ENSEIRB-MATMECA- Section Informatique, 2ième année
Calculabilité, 2021/2022

CALCULABILITÉ

DM- à rendre avant le xx/04/2022, à yy heure.

Sujet : Ce devoir est centré sur les équations (et inéquations) linéaires en nombres entiers. La partie I introduit le problème à résoudre. La partie II propose une méthode de résolution fondée sur l'*algèbre linéaire* sur le corps des nombres rationnels. La partie III propose une méthode fondée sur la théorie des *automates finis* sur le monoide libre $\{0,1\}^*$. La partie IV propose une méthode fondée sur la structure bel-ordonnée de $\mathbb{N}^n$ et les *parties linéaires* de $\mathbb{N}^n$.
Indications : On peut *admettre* une question (voire même toute une partie) et utiliser les résultats de cette question (ou partie) dans la suite du problème.
La partie IV utilise la partie III. Les parties II et III utilisent la partie I.
Tous moyens d'investigation autorisés.
Rédaction finale par groupes de quatre.

Partie I

Équations et inéquations en nombres entiers.

Le problème de la satisfaisabilité d'un système d'*équations* en nombres entiers naturels, que nous nommerons (EQNAT), est le suivant :

- **Instance :** Des entiers $m \geq 1, n \geq 1$, des matrices $A \in \mathbb{M}_{m,n}(\mathbb{Z})$, $\overrightarrow{b} \in \mathbb{M}_{m,1}(\mathbb{Z})$
- **Question :** Existe-t-il un vecteur d'entiers naturels $\overrightarrow{x} \in \mathbb{M}_{n,1}(\mathbb{N})$ tel que
$$A \cdot \overrightarrow{x} = \overrightarrow{b}$$

Le problème de la satisfaisabilité d'un système d'*inéquations* en nombres entiers naturels, que nous nommerons (INEQNAT), est le suivant :

- **Instance :** Des entiers $m \geq 1, n \geq 1$, des matrices $A \in \mathbb{M}_{m,n}(\mathbb{Z})$, $\overrightarrow{b} \in \mathbb{M}_{m,1}(\mathbb{Z})$
- **Question :** Existe-t-il un vecteur d'entiers naturels $\overrightarrow{x} \in \mathbb{M}_{n,1}(\mathbb{N})$ tel que
$$A \cdot \overrightarrow{x} \geq \overrightarrow{b}$$

(où l'ordre $\geq$ est l'ordre coordonnée par coordonnée sur les vecteurs).
Le problème de la résolution d'un système d'inéquations en nombres entiers relatifs, que nous nommerons (INEQREL), a les mêmes instances que (INEQNAT), mais pose la question : Existe-t-il un vecteur d'entiers *relatifs* $\overrightarrow{x} \in \mathbb{M}_{n,1}(\mathbb{Z})$ tel que

$$A \cdot \overrightarrow{x} \geq \overrightarrow{b}$$

Dans ces trois problèmes, on utilise les notations :

$$\begin{array}{rcl} A & = & (a_{i,j})_{1\leq i\leq m, 1\leq j\leq n}, \;\; a_i = (a_{i,1}, \cdots, a_{i,j}, \cdots, a_{i,n}), \\ \overrightarrow{b} & = & {}^t(b_1, \cdots, b_i, \cdots, b_m) \;\; [\,\overrightarrow{b} \text{ est un vecteur-colonne}] \\ \|A\|_\infty & := & \max\{|a_{i,j}||1 \leq i \leq m, 1 \leq j \leq n\}, \;\; \|\overrightarrow{b}\|_\infty := \max\{|b_i||1 \leq i \leq m\}, \\ \alpha & := & \max\{\|A\|_\infty, \|\overrightarrow{b}\|_\infty\}; \;\; q := \max\{m, n\} \\ \tau(A, \overrightarrow{b}) & := & (m \cdot n) + \log_2(\alpha). \end{array}$$

La *taille* de la donnée est le nombre $\tau(A, \overrightarrow{b})$.
1- Montrer que (EQNAT) $\leq_p$ (INEQNAT)
2- Montrer que (INEQNAT) $\leq_p$ (INEQREL)
3- Montrer que (INEQREL) $\leq_p$ (EQNAT)
4- Montrer que ces trois problèmes sont NP-difficiles.
Indication : on pourra montrer que (3SAT)$\leq_p$(INEQNAT). Les booléens True (False) pourront être codés par les nombres $0, 1$.

Fixons pour tout ce qui suit une instance de ces problèmes [1] :

$$m \geq 1, n \geq 1, A \in \mathbb{M}_{m,n}(\mathbb{Z}), \overrightarrow{b} \in \mathbb{M}_{m,1}(\mathbb{Z}) \qquad (1)$$

Partie II

Algèbre linéaire.

