Rapport de stage L3

Sous la supervision de Tristan Vaccon et Simone Naldi

Corentin Cornou

26 juillet 2023

Table des matières

Introduction

1 Spectraèdres réels

1.1 définiion ?

trouver un nom

Définition 1. On appelle *matrice symétrique semi-définie positive* toute matrice réelle symétriques et à valeurs propres positives ou nulles. On notera $\mathcal{S}_n^+(\mathbb{R})$ l'ensemble de telles matrices et $M \succeq 0$ le fait que $M \in \mathcal{S}_n^+(\mathbb{R})$.

Remarque. On remarquera que demander la symétrie, n'est, dans le cas réel, qu'un moyen de s'assurer d'obtenir des valeurs propres réelles grâce au théorème spectral.

Propriété 1. L'ensemble $\mathcal{S}_n^+(\mathbb{R})$ est un cône convexe fermé.

Définition 2. On appelle *spectraèdre* l'intersection de $\mathcal{S}_n^+(\mathbb{R})$ avec un espace affine $\mathcal{L}$ de $\mathcal{S}_n(\mathbb{R})$.

En écrivant l'hyperplan $\mathcal{L}$ de $\mathcal{S}_n^+(\mathbb{R})$ sous sa forme paramétrique *i.e.* comme l'ensemble des matrices de la forme $A_0 + x_1A_1 + \dots x_sA_s$ pour $A_0, \dots, A_s$ des matrices symétriques fixées on peut définir le spéctraèdre $\mathcal{S} = \mathcal{L} \cap \mathcal{S}_n^+(\mathbb{R})$ comme $\mathcal{S} = \{A := A_0 + x_1A_1 + \dots + x_sA_s | A \succeq 0, (x_1, \dots, x_s) \in \mathbb{R}^s\}$. On identifie alors souvent ce dernier à sa préimage dans $\mathbb{R}^s$ $S = \{(x_1, \dots, x_s) \in \mathbb{R}^s | A_0 + x_1A_1 + \dots + x_sA_s \succeq 0\}$.

Exemple. Un exemple celèbre de spectraèdre est l'ensemble des matrices symétrique semi-définie positives avec diagonale $(1, 1, 1)$:

$$S = \left\{ \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} \in \mathbb{R}^3 | A := \begin{pmatrix} 1 & x_1 & x_2 \\ x_1 & 1 & x_3 \\ x_2 & x_3 & 1 \end{pmatrix} \succeq 0 \right\}.$$

La surface algébrique définie par $\det A(x_1, x_2, x_3) = 0$ est dite *cubique de Cayley* (1). Les quatres points singuliers correspondent à quatre matrices semi-définies positives de rang un ; les autres points de la surface, correspondent à des matrices de rang deux (semi-définies si sur la frontière du spectraèdre, avec au moins une valeure propre négative autrement) ; enfin, les matrices à l'intérieur du spectraèdre sont définies positives (toutes valeurs singulières strictement positives).

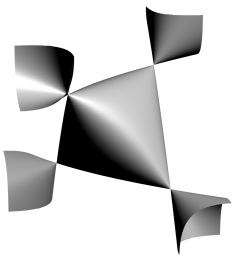

FIGURE 1 – Cubique de Cayley

1.2 Programmation semi-définie

On appelle alors *programmation semi-définie* le problème d'optimisation consistant à minimiser une application linéaire sur un spéctraèdre que l'on formulera comme :

$$\begin{aligned} &\text{Minimiser } \langle c, x\rangle \\ &\text{tel que } A_0 + \sum_{i=1}^{s} x_i A_i \succeq 0 \end{aligned} \tag{PSD}$$

pour $A_0, \ldots, A_s$ des matrices symétriques fixées, $c = (c_1, \ldots, c_s)$ un vecteur représentant le coût et $x \mapsto \langle c, x\rangle := c_1x_1 + \cdots + c_sx_s$ le produit scalaire Euclidien. Le problème d'admissibilité associé au problème d'optimisation (PSD), c'est-à-dire, la question si le spectraèdre $S = \{(x_1, \ldots, x_s) \in \mathbb{R}^s | A_0 + x_1A_1 + \ldots + x_sA_s \succeq 0\}$ est vide, est appelée *inégalité matricielle linéaire (LMI)*.

