b. En déduire que

$$\int_0^1 \left(F^{-1}(u) - G^{-1}(u)\right)^2 du \leq 8\, d_2(\mu,\nu). \tag{4}$$

22. Montrer que $(\mathcal{P}_2, d_2)$ est un espace métrique complet.

23. Pour (x,y) couple de réels, on note $\mathbb{1}_{x>y}$ la fonction valant 1 si $x > y$ et 0 sinon. Soit $\mathcal{K}$ une partie compacte de $(\mathcal{P}_2, d_2)$. Montrer que

$$\lim_{A\to+\infty} \sup_{\mu\in\mathcal{K}} \int_{\mathbf{R}} x^2 \mathbb{1}_{|x|>A} d\mu(x) = 0.$$

En déduire que, pour les sommes S_n définies dans la première partie,

$$\lim_{B\to+\infty} \sup_{n>0} n^{-1}\mathbb{E}(S_n^2 \mathbb{1}_{S_n^2>nB}) = 0.$$

24. Pour tout réel $A > 0$, on note $\mathcal{K}_A$ l'ensemble des lois μ telles que $\mu([-A,A]) = 1$.

a. Montrer que $\mathcal{K}_A$ est une partie compacte de $(\mathcal{P}_2, d_2)$.

b. En déduire un critère de compacité pour les parties fermées de $(\mathcal{P}_2, d_2)$.

MATHÉMATIQUES DE L'INFORMATIQUE

Les *réseaux de Petri* ont été introduits dans les années 60, comme modèles de la communication entre processus parallèles. La décidabilité du *problème de l'accessibilité* pour ces réseaux a été démontrée il y a une quinzaine d'années. On se contentera ici d'étudier certains cas particuliers qui jouent un rôle essentiel dans la preuve de décidabilité. De plus, on montrera qu'un problème plus général, à savoir l'*inclusion des ensembles d'accessibilité*, est indécidable.

Notations et conventions

On note $\mathbf{N}$ (respectivement $\mathbf{Z}$, $\mathbf{Q}$) l'ensemble des entiers naturels (respectivement des entiers relatifs, des nombres rationnels). Si X est un ensemble et $p \in \mathbf{N}$, on note X^p l'ensemble des p-uplets $(a_1,\ldots,a_p)$ où $a_1,\ldots,a_p \in X$. On munit $\mathbf{N}^p$ de l'ordre produit : $(a_1,\ldots,a_p) \leq (b_1,\ldots,b_p)$ si $a_i \leq b_i$ pour $i = 1,\ldots,p$. On note $0_p = (0,\ldots,0)$ le vecteur nul de $\mathbf{Z}^p$, et $e_1,\ldots,e_p$ les vecteurs de la base canonique de $\mathbf{Z}^p$. Enfin, si U et V sont des parties de $\mathbf{Z}^p$, on pose $U + V = \{u + v \mid u \in U, v \in V\}$.

Il n'est pas nécessaire de présenter les algorithmes comme des programmes. On se contentera de les décrire informellement.

I. Préliminaires

On cherche un algorithme pour déterminer si le système linéaire

$$n_1u_1 + \cdots + n_qu_q = v \tag{1}$$

admet une solution $(n_1,\ldots,n_q)$ dans $\mathbf{N}^q$, étant donnés des vecteurs $u_1,\ldots,u_q$, et v de $\mathbf{Z}^p$.

1. Pour chacun des systèmes suivants, existe-t-il une solution dans $\mathbb{N}^2$, dans $\mathbb{Q}^2$?

$$\begin{aligned} n_1(1,-1,1)+n_2(-2,4,1) &= (1,1,4), \\ n_1(1,-1,1)+n_2(-2,4,1) &= (1,1,2), \\ n_1(-2,1,-1)+n_2(4,-2,4) &= (-4,2,-1). \end{aligned}$$

2. Donner une condition nécessaire et suffisante sur a,b,c,a',b',c' pour que les vecteurs (a,b,c) et (a',b',c') soient linéairement dépendants. (Cette condition doit s'exprimer sous la forme d'un énoncé sans quantificateur.)