1- Soit B un matrice carrée extraite de A. Montrer que

$$|\det(B)| \leq (\alpha \cdot q)^q$$

2- Montrer que, si $rg(A) < n$, alors il existe $\overrightarrow{z} \in \mathbb{M}_{n,1}(\mathbb{Z})$ vérifiant :

$$\overrightarrow{z} \neq \overrightarrow{0}, \;\; A \cdot \overrightarrow{z} = \overrightarrow{0} \;\; \text{et} \;\; \|\overrightarrow{z}\|_\infty \leq (\alpha \cdot q)^{2q}$$

3- On suppose que l'instance (1) de (INEQREL) a une solution. Montrer qu'il existe $\overrightarrow{x} \in \mathbb{M}_{n,1}(\mathbb{Z})$ tel que :

$$A \cdot \overrightarrow{x} \geq \overrightarrow{b}, \;\; \exists i \in [1, m], \;\; b_i \leq a_i \cdot \overrightarrow{x} \leq b_i + \alpha$$

1. On remarquera que les 3 problèmes envisagés ont le même ensemble d'instances ; ils ne différent que par la *question* posée

4- On suppose que l'instance (1) de (INEQREL) a une solution et que $rg(A) = n$. Montrer qu'il existe $\overrightarrow{x} \in \mathbb{M}_{n,1}(\mathbb{Z})$ tel que :

$$A \cdot \overrightarrow{x} \geq \overrightarrow{b}, \ \ \forall i \in [1, m], \ \ b_i \leq a_i \cdot \overrightarrow{x} \leq b_i + (\alpha q)^{2q+1}$$

5- On suppose que l'instance (1) de (INEQREL) a une solution. Montrer qu'il existe $\overrightarrow{x} \in \mathbb{M}_{n,1}(\mathbb{Z})$ tel que :

$$A \cdot \overrightarrow{x} \geq \overrightarrow{b}, \ \ \|\overrightarrow{x}\|_\infty \leq (2\alpha \cdot q)^{3q+2}$$

Indication : traiter le cas où $rg(A) = n$; puis se ramener à ce cas en remarquant que l'on peut ajouter n inequations à coefficients dans $\{0, -1, 1\}$ qui sont satisfaites par le vecteur $\overrightarrow{x}$.
6- Montrer que le problème (INEQREL) est dans la classe de complexité NP. Que peut-on conclure concernant la complexité des problèmes (EQNAT),(INEQNAT),(INEQREL) ?

Partie III

Nombres entiers et automates.

On considère ici la représentation des entiers naturels par des mots, basée sur le système de numération binaire. On montre que l'ensemble des représentations des solutions d'un système d'inéquations en nombres entiers est reconnu par un automate fini.
Soit $\Sigma = \{0, 1\}$. On note $\nu : \Sigma^* \to \mathbb{N}$ la valeur d'un mot binaire :

$$\nu(w) = \sum_{j=0}^{\ell-1} w[j] \cdot k^j$$

où $\ell = |w|$ et $w = w[\ell - 1] \cdots w[0]$.
Plus généralement, pour tout entier $m \geq 1$, on définit la valeur d'un mot sur l'alphabet produit Σ^m comme le m-uple d'entiers suivant :

$$\nu : (\Sigma^m)^* \to \mathbb{N}^m$$

$$w = (w_1, \ldots, w_m) \mapsto (\nu(w_1), \ldots, \nu(w_m))$$

ici w_i est la suite des i-ièmes composantes des lettres de w. Par exemple, si $m = 3$ et si $w = [0, 1, 0][0, 0, 1], [1, 1, 0], [0, 0, 1]$ on note $w_1 = 0010, w_2 = 1010, w_3 = 0101$ et

$$\nu(w) = (\nu(w_1), \nu(w_2), \nu(w_3)) = (2, 10, 5).$$

Soit $R \subseteq \mathbb{N}^m$.
1- Montrer que $\nu^{-1}(R)$ est un langage rationnel de $(\Sigma^m)^*$ ssi il existe un langage rationnel $L \subseteq (\Sigma^m)^*$ tel que $\nu(L) = R$.
Indication : on remarquera que l'ajout ou retrait de la lettre $[0, 0, ..., 0]$ à l'extrémité gauche d'un mot ne change pas sa valeur.

Lorsque les conditions de la question 1 sont vérifiées et $m \geq 2$ (resp. $m = 1$), nous dirons que R est une *relation 2-automatique* (resp. une *partie 2-automatique*).

