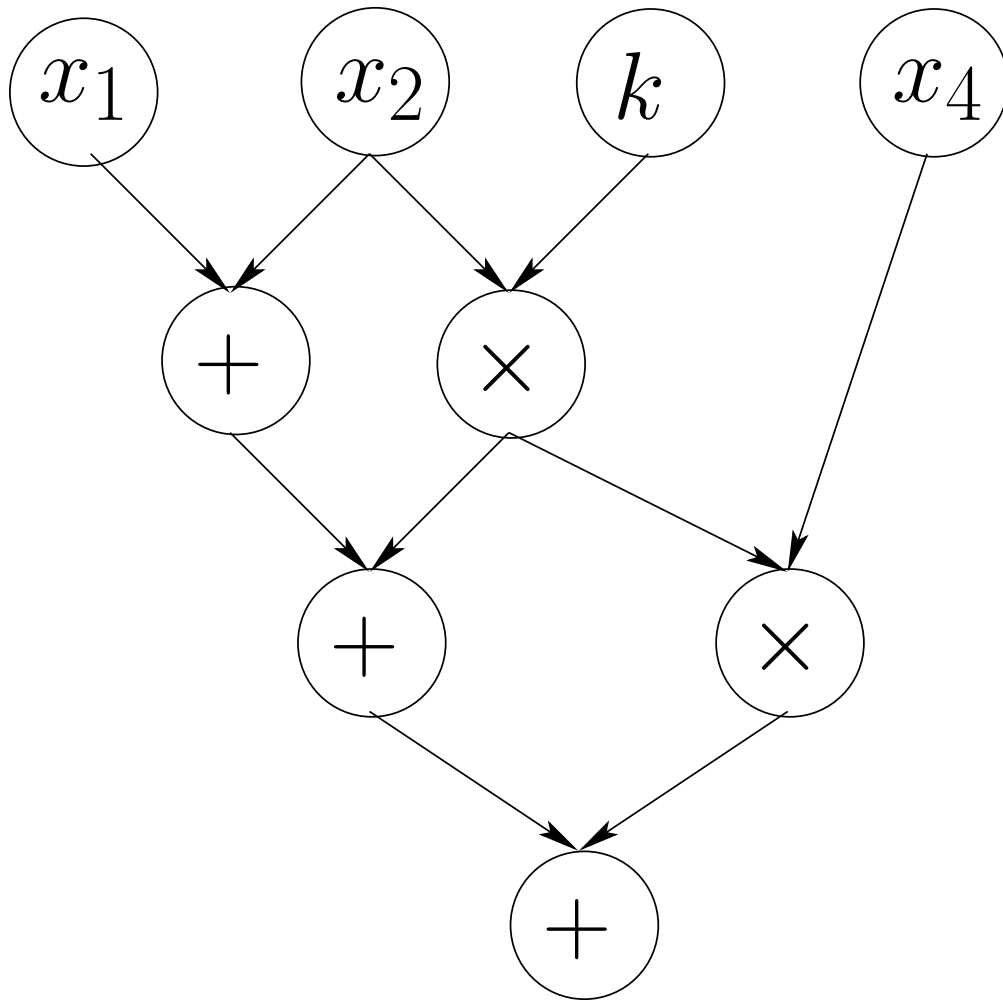
Guillaume Malod

`Guillaume.Malod@umh.ac.be`

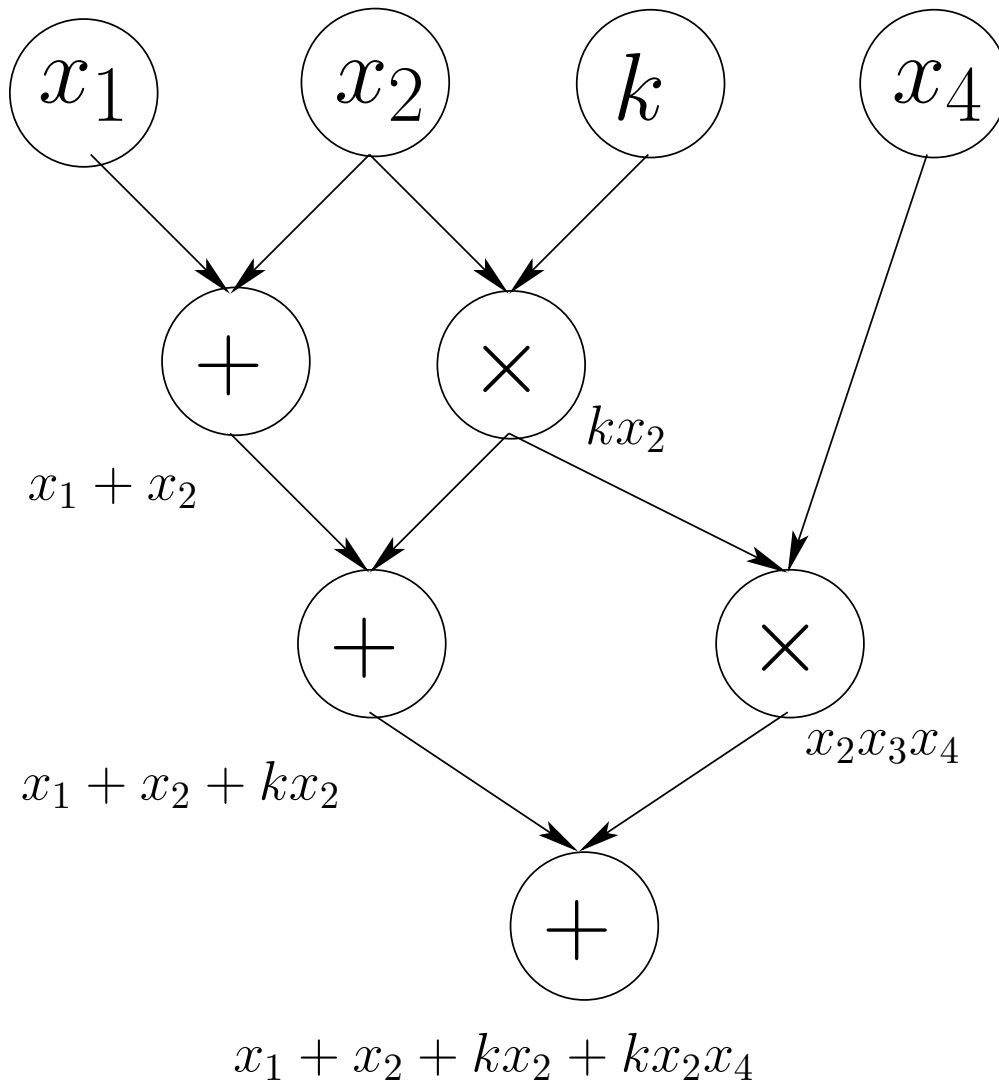
Service de logique mathématique

Université de Mons-Hainaut

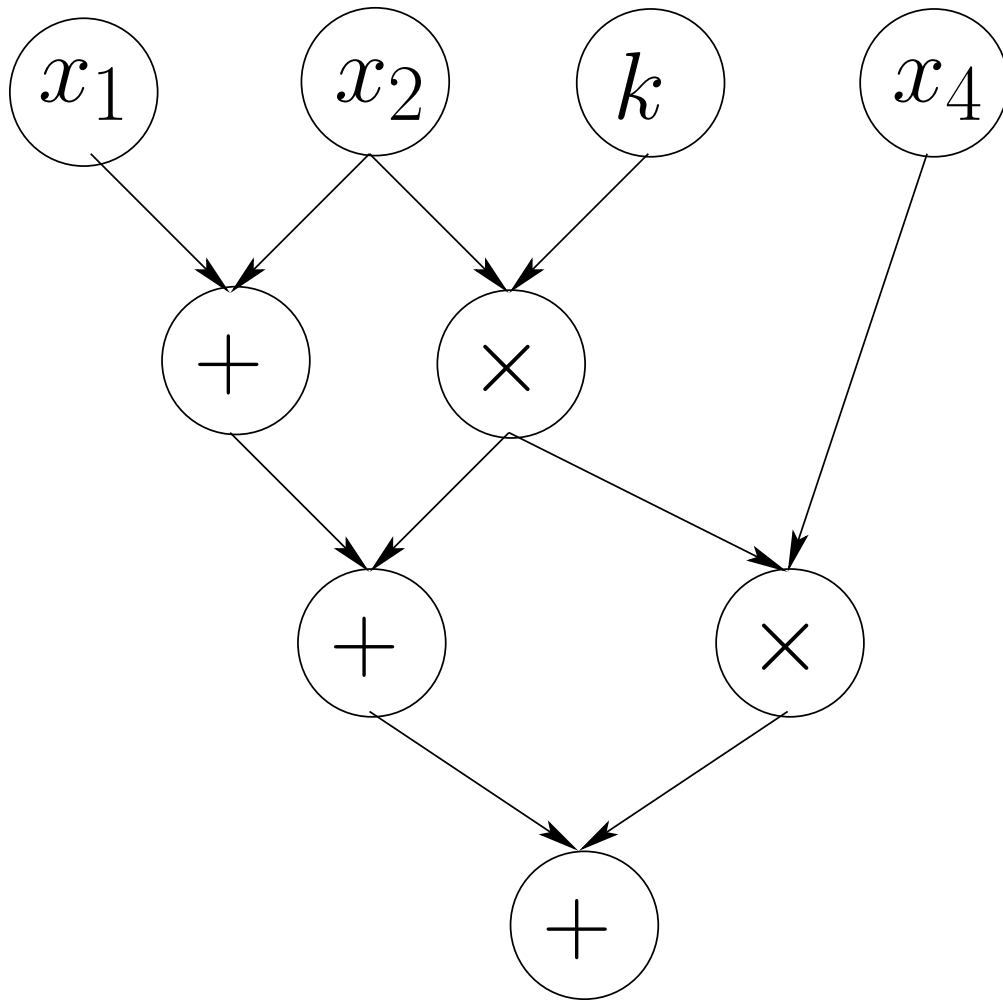
Circuits arithmétiques