3. Soit M une matrice rectangulaire à p lignes et q colonnes, à coefficients dans $\mathbb{Z}$. A quelle condition les q colonnes de M sont-elles linéairement dépendantes?

4. Dans le cas où les vecteurs $u_1,\dots,u_q$ sont linéairement indépendants, donner un algorithme pour décider si le système (1) admet une solution dans $\mathbb{N}^q$? (On pourra commencer par le cas où $p=q$.)

Dans les trois questions suivantes, on suppose que les vecteurs $u_1,\dots,u_q$ sont linéairement dépendants. En particulier, $q \geq 1$.

5. Donner un algorithme pour calculer explicitement des entiers relatifs $m_1,\dots,m_q$ non tous nuls tels que

$$m_1u_1+\cdots+m_qu_q=0. \tag{2}$$

(On pourra remarquer que, dans le cas où les vecteurs $u_1,\dots,u_{q-1}$ sont linéairement indépendants, le système (2) admet une unique solution dans $\mathbb{Q}^q$ telle que $m_q=1$.)

Quitte à changer les signes, on peut supposer que $m_i>0$ pour au moins un i.

6. Montrer que si le système (1) admet une solution dans $\mathbb{N}^q$, alors il en existe une telle que $n_i<m_i$ pour au moins un i.

7. A partir des vecteurs $u_1,\dots,u_q$ et des entiers $m_1,\dots,m_q$, construire un nombre fini de systèmes à $q-1$ inconnues tels que le système (1) admet une solution dans $\mathbb{N}^q$ si et seulement si l'un au moins de ces systèmes admet une solution dans $\mathbb{N}^{q-1}$.

II. Trois notions d'accessibilité

On cherche à résoudre le problème suivant: étant donnés deux points x et y de $\mathbb{N}^p$, peut-on aller de x à y par une suite de déplacements d'un certain type? Le type des déplacements autorisés sera une partie finie D de $\mathbb{Z}^p$. Pour un tel D, on introduit trois notions d'accessibilité:

- y est *accessible* depuis x s'il existe une suite $u_1,\dots,u_n$ de vecteurs de D telle que $y=x+u_1+\cdots+u_n$, et tous les points intermédiaires $x+u_1+\cdots+u_i$ pour $i=1,\dots,n-1$ sont dans $\mathbb{N}^p$;
- y est *faiblement accessible* depuis x s'il existe un point $x' \geq x$ tel que y est accessible depuis x' ;
- y est *virtuellement accessible* depuis x s'il existe une suite $u_1,\dots,u_n$ de vecteurs de D telle que $y=x+u_1+\cdots+u_n$, sans condition sur les points intermédiaires.

Bien entendu, la suite de déplacements peut être vide : en particulier, un point est toujours accessible depuis lui-même. Le *problème de l'accessibilité* (respectivement *de l'accessibilité faible, de l'accessibilité virtuelle*) est le suivant : D, x, y étant donnés, y est-il accessible (respectivement faiblement accessible, virtuellement accessible) depuis x ?

1. Le problème de l'accessibilité virtuelle est-il décidable ?

On note $\mathcal{A}(x,D)$ (respectivement $\mathcal{A}_f(x,D)$, $\mathcal{A}_v(x,D)$) l'ensemble des points $y \in \mathbf{N}^p$ qui sont accessibles (respectivement faiblement accessibles, virtuellement accessibles) depuis x.

2. Calculer $\mathcal{A}(x,D)$, $\mathcal{A}_f(x,D)$ et $\mathcal{A}_v(x,D)$ pour $x = (1,0)$ et $D = \{(1,-1),(-2,2)\}$.

3. En général, quelles inclusions a-t-on, et n'a-t-on pas, entre les ensembles $\mathcal{A}(x,D)$, $\mathcal{A}_f(x,D)$, et $\mathcal{A}_v(x,D)$? (On donnera un contre-exemple pour chaque réponse négative.)

