Complexité : TD 4

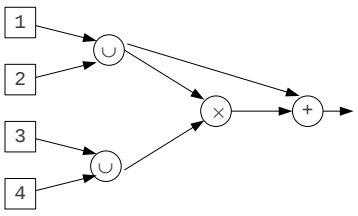
Chargé de TD : Adrien Koutsos

Exercice 1

Un *circuit entier* $\mathcal{C}$ est défini par un graphe orienté sans circuit dont :
- les sommets sans prédécesseur sont appelés les *entrées* et sont étiquetés par un élément de $\mathbb{N}$ (confondu avec le singleton contenant cet entier).
- Les autres sommets sont appelés des *portes* et sont étiquetés par l'une des trois opérations $+, \times, \cup$. Toutes les portes admettent deux prédécesseurs. L'une des portes est appelée *sortie*.

La sémantique d'un circuit consiste à associer à toute porte un ensemble d'entiers défini comme suit. Si g est une porte et E_1, E_2 sont les ensembles associés à ses deux prédécesseurs alors $E(g)$ est défini par :
- g est étiqueté par $+$: $E(g) = \{x + y \mid x \in E_1 \wedge y \in E_2\}$.
- g est étiqueté par $\times$: $E(g) = \{x \times y \mid x \in E_1 \wedge y \in E_2\}$.
- g est étiqueté par $\cup$: $E(g) = E_1 \cup E_2$.

Question 1. Calculez l'ensemble d'entiers associé à la porte de sortie du circuit représenté ci-dessous.



Question 2. Soient $j, k > 0$ deux entiers. Construisez un circuit de sortie *out* ayant pour seule entrée j, tel que $E(out) = \{j, 2j, 3j, \ldots, 2^k j\}$ et comprenant $O(k)$ portes.

Problème du circuit entier. Le problème du circuit entier, noté ICE, est défini par un couple $(\mathcal{C}, x)$ où $\mathcal{C}$ est un circuit entier et x est un entier. Il consiste à déterminer si x appartient à $E(out)$ où *out* désigne la porte de sortie de $\mathcal{C}$.

Question 3. Proposez un algorithme récursif qui prend en entrée un circuit $\mathcal{C}$, un sommet g du circuit $\mathcal{C}$ et un entier x, et détermine si x appartient à $E(g)$.

Question 4. Analysez la complexité spatiale de votre algorithme et en déduire que le problème du circuit entier est dans PSPACE.

Exercice 2

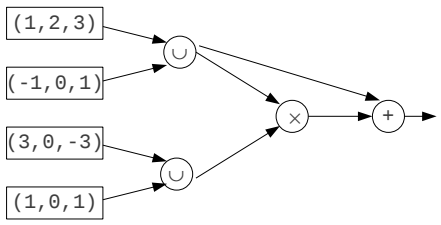
Un *circuit vectoriel* $\mathcal{C}$ de dimension n est défini par un graphe orienté sans circuit dont :

- les sommets sans prédécesseur sont appelés les entrées et sont étiquetés par un vecteur de $\mathbb{Z}^n$ (confondu avec le singleton contenant ce vecteur).
- Les autres sommets sont appelés des portes et sont étiquetés par l'une des trois opérations $+, \times, \cup$. Toutes les portes admettent deux prédécesseurs. L'une des portes est appelée sortie.

La sémantique d'un circuit consiste à associer à toute porte un ensemble de vecteurs défini comme suit. Si g est une porte et E_1, E_2 sont les ensembles associés à ses deux prédécesseurs alors $E(g)$ est défini par :

- g est étiqueté par $+$: $E(g) = \{x + y \mid x \in E_1 \wedge y \in E_2\}$.
- g est étiqueté par $\times$: $E(g) = \{x \times y \mid x \in E_1 \wedge y \in E_2\}$ avec $(x \times y)_i = x_i y_i$, i.e. le produit terme à terme.
- g est étiqueté par $\cup$: $E(g) = E_1 \cup E_2$.

Question 5. Calculez l'ensemble de vecteurs associé à la porte de sortie du circuit vectoriel représenté ci-dessous.