Circuits arithmétiques

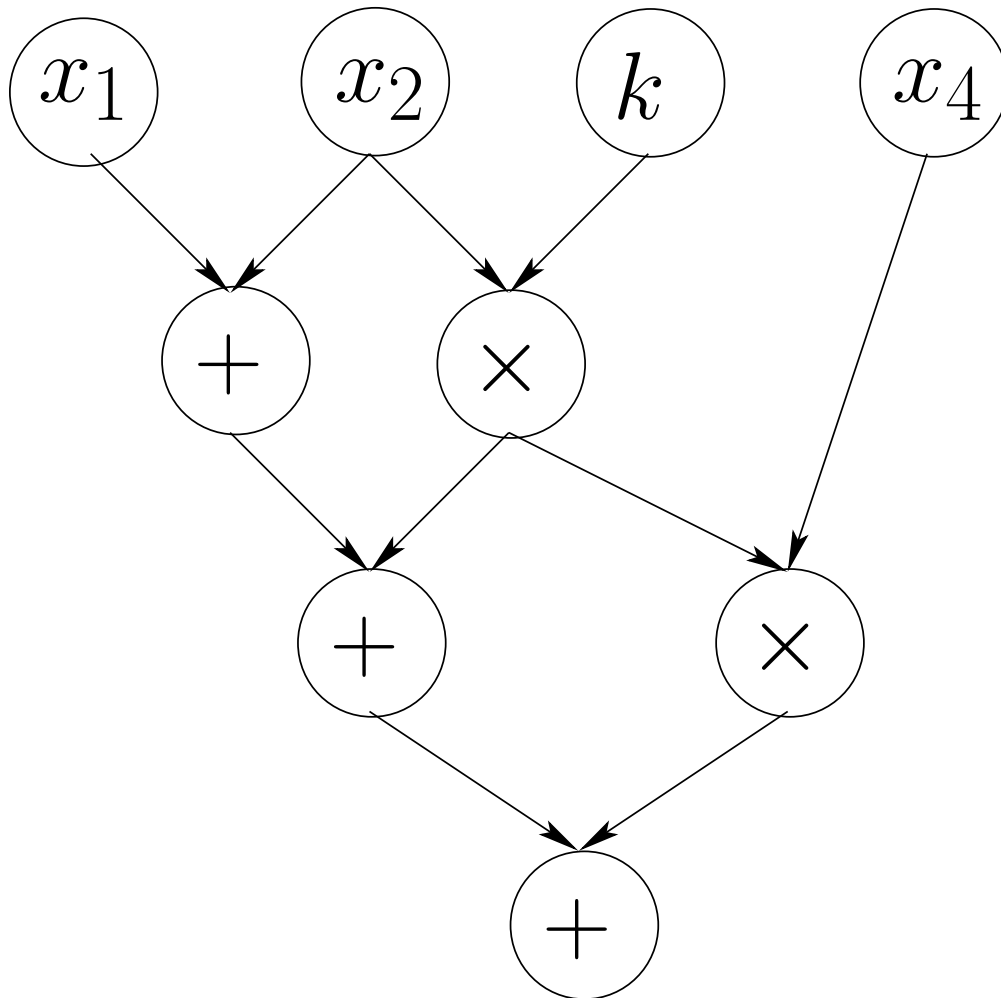


Circuits arithmétiques



Size : 9

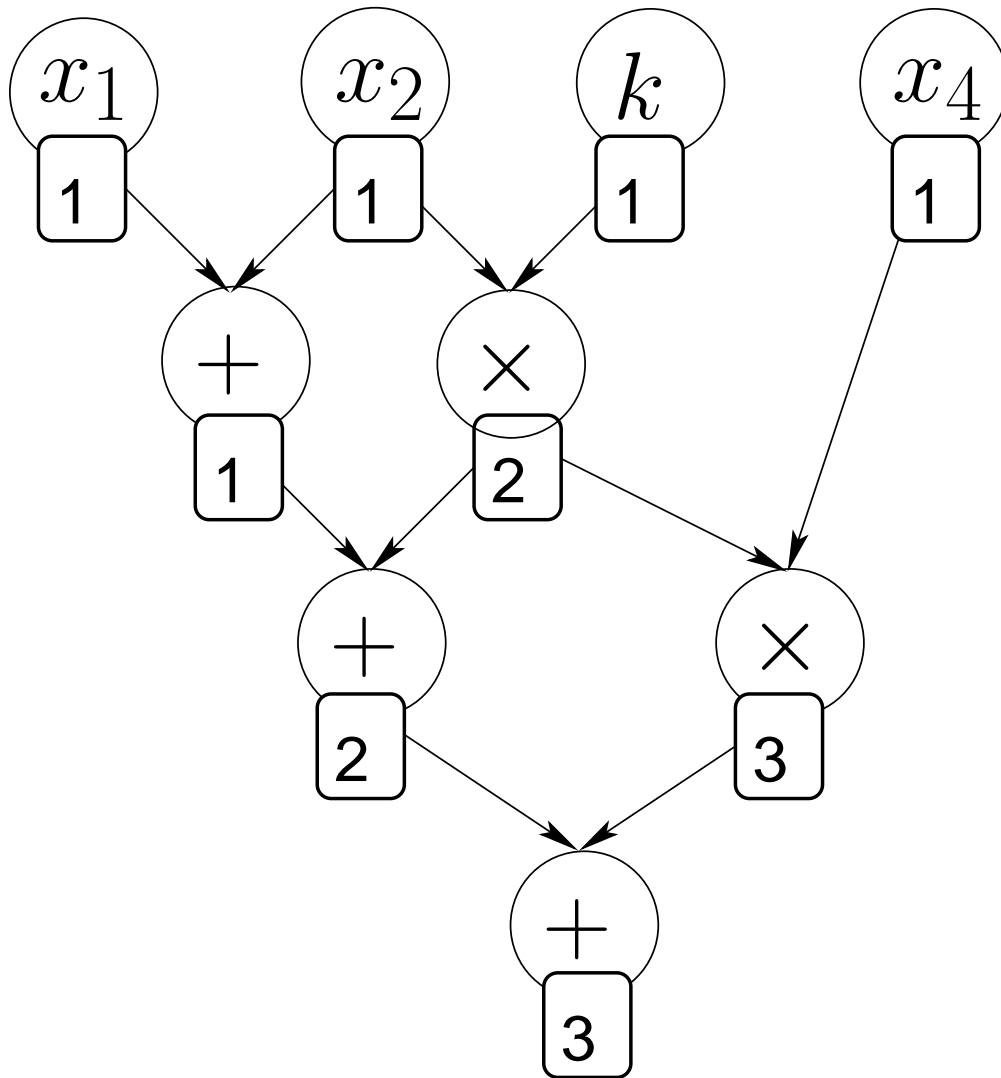
Circuits arithmétiques



Size : 9

Depth : 3

Circuits arithmétiques

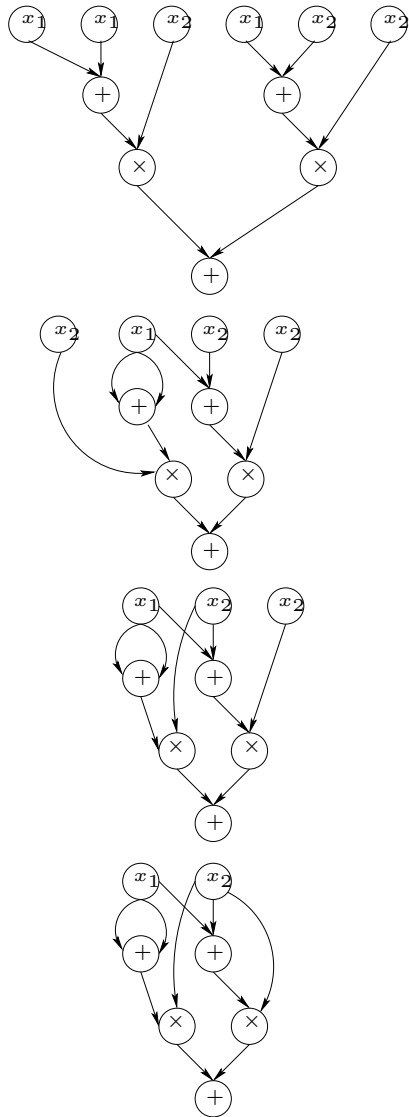