4. Même question quand on se limite à la dimension $p = 1$.

On va maintenant montrer que le problème de l'accessibilité faible et celui de l'accessibilité virtuelle se ramènent au problème de l'accessibilité. On se donne une partie finie D de $\mathbf{Z}^p$, et on note $\mathcal{A}(D)$ (respectivement $\mathcal{A}_f(D)$, $\mathcal{A}_v(D)$) l'ensemble des couples $(x,y) \in \mathbf{N}^p \times \mathbf{N}^p$ tels que y est accessible (respectivement faiblement accessible, virtuellement accessible) depuis x.

5. Construire une partie finie D_f de $\mathbf{Z}^p$ telle que $\mathcal{A}_f(D) = \mathcal{A}(D_f)$. (Aucune justification n'est demandée.)

6. Construire une partie finie D_v de $\mathbf{Z}^{p+1}$ telle que

$$\mathcal{A}_v(D) = \{(x,y) \in \mathbf{N}^p \times \mathbf{N}^p \mid (\iota(x),\iota(y)) \in \mathcal{A}(D_v)\}$$

où $\iota(a_1,\ldots,a_p) = (a_1,\ldots,a_p,0)$. (Aucune justification n'est demandée.)

III. Problème de l'accessibilité faible

Un *idéal additif* de $\mathbf{N}^p$ est une partie X de $\mathbf{N}^p$ telle que $X + \mathbf{N}^p = X$. Autrement dit, si $x \in X$ et $x' \geq x$, alors $x' \in X$. Par exemple, si x est un point de $\mathbf{N}^p$, l'ensemble $\overline{x} = \{x' \in \mathbf{N}^p \mid x' \geq x\}$ est le plus petit idéal additif contenant x. Un tel idéal additif est dit *principal*.

1. Quels sont les idéaux additifs de $\mathbf{N}$?

Pour $i = 1,\ldots,p$ et $n \in \mathbf{N}$, on note H_n^i l'ensemble des points de $\mathbf{N}^p$ dont la i-ème coordonnée vaut n.

2. Si x est un point de $\mathbf{N}^p$, exprimer le complémentaire de $\overline{x}$ dans $\mathbf{N}^p$ sous la forme d'une union finie de H_n^i.

3. Montrer que si X est une partie de $\mathbf{N}^p$, l'ensemble $\underline{X}$ de ses points minimaux est fini.

4. Montrer que tout idéal additif de $\mathbf{N}^p$ est une union finie d'idéaux additifs principaux.

On se donne $x \in \mathbf{N}^p$ et une partie finie D de $\mathbf{Z}^p$. On suppose que D contient le vecteur nul 0_p. Sinon, on peut toujours le rajouter sans changer les différentes notions d'accessibilité. Si X est une partie de $\mathbf{N}^p$, on pose $\Phi(X) = (X + D) \cap \mathbf{N}^p$. Par définition, on a

$$\mathcal{A}_f(x,D) = \bigcup_{n \in \mathbf{N}} X_n, \text{ où } X_n = \Phi^n(\overline{x}).$$

5. Montrer que la suite des X_n est stationnaire.

6. Expliciter les $\underline{X_n}$ dans le cas où $x = (1,1)$ et $D = \{(0,0),(1,-1),(-2,2)\}$.

7. Exprimer $\underline{X_{n+1}}$ directement en fonction de $\underline{X_n}$.

8. Comment décide-t-on si un point y est faiblement accessible depuis x?

IV. Chemins dans un graphe orienté

Si X est un ensemble, on note $\mathbf{Z}X$ le $\mathbf{Z}$-module libre engendré par X, c'est-à-dire l'ensemble des combinaisons linéaires formelles $u = \sum_{\xi\in X} a_\xi[\xi]$, où les a_ξ sont des entiers relatifs presque tous nuls, et les $[\xi]$ sont des générateurs associés aux éléments de X. On note $\mathbf{N}X$ l'ensemble des u pour lesquels les a_ξ sont des entiers naturels, et dans ce cas, on pose $||u|| = \sum_{\xi\in X} a_\xi$.