Problème du circuit vectoriel. Le problème du circuit vectoriel, noté VCE, est défini par un couple $(\mathcal{C}, x)$ où $\mathcal{C}$ est un circuit vectoriel et x est un vecteur de même dimension. Il consiste à déterminer si x appartient à $E(out)$ où out désigne la porte de sortie de $\mathcal{C}$.

Dans la suite de cette partie, on établit une réduction en temps polynomial du problème QBF-DNF de l'évaluation d'une formule quantifiée booléenne $\varphi \equiv Q_n x_n \dots Q_1 x_1 \psi$ où ψ est donnée sous forme DNF (i.e. ψ est une disjonction de clauses conjonctives) vers le problème VCE.

Préliminaires.

- Les variables (libres ou liées) des formules de cette partie sont incluses dans $\{x_1, \dots, x_n\}$ et les circuits sont de dimension n.
- Un vecteur $\vec{v} = (v_1, \dots, v_n)$ tel que pour tout i, $v_i \in \{-1, 1\}$ est appelé un *vecteur d'affectation* ; il correspond à l'affectation des variables définie par $x_i = \textbf{true}$ (resp. $x_i = \textbf{false}$) si $v_i = 1$ (resp. $v_i = -1$).

— Soit φ une formule, la *table de vérité* de φ, notée $\mathbf{T}(\varphi)$ est l'ensemble des vecteurs d'affectation correspondant aux affectations satisfaisant φ. Attention, les affectations n'affectent que les variables libres. Par conséquent, la table de vérité d'une formule close est soit l'ensemble de tous les vecteurs d'affectation, soit l'ensemble vide.
— $\vec{1}[k]$ désigne le vecteur défini par $\vec{1}[k]_k = 1$ et pour tout $i \neq k$, $\vec{1}[k]_i = 0$. On note aussi $\vec{1} = \sum_{k=1}^{n} \vec{1}[k]$ et pour $p \in \mathbb{Z}$, $\vec{p} = p\vec{1}$.
— $I\vec{n}v[k]$ désigne le vecteur défini par $I\vec{n}v[k]_k = -1$ et pour tout $i \neq k$, $I\vec{n}v[k]_i = 1$.

Question 6. Soit $n = 4$ et la clause $\varphi = x_1 \wedge \neg x_2$. Construisez un circuit $\mathcal{C}$ de sortie *out* dont les entrées sont $(1, -1, 0, 0)$, $\vec{1}[3]$, $-\vec{1}[3]$, $\vec{1}[4]$ et $-\vec{1}[4]$ tel que $E(out) = \mathbf{T}(\varphi)$.

Question 7. Généralisez la construction de la question précédente pour toute clause conjonctive φ et montrez que la taille du circuit construit est polynomiale par rapport à n.

Question 8. Soit φ une formule DNF composée de m clauses conjonctives. Utilisez la construction précédente pour construire un circuit $\mathcal{C}$ de sortie *out* tel que $E(out) = \mathbf{T}(\varphi)$ et dont la taille est polynomiale par rapport à $\max(m, n)$.

Soit la formule $\varphi \equiv Q_n x_n \dots Q_1 x_1 \psi$. On note $\varphi^i \equiv Q_i x_i \dots Q_1 x_1 \psi$. Ainsi $\varphi^0 \equiv \psi$ et $\varphi^n \equiv \varphi$. Un *k-vecteur d'affectation* est un vecteur $\vec{v} = 2^k \vec{w}$ avec $\vec{w}$ vecteur d'affectation ; ainsi un vecteur d'affectation est un 0-vecteur d'affectation. On note $\mathbf{Af}^k$ l'ensemble des k-vecteurs d'affectation et de manière similaire pour une formule φ, on définit $\mathbf{T}^k(\varphi) = \{\vec{v} \mid \exists \vec{w} \in \mathbf{T}(\varphi)\ \vec{v} = 2^k \vec{w}\}$. Un circuit $\mathcal{C}$ de sortie *out*, *k-représente* une formule θ si :

1. $\forall \vec{v} \in E(out)\ \forall i \leq n\ |v_i| \leq 2^k$
2. $\mathbf{T}^k(\theta) = E(out) \cap \mathbf{Af}^k$

Question 9. On suppose que $\varphi^{k+1} \equiv \exists x_{k+1}\ \varphi^k$ et qu'un circuit $\mathcal{C}'$ k-représente φ^k. Construisez à partir de $\mathcal{C}'$, un circuit $\mathcal{C}$ qui $(k+1)$-représente φ^{k+1}.