Size : 9

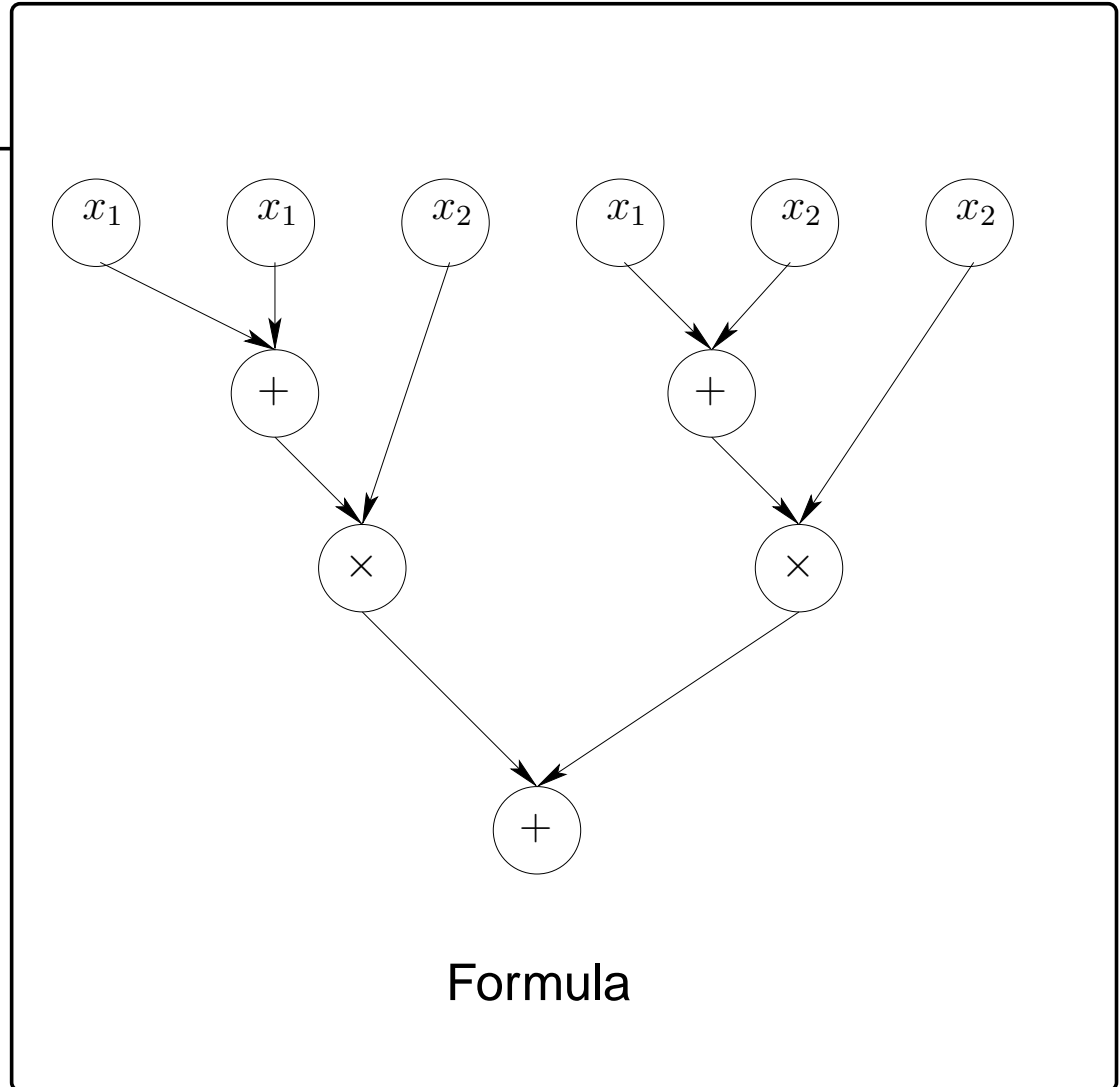
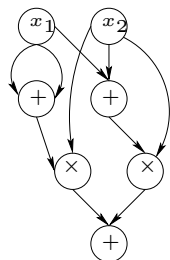
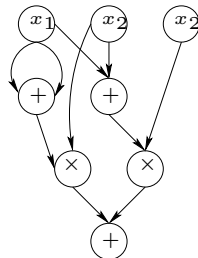
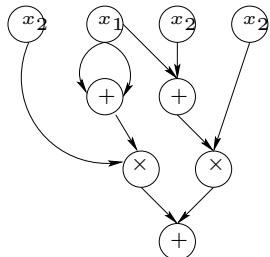
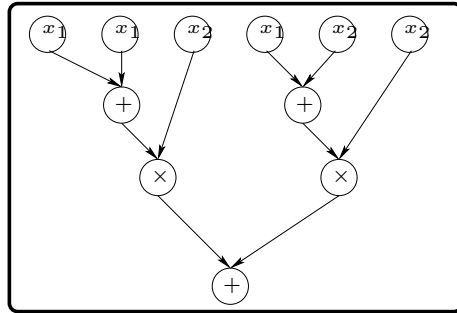
Depth : 3