Un *graphe orienté* G est défini par un ensemble S de *sommets*, un ensemble A d'*arêtes*, et la donnée, pour chaque arête α, de deux sommets respectivement appelés *source* et *but* de α. On écrit $\sigma \xrightarrow{\alpha} \tau$ si α est une arête de source σ et de but τ. On permet que la source et le but d'une même arête soient identiques (*arête fermée*). On permet aussi que deux arêtes distinctes aient même source et même but.

Un *sous-graphe* de G est défini par une partie S' de S, et une partie A' de A telle que, si $\sigma \xrightarrow{\alpha} \tau$ est dans A', alors σ et τ sont dans S'. On dit que G est *connexe* s'il est non vide, et s'il ne peut être décomposé en deux sous-graphes non vides disjoints.

Un *chemin* $\sigma \xrightarrow{\gamma} \tau$ dans G est une suite $\sigma = \sigma_0 \xrightarrow{\alpha_1} \sigma_1 \xrightarrow{\alpha_2} \cdots \xrightarrow{\alpha_n} \sigma_n = \tau$. On pose alors $[\gamma] = [\alpha_1] + \cdots + [\alpha_n] \in \mathbf{N}A$. En particulier, on a un *chemin vide* $\sigma \xrightarrow{\varepsilon_\sigma} \sigma$ pour chaque sommet σ de G, et $[\varepsilon_\sigma] = 0$.

1. Montrer que l'application $\gamma \mapsto [\gamma]$ n'est pas nécessairement injective, même si on la restreint à l'ensemble des chemins non vides.

On définit une application $\mathbf{Z}$-linéaire $\partial : \mathbf{Z}A \to \mathbf{Z}S$ en posant $\partial[\alpha] = [\tau] - [\sigma]$ pour tout $\sigma \xrightarrow{\alpha} \tau$. Il est clair que $\partial[\gamma] = [\tau] - [\sigma]$ pour tout chemin $\sigma \xrightarrow{\gamma} \tau$. On se donne maintenant deux sommets σ et τ de G, non nécessairement distincts.

2. Montrer que, si $u \in \mathbf{N}A$ est tel que $\partial u = [\tau] - [\sigma]$, il n'existe pas nécessairement de chemin $\sigma \xrightarrow{\gamma} \tau$ tel que $u = [\gamma]$.

3. Montrer que, sous les hypothèses de la question précédente, il existe un chemin $\sigma \xrightarrow{\gamma} \tau$ et $v \in \mathbf{N}A$ tels que $u = [\gamma] + v$. (On pourra raisonner par récurrence sur $||u||$.)

Etant donné $u = \sum_{\alpha\in A} a_\alpha[\alpha] \in \mathbf{N}A$, on définit le sous-graphe G_u de G dont les arêtes sont les α tels que $a_\alpha \neq 0$, et les sommets sont les sources et les buts de ces arêtes. Il est clair que, si $u = [\gamma]$ où γ est un chemin non vide, alors G_u est connexe.

4. Montrer que, si $u \in \mathbf{N}A$ est tel que σ est un sommet de G_u et $\partial u = 0$, alors il existe un chemin fermé non vide $\sigma \xrightarrow{\gamma} \sigma$ et $v \in \mathbf{N}A$ tels que $u = [\gamma] + v$.

5. Montrer que, si $u \in \mathbf{N}A$ est tel que G_u est connexe, σ est un sommet de G_u, et $\partial u = [\tau] - [\sigma]$, alors il existe un chemin $\sigma \xrightarrow{\gamma} \tau$ tel que $u = [\gamma]$.

V. Problèmes d'accessibilité pour un graphe

On suppose que G est un graphe orienté fini, c'est-à-dire que l'ensemble S des sommets et l'ensemble A des arêtes sont finis. On pourra donc identifier $\mathbf{N}S$ (respectivement $\mathbf{Z}S$, $\mathbf{N}A$, $\mathbf{Z}A$) avec $\mathbf{N}^s$ (respectivement $\mathbf{Z}^s$, $\mathbf{N}^q$, $\mathbf{Z}^q$) où s est le nombre de sommets et q le nombre d'arêtes.