Question 10. On suppose que $\varphi^{k+1} \equiv \forall x_{k+1}\ \varphi^k$ et qu'un circuit $\mathcal{C}'$ k-représente φ^k. Construisez à partir de $\mathcal{C}'$, un circuit $\mathcal{C}$ qui $(k+1)$-représente φ^{k+1}. On vous demande de justifier la construction.

Question 11. Déduire des questions précédentes qu'il existe une réduction en temps polynomial de QBF-DNF vers VCE (et donc que VCE est PSPACE-difficile). On précisera le vecteur testé dans le problème VCE.

Exercice 3

Dans cette partie on transforme la réduction précédente en une réduction vers le problème du circuit entier noté ICE ce qui démontrera que le problème ICE est PSPACE-difficile et donc PSPACE-complet.

Question 12. Soit $\mathcal{C}$ le circuit vectoriel de la question 11. Supposons que chaque entrée vectorielle soit remplacée par un entier borné par $M \geq 2$ afin de fabriquer un circuit entier $\mathcal{C}'$ de sortie out'. Montrez que tout entier de $E(out')$ est borné par M^{2n+1}.

On admet les deux résultats suivants.

1. Soit p_k le $k$ième nombre premier alors pour k assez grand, $p_k < k^2$.
2. Soient $m_1, \ldots, m_n \in \mathbb{N}$ impairs et premiers entre eux et $M = \prod_{i=1}^{n} m_i$. On note $V = [(-m_1+1)/2, (m_1-1)/2] \times \ldots \times [(-m_n+1)/2, (m_n-1)/2]$. Alors il existe $z_1, \ldots, z_n \in \mathbb{Z}$ calculables en temps polynomial tels que :
   — $h : V \mapsto [0, \ldots, M-1]$ définie par : $h(x_1, \ldots, x_n) = \sum_{i=1}^{n} z_i x_i \mod M$ est bijective.
   — Pour tout $\vec{v}, \vec{w} \in V$, si $\vec{v} + \vec{w} \in V$ alors $h(\vec{v} + \vec{w}) = h(\vec{v}) + h(\vec{w}) \mod M$
   — Pour tout $\vec{v}, \vec{w} \in V$, si $\vec{v} \times \vec{w} \in V$ alors $h(\vec{v} \times \vec{w}) = h(\vec{v})h(\vec{w}) \mod M$
   On choisit pour définir h, $m_i = (p_{i+1})^{n+1}$.

Question 13. Montrez que la représentation binaire de M est de taille polynomiale par rapport à n.

Question 14. Soit $\mathcal{C}$ le circuit vectoriel de sortie out de la question 11. Supposons que chaque entrée vectorielle $\vec{v}$ soit remplacée par $h(\vec{v})$ ce qui nous donne un circuit entier $\mathcal{C}'$ de sortie out'. Soit $\vec{v}$ le vecteur associé au problème de la question 11. Montrez que $\vec{v} \in E(out)$ ssi $\exists x \in E(out')\ x \mod M = h(\vec{v})$.

Question 15. En ajoutant une entrée et une porte complétez le circuit $\mathcal{C}'$ en un circuit $\mathcal{C}''$ tel que $\vec{v} \in E(out)$ ssi $\exists x \in E(out'')\ x \mod M = 0$.

Question 16. En vous servant des questions 2 et 12, complétez le circuit $\mathcal{C}''$ en un circuit $\mathcal{C}^*$ de taille polynomiale vis à vis de la taille de $\mathcal{C}$ et de n tel que $\vec{v} \in E(out)$ ssi $M^{2n+2} \in E(out^*)$. Conclure.