Degree : 3

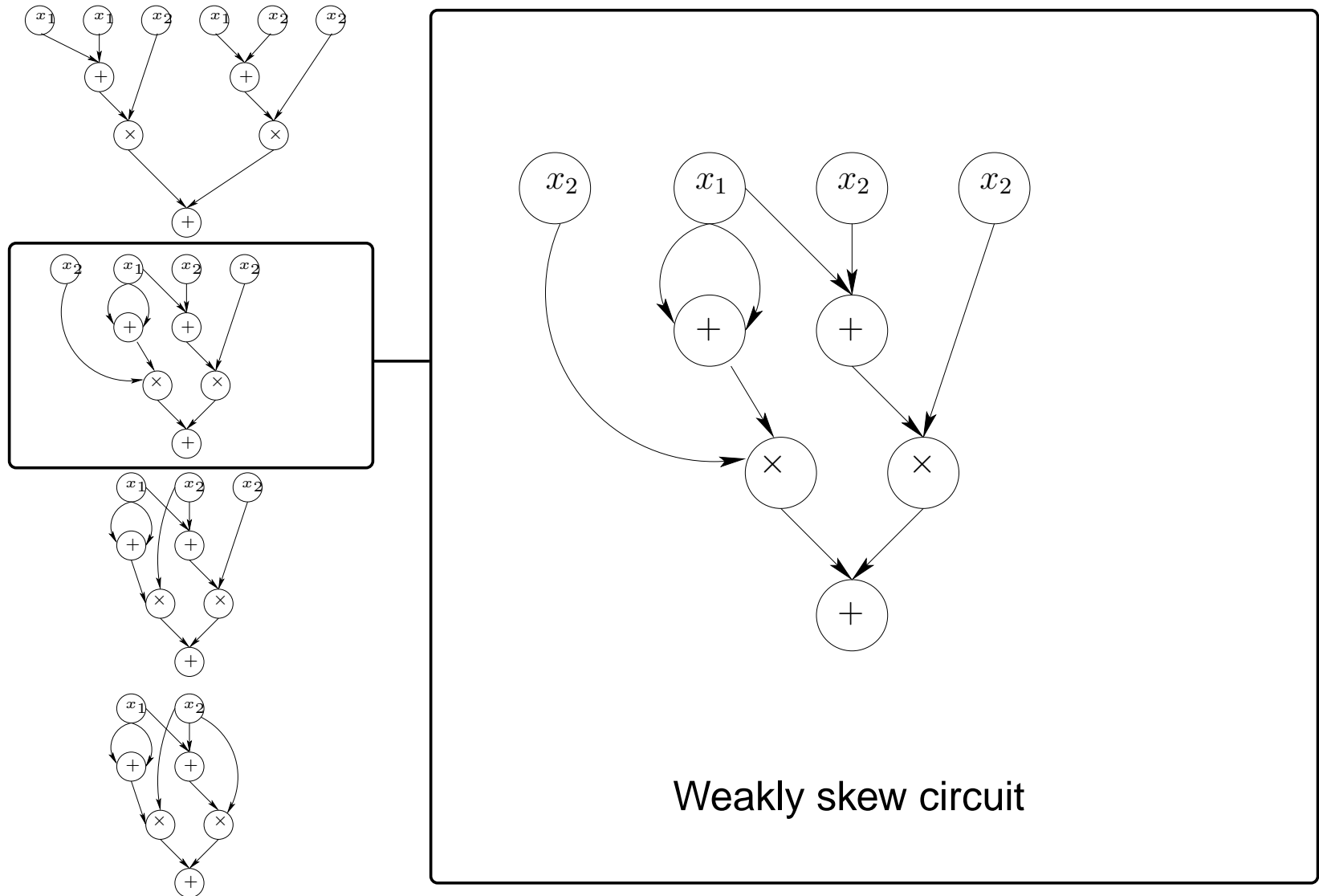
Formules et circuits



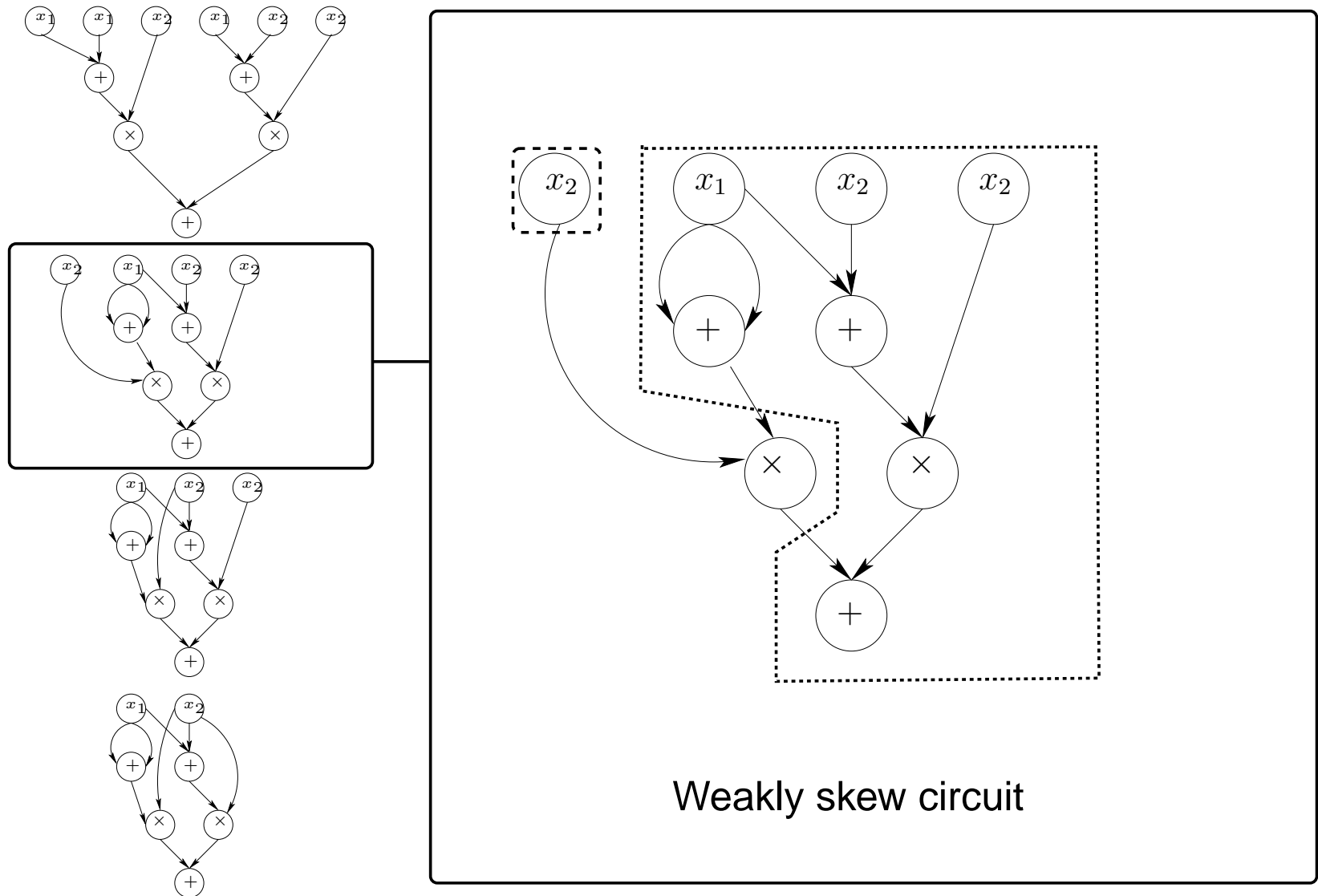
Formules et circuits



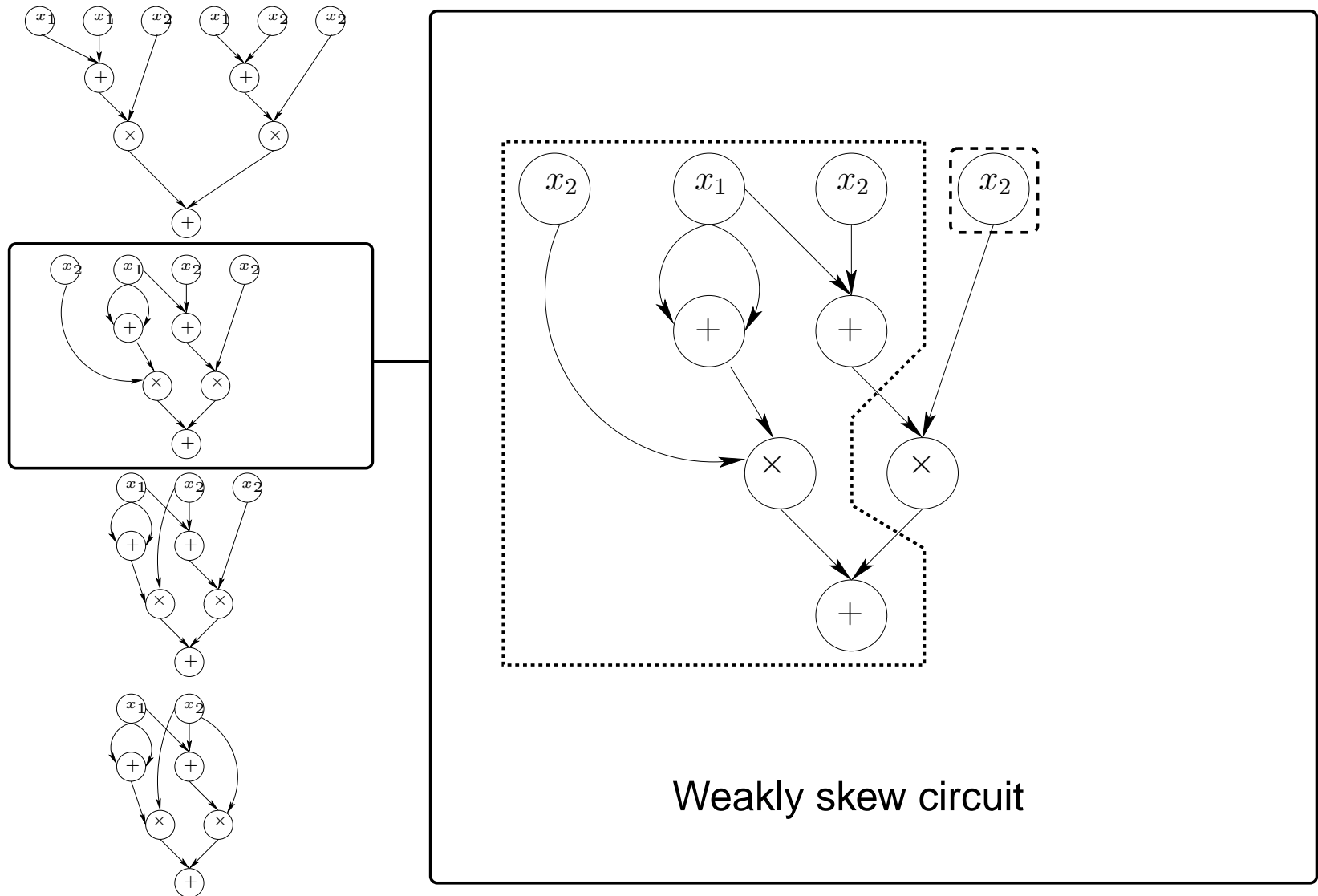
Formules et circuits