1. Construire une partie finie D de $\mathbf{Z}S$ telle que $([\sigma],[\tau]) \in \mathcal{A}(D)$ si et seulement s'il existe un chemin $\sigma \xrightarrow{\gamma} \tau$. (Aucune justification n'est demandée.)

On se donne une application $\alpha \mapsto \Delta\alpha$, de A vers $\mathbf{Z}^p$, et on généralise les notions d'accessibilité de la partie II, en considérant cette fois des couples (σ, x) et (τ, y) dans $S \times \mathbf{N}^p$:

- (τ, y) est *accessible* depuis (σ, x) s'il existe un chemin

$$\sigma = \sigma_0 \xrightarrow{\alpha_1} \sigma_1 \xrightarrow{\alpha_2} \cdots \xrightarrow{\alpha_n} \sigma_n = \tau$$

  tel que $y = x + \Delta\alpha_1 + \cdots + \Delta\alpha_n$, et tous les points intermédiaires $x + \Delta\alpha_1 + \cdots + \Delta\alpha_i$ pour $i = 1, \ldots, n-1$ sont dans $\mathbf{N}^p$;

- (τ, y) est *faiblement accessible* depuis (σ, x) s'il existe un point $x' \geq x$ tel que (τ, y) est accessible depuis (σ, x') ;

- (τ, y) est *virtuellement accessible* depuis (σ, x) s'il existe un chemin

$$\sigma = \sigma_0 \xrightarrow{\alpha_1} \sigma_1 \xrightarrow{\alpha_2} \cdots \xrightarrow{\alpha_n} \sigma_n = \tau$$

  tel que $y = x + \Delta\alpha_1 + \cdots + \Delta\alpha_n$, sans condition sur les points intermédiaires.

Dans le cas où le graphe G n'a qu'un seul sommet, on retrouve les notions de la partie II en posant $D = \{\Delta\alpha \mid \alpha \in A\}$. Le *problème de l'accessibilité* (respectivement *de l'accessibilité faible*, *de l'accessibilité virtuelle*) pour G est le suivant : Δ, (σ, x), (τ, y) étant donnés, (τ, y) est-il accessible (respectivement faiblement accessible, virtuellement accessible) depuis (σ, x) ?

2. Montrer que, si G est sans arête fermée, le problème de l'accessibilité pour G en dimension p se ramène au problème de l'accessibilité (celui qui est défini dans la partie II) en dimension $s + p$.

3. Montrer que le problème de l'accessibilité pour G se ramène au problème de l'accessibilité pour un G' sans arête fermée.

4. Montrer que le problème de l'accessibilité faible pour G est décidable.

On note Δ l'application $\mathbf{Z}$-linéaire de $\mathbf{Z}A$ vers $\mathbf{Z}^p$ définie par $\Delta[\alpha] = \Delta\alpha$.

5. Exprimer l'accessibilité virtuelle pour G en termes de vecteurs de $\mathbf{N}A$ plutôt qu'en termes de chemins.

6. Montrer que le problème de l'accessibilité virtuelle pour G est décidable.

VI. Simulation du calcul d'un polynôme

On appelle *automate à p registres* un graphe orienté fini G, muni d'une application $\alpha \mapsto \Delta\alpha$ de l'ensemble des arêtes de G vers $\mathbb{Z}^p$, de deux sommets non nécessairement distincts σ (l'*état initial*) et τ (l'*état final*), et de deux suites $i_1, \ldots, i_k$ (les *registres d'entrée*) et $j_1, \ldots, j_\ell$ (les *registres de sortie*) dans $\{1, \ldots, p\}$. La suite $i_1, \ldots, i_k$ n'est pas nécessairement croissante, mais elle doit être sans répétition. Il en va de même pour la suite $j_1, \ldots, j_\ell$.

La figure 1 représente des automates à registres. Chaque arête α est étiquetée par $\Delta\alpha$, sauf quand $\Delta\alpha = 0_p$, auquel cas on ne le mentionne pas. L'état initial est indiqué par une flèche entrante, et l'état final par une flèche sortante.