2- Montrer que les parties (et relations) suivantes sont 2-automatiques :

$$P_1 = \{n \in \mathbb{N} \mid n \equiv 1 \pmod 3\}, \quad \text{INF} = \{(n, p) \in \mathbb{N}^2 \mid n \leq p\}, \quad \text{ADD} = \{(n, p, q) \in \mathbb{N}^3 \mid n+p = q\}.$$

On pourra donner, pour chaque relation, un automate fini, lisant les mots de droite à gauche, et reconnaissant l'image réciproque par ν de la relation.
Soit I une partie de $[1, m]$ dont les éléments sont $i_1 < i_2 < \ldots < i_k$ (k est le cardinal de I). La projection $\pi_I : \mathbb{N}^m \to \mathbb{N}^k$ est définie par :

$$\pi_I(u_1, \ldots, u_i, \ldots, u_m) := (u_{i_1}, u_{i_2}, \ldots, u_{i_k}).$$

On l'étend aux relations en posant, pour tout $R \subseteq \mathbb{N}^m$, $\pi_I(R) := \{\pi_I(\overrightarrow{u}) \mid \overrightarrow{u} \in R\}$.
Soit $\sigma : [1, m] \to [1, m]$ une permutation des entiers de 1 à m. On note $S(\sigma) : \mathbb{N}^m \to \mathbb{N}^m$ la permutation des composantes des vecteurs :

$$S(\sigma)(\overrightarrow{u}) := (u_{\sigma(1)}, \ldots, u_{\sigma(i)}, \ldots, u_{\sigma(m)}),$$

que l'on étend naturellement aux relations.

3- Montrer que l'ensemble des relations 2-automatiques est clos par les opérations suivantes : union, intersection, complémentaire, projection, permutation des composantes.
4- Étant donnés $m \geq 1$, des entiers $m_1, m_2, m_3 \geq 1$ tels que $m_1 + m_2 + m_3 = m$ et des relations R, R' d'arités respectives $m_1 + m_2, m_2 + m_3$, on définit la *jointure* simple de ces relations par :

$$J(R, R') := \{\overrightarrow{u} \in \mathbb{N}^m \mid \pi_{[1,m_1+m_2]}(\overrightarrow{u}) \in R, \pi_{[m_1+1,m]}(\overrightarrow{u}) \in R'\}.$$

Montrer que si R, R' sont 2-automatiques, alors leur jointure simple est 2-automatique.

6- Montrer que si $R \subseteq \mathbb{N}^{m_1} \times \mathbb{N}^{m_2}$ et $R' \subseteq \mathbb{N}^{m_2} \times \mathbb{N}^{m_3}$ sont 2-automatiques, alors leur composée

$$R' \circ R := \{(\overrightarrow{x}, \overrightarrow{z}) \in \mathbb{N}^{m_1} \times \mathbb{N}^{m_3} \mid \exists \overrightarrow{y} \in \mathbb{N}^{m_2}, (\overrightarrow{x}, \overrightarrow{y}) \in R, (\overrightarrow{y}, \overrightarrow{z}) \in R'\}$$

est 2-automatique.
7- Étant donnés $m, p \geq 1, I_1, I_2, \ldots I_p \subseteq [1, m]$ et des relations $R_1, R_2, \ldots, R_p$ d'arités respectives $\#(I_1), \#(I_2), \ldots \#(I_p)$
la *jointure* de ces relations sur les ensembles d'indices I_j est :

$$J_{m,I_1,I_2,\ldots,I_p}(R_1, R_2, \ldots, R_p) := \{\overrightarrow{u} \in \mathbb{N}^m \mid \forall j \in [1, p], \pi_{I_j}(\overrightarrow{u}) \in R_j\}$$

Montrer que si $R_1, R_2, \ldots, R_p$ sont 2-automatiques, alors leur jointure est 2-automatique.
Indication : on pourra traiter le cas $p = 1$ (l'opération s'appelle alors la *cylindrification*) ; puis en déduire le cas $p \geq 2$ en utilisant la question 3.
8- Soit $A \in \mathbb{M}_{m,n}(\mathbb{N})$, $\overrightarrow{b} \in \mathbb{M}_{m,1}(\mathbb{N})$. Montrer que $\{\overrightarrow{x} \in \mathbb{N}^n \mid A \cdot \overrightarrow{x} = \overrightarrow{b}\}$ est 2-automatique.

Soit $\mathcal{S} \subseteq \mathbb{N}^n$ l'*ensemble* des solutions au problème (EQNAT) sur l'instance (1) :

$$\mathcal{S} := \{\overrightarrow{x} \in \mathbb{M}_{n,1}(\mathbb{N}) \mid A \cdot \overrightarrow{x} = \overrightarrow{b}\}. \tag{2}$$

9- 9.1 Montrer que $\mathcal{S}$ est 2-automatique.
9.2 Expliquer comment on peut *construire* un automate fini reconnaissant les représentations des solutions de (1).