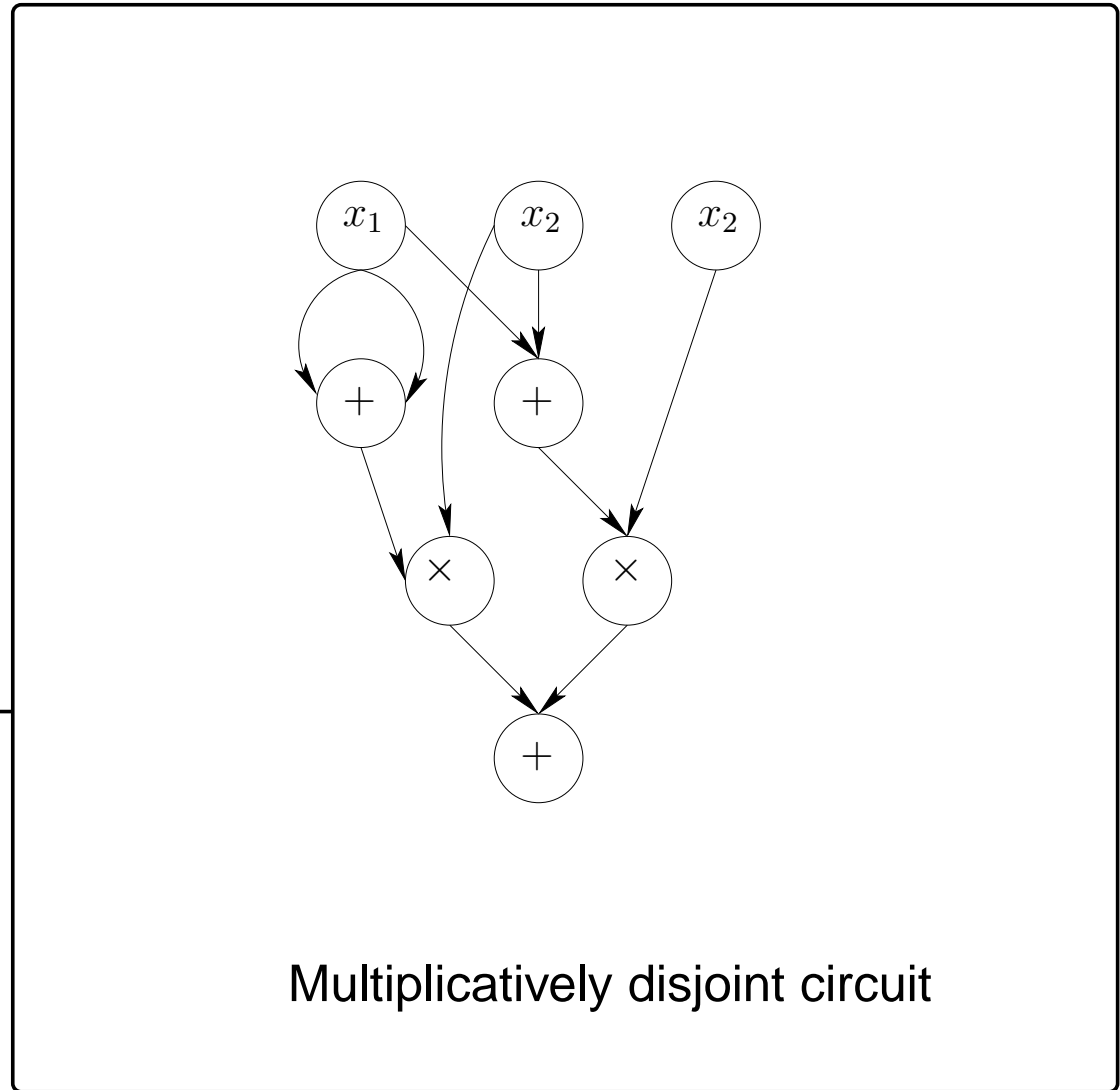
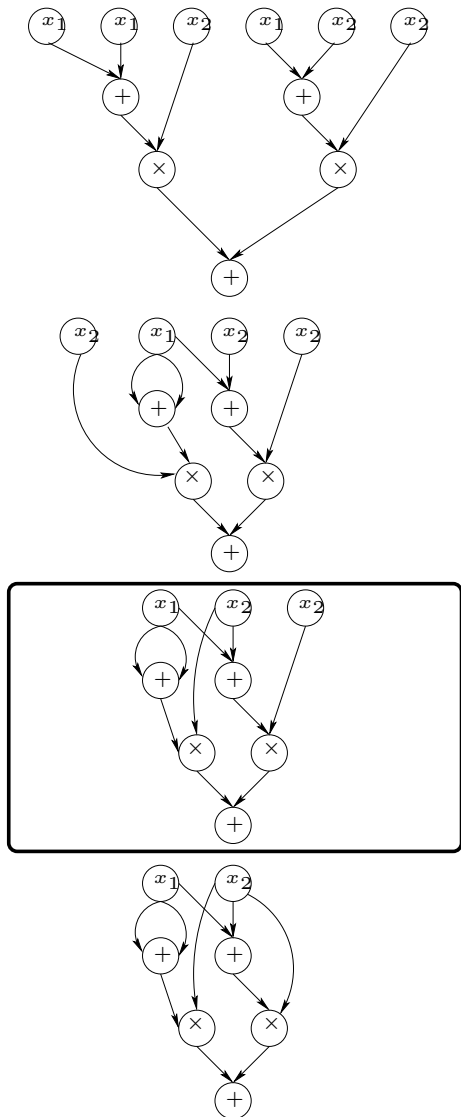
Formules et circuits



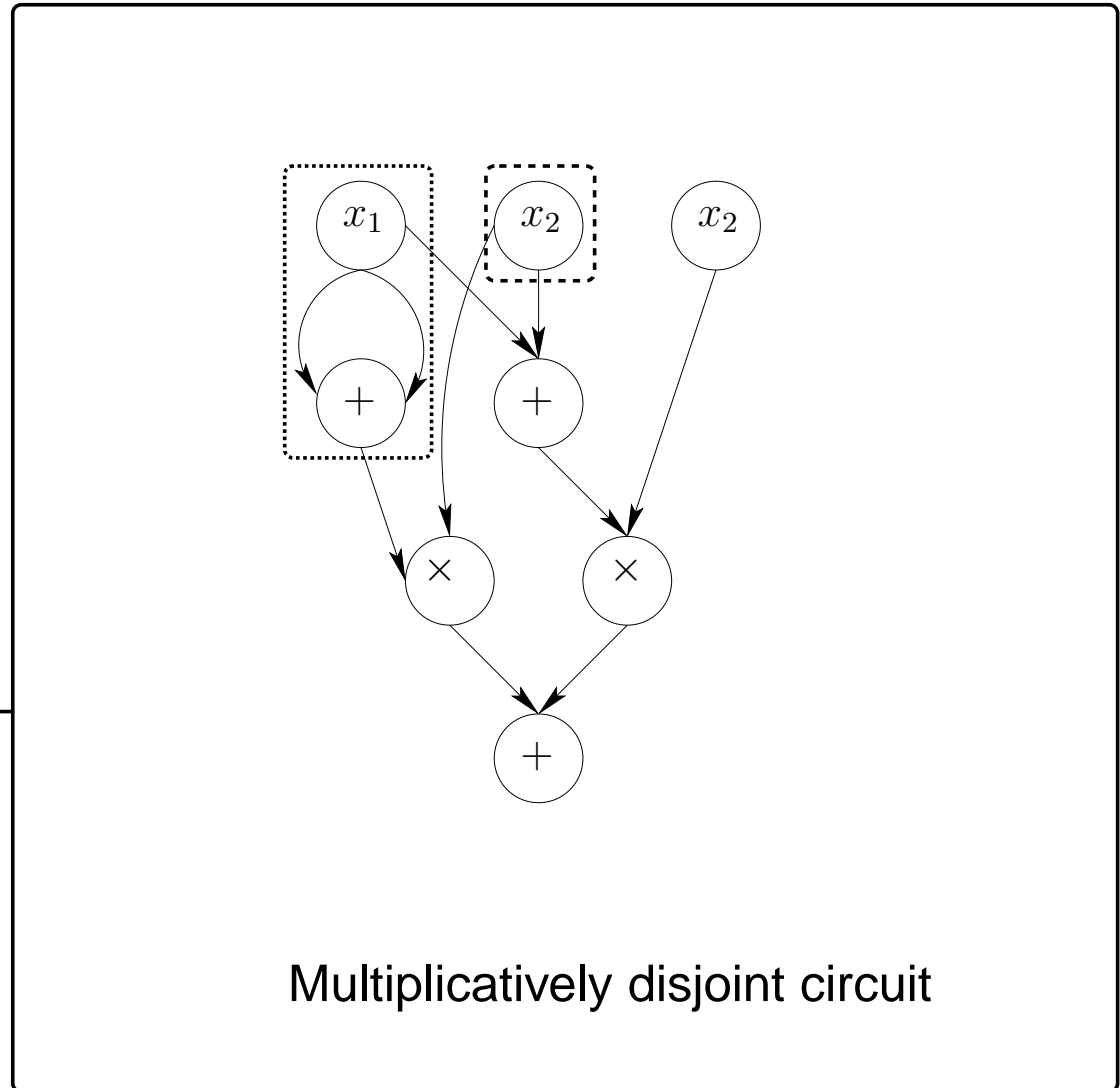
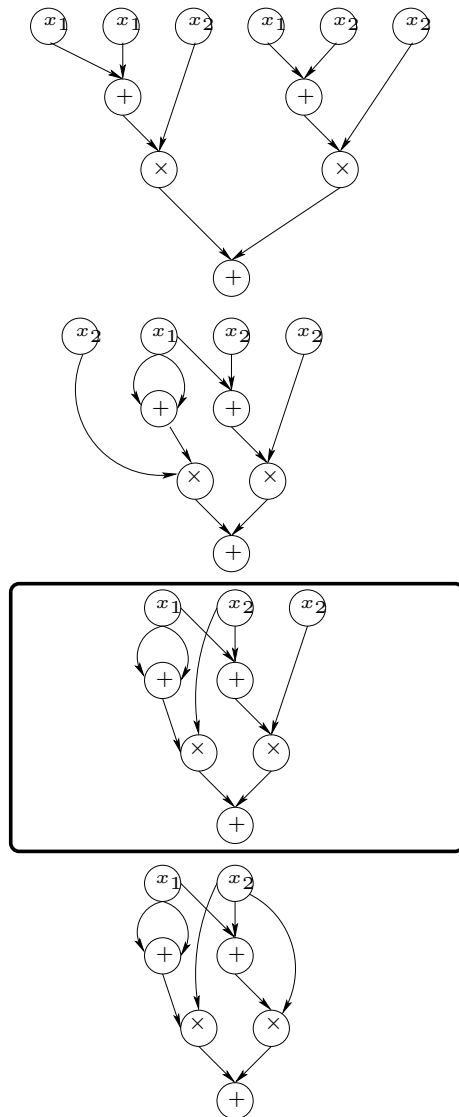
Formules et circuits