Pour un tel automate, on considère l'injection $\iota : \mathbf{N}^k \to \mathbf{N}^p$ qui à $(a_1, \ldots, a_k)$ associe $(b_1, \ldots, b_p)$ où $b_{i_1} = a_1, \ldots, b_{i_k} = a_k$, et $b_i = 0$ si i n'est pas un registre d'entrée, ainsi que la projection $\pi : \mathbf{N}^p \to \mathbf{N}^\ell$ qui à $(a_1, \ldots, a_p)$ associe $(a_{j_1}, \ldots, a_{j_\ell})$. On dit que l'automate *réalise* l'application $f : \mathbf{N}^k \to \mathbf{N}^\ell$ si les deux conditions suivantes sont vérifiées :

i) pour tout $x \in \mathbf{N}^k$, il existe $y \in \mathbf{N}^p$ tel que (τ, y) est accessible depuis $(\sigma, \iota(x))$ et $\pi(y) = f(x)$;

ii) pour tout $x \in \mathbf{N}^k$ et pour tout $y \in \mathbf{N}^p$ tel que (τ, y) est accessible depuis $(\sigma, \iota(x))$, on a $\pi(y) \leq f(x)$.

Si un tel automate existe, on dit que l'application f est *réalisable*.

1. Quelles applications sont réalisées par les 5 automates de la figure 1 ? (Aucune justification n'est demandée.)

2. Montrer que toute application réalisable est croissante.

3. Construire un automate réalisant l'application $\delta_k : \mathbf{N}^k \to \mathbf{N}^{2k}$ qui à $(a_1, \ldots, a_k)$ associe $(a_1, \ldots, a_k, a_1, \ldots, a_k)$.

4. Etant donné un automate réalisant l'application $f : \mathbf{N}^k \to \mathbf{N}^\ell$, construire un automate réalisant l'application $f \times \mathbf{N}^m : \mathbf{N}^{k+m} \to \mathbf{N}^{\ell+m}$ qui à $(a_1, \ldots, a_{k+m})$ associe $(b_1, \ldots, b_\ell, a_{k+1}, \ldots, a_{k+m})$ où $(b_1, \ldots, b_\ell) = f(a_1, \ldots, a_k)$.

5. Etant donnés deux automates réalisant les applications $f : \mathbf{N}^k \to \mathbf{N}^\ell$ et $g : \mathbf{N}^\ell \to \mathbf{N}^m$, construire un automate réalisant l'application $g \circ f : \mathbf{N}^k \to \mathbf{N}^m$.

6. Montrer que si les applications $f : \mathbf{N}^k \to \mathbf{N}$ et $g : \mathbf{N}^k \to \mathbf{N}$ sont réalisables, alors les applications $f + g$ et fg le sont aussi.

7. Montrer que pour tout polynôme P à k indéterminées, à coefficients dans $\mathbf{N}$, l'application $(a_1, \ldots, a_k) \mapsto P(a_1, \ldots, a_k)$ est réalisable.

VII. Un problème indécidable

Pour toute application $f : \mathbf{N}^k \to \mathbf{N}$, on pose

$$\Gamma(f) = \{(a_1, \ldots, a_k, b) \in \mathbf{N}^{k+1} \mid b \leq f(a_1, \ldots, a_k)\}.$$

On considère les problèmes suivants :

($\mathcal{P}1$) Etant donné un polynôme P à k indéterminées, à coefficients dans $\mathbb{Z}$, existe-t-il $(a_1, \ldots, a_k) \in \mathbf{N}^k$ tel que $P(a_1, \ldots, a_k) = 0$?

($\mathcal{P}2$) Etant donnés deux polynômes P et Q à k indéterminées, à coefficients dans $\mathbf{N}$, existe-t-il $(a_1, \ldots, a_k) \in \mathbf{N}^k$ tel que $P(a_1, \ldots, a_k) \leq Q(a_1, \ldots, a_k)$?

($\mathcal{P}3$) Etant donnés deux polynômes P et Q à k indéterminées, à coefficients dans $\mathbf{N}$, a-t-on $\Gamma(Q) \subset \Gamma(P)$?