Partie IV

Parties linéaires de $\mathbb{N}^n$.

Soit E un ensemble et $\preceq$ une relation d'ordre sur E. On note $\prec$ la relation : $x \prec y \Leftrightarrow (x \preceq y$ et $x \neq y)$. On rappelle que l'ordre $\preceq$ est *bien-fondé* ssi, il n'existe pas de suite $(e_n)_{n \geq 0}$ telle que $\forall n, e_{n+1} \prec e_n$.
1- Montrer que les conditions suivantes sur l'ordre $\preceq$ sont équivalentes :

(i) toute partie non-vide de E a un nombre fini, non-nul, d'éléments minimaux

(ii) $\preceq$ est bien-fondé et, pour toute partie infinie P de E, il existe $x, y \in P$ tels que $x \prec y$

(iii) pour toute suite $(e_n)_{n \geq 0}$ d'éléments de E , il existe une suite strictement croissante d'entiers $n_0 < n_1 < ... < n_i < n_{i+1} < ...$ telle que $e_{n_0} \preceq \cdots \preceq e_{n_i} \preceq e_{n_{i+1}} \preceq \cdots$

(iv) pour toute suite $(e_n)_{n\geq 0}$ d'éléments de E , il existe $i < j$ tels que $e_i \preceq e_j$.

Lorsque l'une de ces propriétés est vérifiée on dit que $\preceq$ est un *bel-ordre*.

2- Montrer que si $(E_1, \preceq_1), (E_2, \preceq_2)$ sont des ensembles munis chacun d'un bel-ordre, alors l'ordre-produit sur $E_1 \times E_2$:

$$(x_1, x_2) \preceq (y_1, y_2) \Leftrightarrow (x_1 \preceq_1 y_1 \text{ et } x_2 \preceq_2 y_2)$$

est un bel-ordre.

3- En déduire que l'ordre produit sur $\mathbb{N}^n$:

$$\overrightarrow{x} \leq \overrightarrow{y} \Leftrightarrow (\forall i \in [1, n], x_i \leq y_i)$$

est un bel-ordre.

On rappelle qu'un sous-monoïde du monoïde $(\mathbb{N}^n, +, 0)$ est une partie possédant 0 et stable par addition. Étant donnée une partie P du monoïde $(\mathbb{N}^n, +, 0)$, on note P^* le sous-monoïde *engendré par* P . Il s'agit du plus petit sous-monoïde de $\mathbb{N}^n$ contenant P. Il est caractérisé par :

$$x \in P^* \Leftrightarrow \exists k \in \mathbb{N}, \exists p_1, p_2, \dots p_k \in P, x = p_1 + p_2 + \cdots + p_k.$$

4- Soit M un sous-monoïde du monoïde $(\mathbb{N}^n, +, 0)$. Montrer que M est de *type fini* c'est à dire : il existe une partie finie $G \subseteq M$ telle que, $M = G^*$.
Indication : considérer l'ensemble G des éléments de $M \setminus \{0\}$ qui sont minimaux pour l'ordre produit.

Notons S_0 l'ensemble des éléments minimaux de l'ensemble $\mathcal{S}$ défini en (2).
5- Montrer que S_0 est finie.

Notons $M \subseteq \mathbb{N}^n$ l'ensemble

$$M := \{\overrightarrow{x} \in \mathbb{N}^n \mid A\overrightarrow{x} = \overrightarrow{0_n}\}.$$

6- Vérifier que M est un sous-monoïde de $\mathbb{N}^n$.
7- Montrer qu'il existe des parties finies $P, Q \subseteq \mathbb{N}^n$ telles que

$$\mathcal{S} = P + Q^*.$$

Une partie L de $\mathbb{N}^n$ la forme $L = P+Q^*$ pour des parties finies $P, Q \subseteq \mathbb{N}^n$ est dite *linéaire*. On appelle (P, Q) une *description linéaire* de L.

8- Comment peut-on calculer une description linéaire de $\mathcal{S}$ à partir de A, $\overrightarrow{b}$?
Rappel : on peut utiliser les parties précédentes du devoir.

9- Donner une description linéaire de l' ensemble des solutions en nombres entiers naturels de chacun des cinq systèmes :

$$2x - y = 5$$

$$2x - y - z = 7$$

$$2x - y \geq 7$$

$$2x - 3y - z = -1 \text{ et } x - y - t = 3$$

$$2x - 3y \geq -1 \text{ et } x - y \geq 3$$