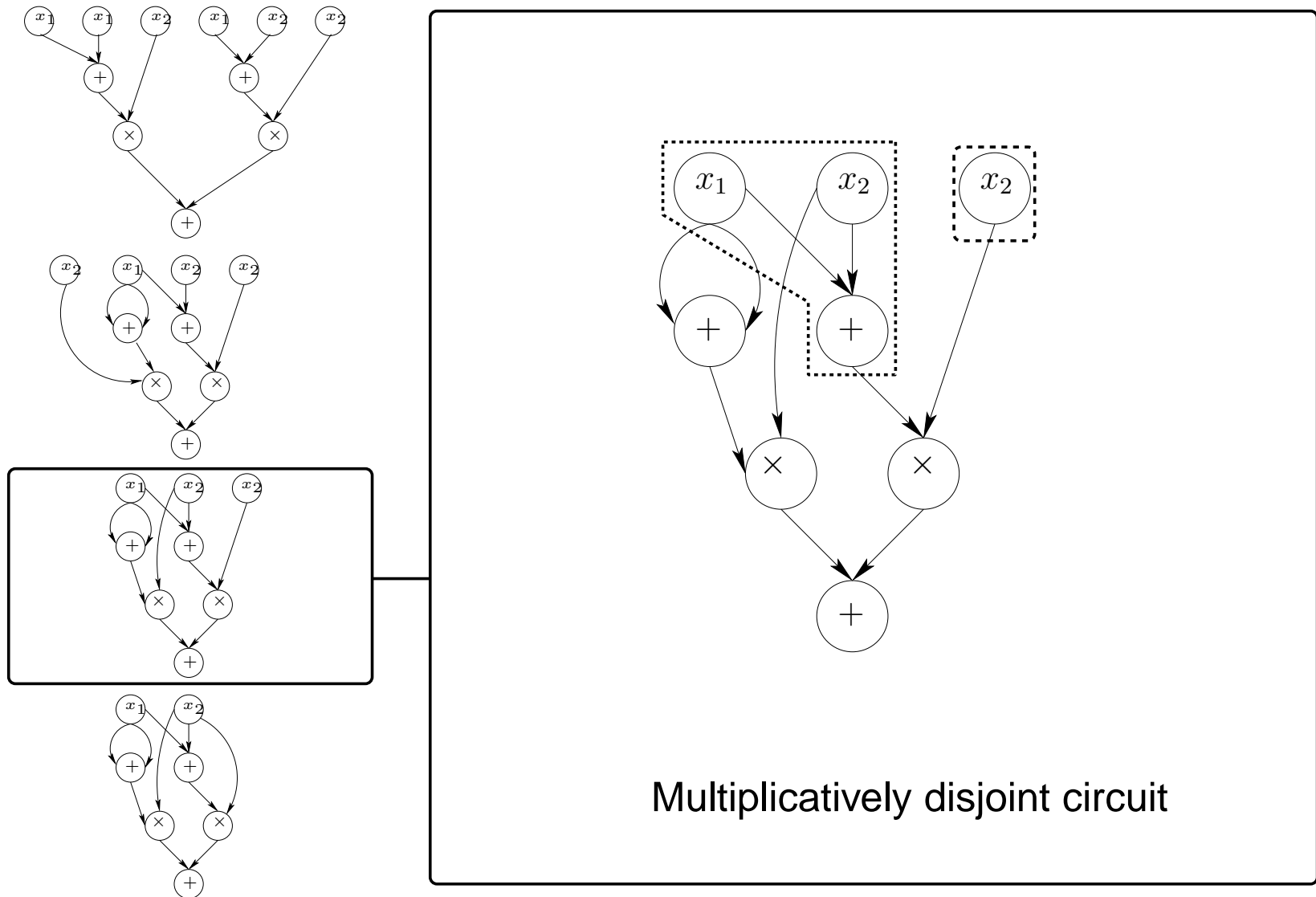
Formules et circuits



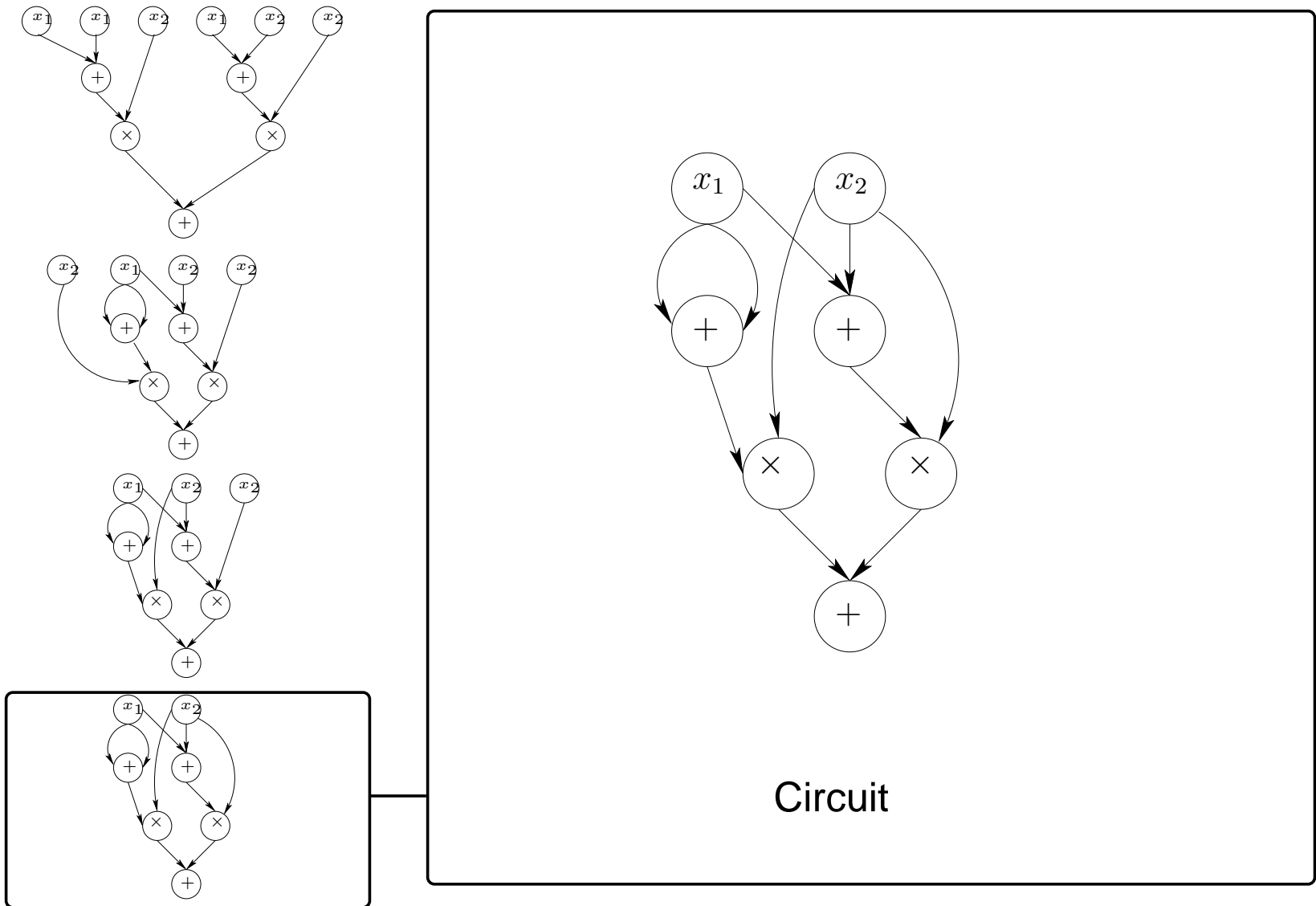
Formules et circuits



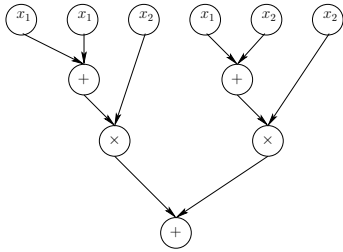
Formules et circuits



Formules et circuits



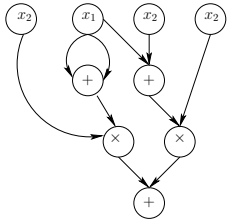
Classes de complexité



Formules

VP_e

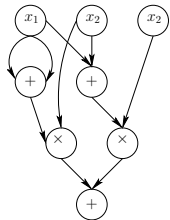
NC_1



Circuits
weakly skew

VP_{ws}

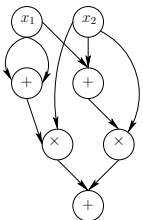
NL



Circuits MD

VP

LOGCFL



Circuits

VP_{nb}

P

Classes de complexité

$(f_n) \in VP_e$ s'il existe une suite de formules (C_n) de taille polynomialement bornée telle que C_n représente f_n .