($\mathcal{P}4$) Etant donnés $x, y \in \mathbf{N}^p$ et des parties finies D, E de $\mathbb{Z}^p$, a-t-on $\mathcal{A}(y, E) \subset \mathcal{A}(x, D)$?

On admet que ($\mathcal{P}1$) est indécidable (théorème de Matijasevič).

1. Montrer que ($\mathcal{P}2$) et ($\mathcal{P}3$) sont indécidables.

Si $k \leq p$, on note $\pi_p^k : \mathbf{N}^p \to \mathbf{N}^k$ la projection qui à $(a_1, \ldots, a_p)$ associe $(a_1, \ldots, a_k)$. On dit qu'un automate à p registres, sans registre d'entrée, et dont les registres de sortie sont $1, \ldots, k$, *réalise* la partie X de $\mathbf{N}^k$ si les deux conditions suivantes sont vérifiées :

iii) pour tout $x \in X$, il existe $y \in \mathbf{N}^p$ tel que (τ, y) est accessible depuis $(\sigma, 0_p)$ et $\pi_p^k(y) = x$;

iv) pour tout sommet σ' et pour tout $y \in \mathbf{N}^p$ tel que (σ', y) est accessible depuis $(\sigma, 0_p)$, on a $\pi_p^k(y) \in X$.

Si un tel automate existe, on dit que la partie X est *réalisable*.

2. Etant donné un automate à p registres réalisant l'application $f : \mathbf{N}^k \to \mathbf{N}$, construire un automate à $k + 1 + p$ registres réalisant la partie $\Gamma(f)$.

3. Montrer que pour toute partie réalisable X de $\mathbf{N}^k$, il existe $p \geq k$, $x \in \mathbf{N}^p$ et une partie finie D de $\mathbb{Z}^p$ tels que $\pi_p^k(\mathcal{A}(x, D)) = X$.

On se donne maintenant $x \in \mathbf{N}^p$ et une partie finie D de $\mathbb{Z}^p$ tels que $\pi_p^k(\mathcal{A}(x, D)) = X$. Si $u = (a_1, \ldots, a_p) \in \mathbb{Z}^p$ et $a_{p+1}, \ldots, a_{p+4} \in \mathbb{Z}$, on note $(u, a_{p+1}, \ldots, a_{p+4})$ le vecteur $(a_1, \ldots, a_{p+4}) \in \mathbb{Z}^{p+4}$. On pose $x^\sharp = (x, 1, 0, 0, 0)$ et

$$\begin{aligned} D^\sharp = {} & \{(u, -1, 1, 0, 0) \mid u \in D\} \cup \{(\pm e_i, 0, 0, -1, 1) \mid k + 1 \leq i \leq p\} \cup \\ & \{(0_p, 1, -1, 0, 0), (0_p, -1, 0, 1, 0), (0_p, 0, 0, 1, -1), (0_p, 0, 0, -1, 0)\}. \end{aligned}$$

4. Calculer $\mathcal{A}(x^\sharp, D^\sharp) \cap \{(y, 0, 0, 0, 0) \mid y \in \mathbf{N}^p\}$.

5. Montrer que ($\mathcal{P}4$) est indécidable.

En fait, on n'a pas vraiment besoin du théorème de Matijasevič. On peut utiliser un résultat plus ancien dû à Davis, Putnam et Robinson. Il faut alors étendre la classe des polynômes en ajoutant l'exponentiation.

6. Montrer que l'application $a \mapsto 2^a$ est réalisable.

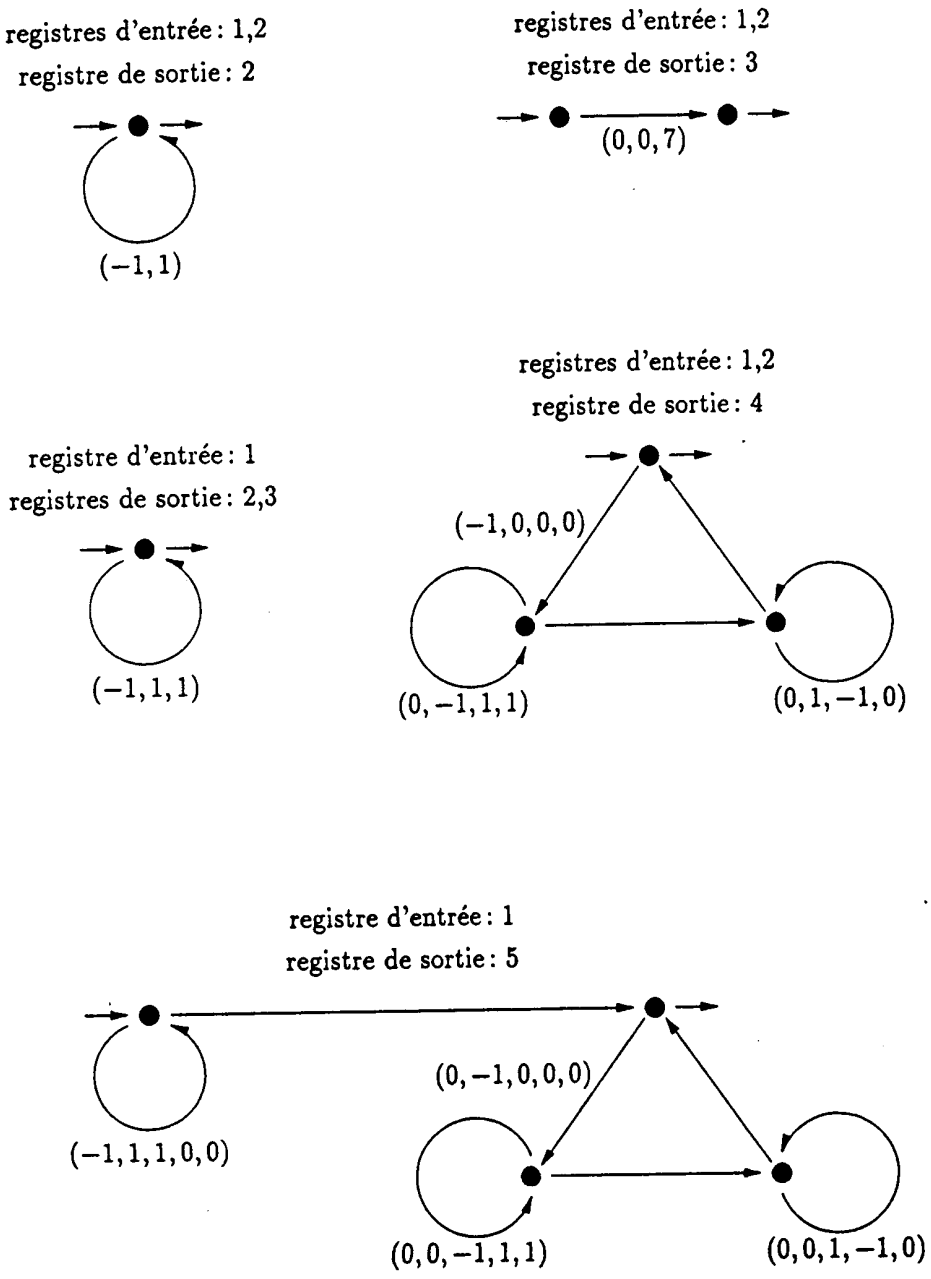
registres d'entrée : 1,2
registre de sortie : 2
(−1, 1)
registres d'entrée : 1,2
registre de sortie : 3
(0, 0, 7)
registre d'entrée : 1
registres de sortie : 2,3
(−1, 1, 1)
registres d'entrée : 1,2
registre de sortie : 4
(−1, 0, 0, 0)
(0, −1, 1, 1)
(0, 1, −1, 0)
registre d'entrée : 1
registre de sortie : 5
(−1, 1, 1, 0, 0)
(0, −1, 0, 0, 0)
(0, 0, −1, 1, 1)
(0, 0, 1, −1, 0)

Figure 1