Classes de complexité

$(f_n) \in VP_e$ s'il existe une suite de formules (C_n) de taille polynomialement bornée telle que C_n représente f_n .

$(f_n) \in VP_{ws}$ s'il existe une suite de circuits weakly skew (C_n) de taille polynomialement bornée telle que C_n représente f_n .

$(f_n) \in VP$ s'il existe une suite de circuits MD (C_n) de taille polynomialement bornée telle que C_n représente f_n .

$(f_n) \in VP_{nb}$ s'il existe une suite de circuits (C_n) de taille polynomialement bornée telle que C_n représente f_n .

Classes avec une somme

$(f_n) \in \text{VNP}$ s'il existe un polynôme p et une suite $(g_n) \in \text{VP}$ tels que :

$$f_n(\bar{x}) = \sum_{\bar{\epsilon} \in \{0,1\}^{p(|\bar{x}|)}} g_n(\bar{x}, \bar{\epsilon}).$$

Classes avec une somme

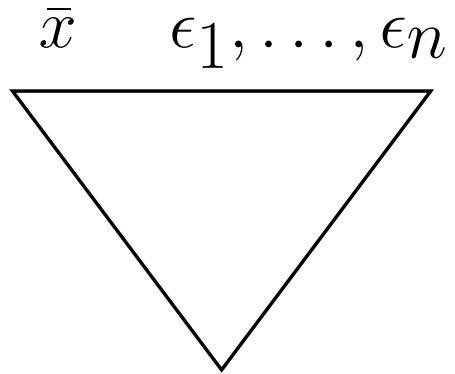
$(f_n) \in \text{VNP}$ s'il existe un polynôme p et une suite $(g_n) \in \text{VP}$ tels que :

$$f_n(\bar{x}) = \sum_{\bar{\epsilon} \in \{0,1\}^{p(|\bar{x}|)}} g_n(\bar{x}, \bar{\epsilon}).$$

$(f_n) \in \text{VNP}_{\text{nb}}$ s'il existe un polynôme p et une suite $(g_n) \in \text{VP}_{\text{nb}}$ tels que :

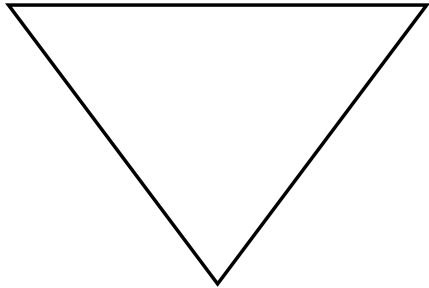
$$f_n(\bar{x}) = \sum_{\bar{\epsilon} \in \{0,1\}^{p(|\bar{x}|)}} g_n(\bar{x}, \bar{\epsilon}).$$

Classes avec une somme

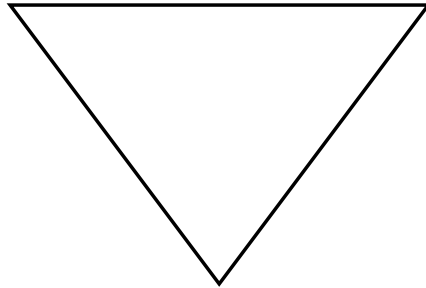


Classes avec une somme

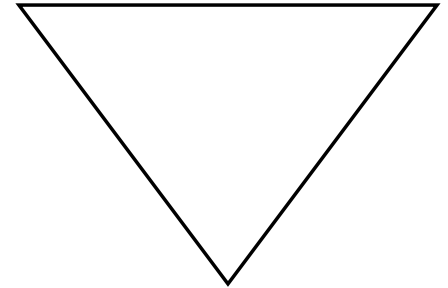
\bar{x} $0, \dots, 0$



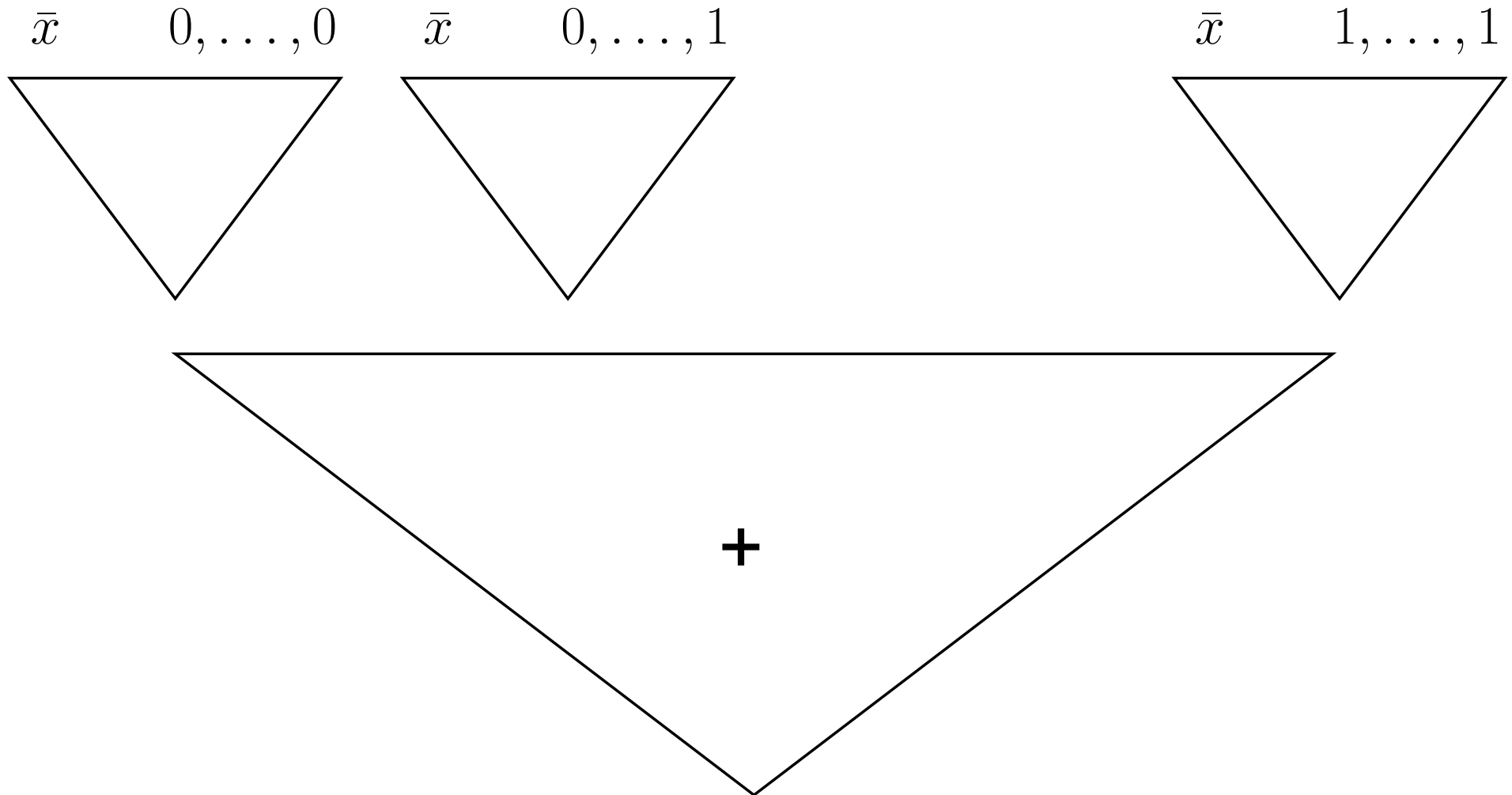
\bar{x} $0, \dots, 1$



\bar{x} $1, \dots, 1$



Classes avec une somme



Réductions

Un polynôme f est une *projection* d'un polynôme g si :

$$f(\bar{x}) = g(a_1, \dots, a_m),$$

où les a_i sont soit des constantes, soit des variables.

Réductions

Un polynôme f est une *projection* d'un polynôme g si :

$$f(\bar{x}) = g(a_1, \dots, a_m),$$

où les a_i sont soit des constantes, soit des variables.

Une suite (f_n) est une *p-projection* d'une suite (g_n) s'il existe une fonction polynomialement bornée $t(n)$ telle que f_n soit une projection de $g_{t(n)}$ pour tout n .

Déterminant et permanent

$$\text{DET}_n = \sum_{\sigma \in S_n} \epsilon(\sigma) \prod_{i=1}^n z_{i, \sigma(i)}$$

$$\text{PER}_n = \sum_{\sigma \in S_n} \prod_{i=1}^n z_{i, \sigma(i)}$$

Complétude

Théorème [Valiant] La suite (PER_n) est VNP-complète sur tout corps de caractéristique différente de 2.

Complétude

Théorème [Valiant] La suite (PER_n) est VNP-complète sur tout corps de caractéristique différente de 2.

Corollaire Sur un corps de caractéristique différente de 2, $\text{VP} = \text{VNP}$ ssi $\text{PER} \in \text{VP}$.

Complétude

Théorème [Valiant] La suite (PER_n) est VNP-complète sur tout corps de caractéristique différente de 2.

Corollaire Sur un corps de caractéristique différente de 2, $\text{VP} = \text{VNP}$ ssi $\text{PER} \in \text{VP}$.

Théorème La suite (DET_n) est VP_{WS} -complète sur tout corps.

Complétude

Théorème [Valiant] La suite (PER_n) est VNP-complète sur tout corps de caractéristique différente de 2.

Corollaire Sur un corps de caractéristique différente de 2, $\text{VP} = \text{VNP}$ ssi $\text{PER} \in \text{VP}$.

Théorème La suite (DET_n) est VP_{WS} -complète sur tout corps.

Corollaire Sur tout corps de caractéristique différente de 2, $\text{VP}_{\text{WS}} = \text{VNP}$ ssi le permanent est une p -projection du déterminant.

Suites complètes

VP_e	Formules	– produit de n matrices d'ordre 3
VP_{ws}	Circuits WS	– produit de n matrices d'ordre n – puissance n^e d'une matrice d'ordre n – inverse d'une matrice d'ordre n – déterminant d'une matrice d'ordre n
VP	Circuits MD	
VP_{nb}	Circuits	– alternance de produits et d'élevations au carré de matrices d'ordre n
VNP		– permanent ou hamiltonien d'une matrice d'ordre n , ...
VNP_{nb}		

Suites complètes

VP_e	Formules prof. $\log n$	formules matricielles (dimension constante)
VP_{ws}		formules matricielles
VP	Circuits semi-bornés prof. $\log n$	formules tensorielles <i>tame</i>
VP_{nb}		circuits tensoriels
VNP		formules tensorielles
VNP_{nb}		

Une propriété du déterminant

Peut-on écrire toute combinaison linéaire

$$\lambda_1 \text{DET} X_1 + \dots + \lambda_n \text{DET} X_n$$

comme un déterminant $\text{DET} X_m$,
où la taille de X_m est polynomialement bornée en n et le
maximum des tailles des X_i ?

Une propriété du déterminant

Peut-on écrire toute combinaison linéaire

$$\lambda_1 \text{DET} X_1 + \dots + \lambda_n \text{DET} X_n$$

comme un déterminant $\text{DET} X_m$,

où la taille de X_m est polynomialement bornée en n et le maximum des tailles des X_i ?

Théorème Le déterminant est linéairement clos.

Dérivation

Théorème Les propriétés suivantes sont équivalentes :

1. $VP = VNP$.
2. La classe VP est stable pour la prise de dérivées partielles itérées d'ordre polynomialement borné.

Dérivation

Théorème Les propriétés suivantes sont équivalentes :

1. $VP = VNP$.
2. La classe VP est stable pour la prise de dérivées partielles itérées d'ordre polynomialement borné.

Théorème (En caractéristique non-nulle) Les propriétés suivantes sont équivalentes :

1. $VP_{nb} = VNP_{nb}$.
2. La classe VP_{nb} est stable pour la prise de dérivées partielles itérées d'ordre polynomialement borné.

Dérivation

$$f_n(\bar{y}, \bar{z}) = \prod_{i=1}^n \left(\sum_{j=1}^n z_{i,j} y_j \right)$$

Le coefficient de $y_1 \cdots y_n$ dans f_n est le permanent des $(z_{i,j})$.

Dérivation

$$f_n(\bar{y}, \bar{z}) = \prod_{i=1}^n \left(\sum_{j=1}^n z_{i,j} y_j \right)$$

Le coefficient de $y_1 \cdots y_n$ dans f_n est le permanent des $(z_{i,j})$.

$$\frac{\partial^n f_n}{\partial y_1 \cdots \partial y_n} = \text{PER}_n(z_{i,j})$$

Fonctions coefficients

$$f(\bar{x}) = \sum_{\bar{\epsilon} \in \{0,1\}^{n \lceil \log d \rceil}} g(\bar{\epsilon}) \bar{x}^{\bar{\epsilon}}.$$

$$f(\bar{x}, \bar{y}) = \sum_{\bar{\epsilon} \in \{0,1\}^{n \lceil \log d \rceil}} g(\bar{y}, \bar{\epsilon}) \cdot \bar{x}^{\bar{\epsilon}}.$$

Coefficients binomiaux

$$(x + y)^{2^n} = \sum_{k=0}^{2^n} \binom{2^n}{k} x^k y^{2^n - k}$$

Coefficients binomiaux

$$(x + y)^{2^n} = \sum_{k=0}^{2^n} \binom{2^n}{k} x^k y^{2^n - k}$$

Théorème [Lucas, 1878] Soit $m = m_0 + m_1p + \dots + m_dp^d$ et $n = n_0 + n_1p + \dots + n_dp^d$ deux entiers décomposés en base p , alors :

$$\binom{n}{m} \equiv \binom{n_0}{m_0} \binom{n_1}{m_1} \dots \binom{n_d}{m_d} \pmod{p}.$$

La factorielle

Si on sait calculer rapidement ces gros coefficients binomiaux, alors on sait calculer rapidement la factorielle.

La factorielle

Si on sait calculer rapidement ces gros coefficients binomiaux, alors on sait calculer rapidement la factorielle.

Théorème [Shub & Smale 1996] Si $k!$ n'est pas *ultimately easy to compute*, $P \neq NP$ sur \mathbb{C} .

La factorielle

Si on sait calculer rapidement ces gros coefficients binomiaux, alors on sait calculer rapidement la factorielle.

Théorème [Shub & Smale 1996] Si $k!$ n'est pas *ultimately easy to compute*, $P \neq NP$ sur \mathbb{C} .

Théorème [Koiran 2004] Si $k!$ n'est pas *ultimately easy to compute*, alors soit $VP^0 \neq VNP^0$, soit $P \neq PSPACE$.

La factorielle

Si on sait calculer rapidement ces gros coefficients binomiaux, alors on sait calculer rapidement la factorielle.

Théorème [Shub & Smale 1996] Si $k!$ n'est pas *ultimately easy to compute*, $P \neq NP$ sur \mathbb{C} .

Théorème [Koiran 2004] Si $k!$ n'est pas *ultimately easy to compute*, alors soit $VP^0 \neq VNP^0$, soit $P \neq PSPACE$.

Théorème [Bürgisser 2007] Si $k!$ n'est pas *easy to compute*, alors $VP^0 \neq VNP^0$.

Sommes multiples

(Poizat 2007)

Sommes multiples

(Poizat 2007)

Un circuit peut utiliser des portes « sommes de Valiant » de manière arbitraire.

Sommes multiples

(Poizat 2007)

Un circuit peut utiliser des portes « sommes de Valiant » de manière arbitraire.

Théorème La classe VSP est stable pour la prise de fonctions coefficients.

Sommes multiples

(Poizat 2007)

Un circuit peut utiliser des portes « sommes de Valiant » de manière arbitraire.

Théorème La classe VSP est stable pour la prise de fonctions coefficients.

Théorème La factorielle est calculable par un circuit à sommes multiples de taille polynomiale.

Sommes multiples

(Poizat 2007)

Un circuit peut utiliser des portes « sommes de Valiant » de manière arbitraire.

Théorème La classe VSP est stable pour la prise de fonctions coefficients.

Théorème La factorielle est calculable par un circuit à sommes multiples de taille polynomiale.

Théorème Si $VSP \neq VP_{nb}$, alors soit $P \neq PSPACE$, soit $VP^0 \neq VNP^0$.

Circuits et analyse numérique

Soit une fonction à calculer :

1. on trouve un moyen de la calculer dans un modèle parfait comme les circuits arithmétiques avec divisions.
2. on effectue ce calcul à une précision donnée.

Circuits et analyse numérique

Soit une fonction à calculer :

1. on trouve un moyen de la calculer dans un modèle parfait comme les circuits arithmétiques avec divisions.
2. on effectue ce calcul à une précision donnée.

Sur la donnée d'un entier k en unaire, d'un circuit avec divisions prenant des nombres flottants en entrée, avec la promesse que le circuit ne vaut pas 0 et ne fait pas de divisions par 0, calculer une approximation du résultat à la précision k .

Circuits et analyse numérique

PosSLP : Sur la donnée d'un circuit arithmétique (sans divisions) dont la seule entrée est -1 , déterminer si l'entier calculé est strictement positif.

Circuits et analyse numérique

P_{PosSLP} : Sur la donnée d'un circuit arithmétique (sans divisions) dont la seule entrée est -1 , déterminer si l'entier calculé est strictement positif.

Proposition [ABKPM 2005] L'étape (2) ci-dessus est équivalente au problème P_{PosSLP} .

Circuits et analyse numérique

P_{PosSLP} : Sur la donnée d'un circuit arithmétique (sans divisions) dont la seule entrée est -1 , déterminer si l'entier calculé est strictement positif.

Proposition [ABKPM 2005] L'étape (2) ci-dessus est équivalente au problème P_{PosSLP} .

Théorème [ABKPM 2005] $P^{P_{\text{PosSLP}}} = \text{BP}(\mathbb{P}_{\mathbb{R}}^{\text{algebraic}})$