En précision finie ε, ce problème se résout en temps polynomial en la dimension de l'entrée (taille des matrices, nombre de variables, taille binaire des coefficients), en $\log(1/\varepsilon)$ et $\log(R)$, où R est une borne *a priori* sur la norme d'une solution. En arithmétique exacte, la complexité de la programmation semi-définie est un problème essentiellement ouvert, cf [De 06, Sec.1.9], [Ram97 ; PK97] et [HNE16].

Si à première vue ce problème peut sembler très spécifique il n'en est rien et de nombreux autres problèmes se rapportent à celui-ci. Par exemple, tout problème d'optimisation linéaire est en particulier un problème SDP :

Remarque. Un polyèdre est un spectraèdre ; en particulier, l'optimisation linéaire est une sous-classe de l'optimisation semi-définie. En effet, soit $P = \{x \in \mathbb{R}^s | \ell_1(x) \geq 0, \ldots, \ell_d(x) \geq 0\}$ le polyèdre défini par les inégalités linéaires $\ell_1, \ldots, \ell_d$, et soit D la matrice linéaire diagonale avec entrées $\ell_1, \ldots, \ell_d$. Alors P est le spectraèdre défini par $D \succeq 0$.

2 Introduction aux nombres p-adiques

On se contentera dans cette section d'une description très élémentaire des différentes définitions et propriétés des nombres p-adiques. La plupart des preuves relatives à cette section ainsi que de plus amples informations sont disponibles en A. Cette section est très largement inspiré du cours de Xavier Caruso [Car17] que l'on invite d'ailleurs à aller consulter pour une vision plus complète mais très largement compréhensible.

Notation. On considère pour tout ce rapport p un nombre premier.

2.1 Entiers p-adique

Définition 3. Entier p-adique

On appelle entier p-adique la somme formelle :

$$z = a_0 + a_1 p + \ldots + a_n p^n + \ldots$$

où les a_i sont des entiers compris entre 0 et $p-1$.

Remarques.
- On note $\mathbb{Z}_p$ l'ensemble des entier $p-$adiques.
- Par commodité on notera $\overline{\ldots a_n \ldots a_1 a_0}^p$ ou plus simplement $\ldots a_n \ldots a_1 a_0$ l'entier p-adique $\sum a_i p^i$

Exemple.

Ainsi les sommes $\sum_{i=0}^{\infty} p^i = \overline{\ldots 1111111}^p$ ou $\sum_{i=0}^{\infty} (i \bmod p) p^i = \overline{\ldots 210(p-1)\ldots 21}^p$ sont des entiers p-adiques parfaitement définis bien que ne convergeant pas dans le cas réel.

Propriété 2. $\mathbb{Z}_p$ peut être muni d'une structure d'anneau commutatif intègre en lui adjoignant l'addition terme à terme avec retenue et la multiplication.

Par exemple dans $\mathbb{Z}_5$

Définition 4. L'anneau $\mathbb{Z}$ des entiers relatifs s'identifie naturellement à un sous-anneau de $\mathbb{Z}_p$.

TABLE 1 – Exemples d'opérations dans $\mathbb{Z}_p$

$$\begin{array}{rr} & \ldots 34202243 \\ + & \ldots 01423401 \\ \hline & \ldots 41131144 \end{array} \qquad \begin{array}{rr} & \ldots 02243 \\ \times & \ldots 23401 \\ \hline & \ldots 02243 \\ & \ldots 0000 \\ & \ldots 132 \\ & \ldots 34 \\ + & \ldots 1 \\ \hline & \ldots 14443 \end{array}$$

Remarque. Si l'on a vu que les entiers relatifs étaient des entiers p-adiques, certains entiers p-adique ont du sens en tant que nombre rationnels sans être des entiers relatifs, ainsi on a par exemple $\frac{1}{2} = \ldots 2223 \in \mathbb{Z}_5$. Cependant tous les rationnels ne sont pas éléments de $\mathbb{Z}_p$, $\frac{1}{p}$ n'étant par exemple jamais inclus dans $\mathbb{Z}_p$.

2.2 Nombres p-adiques

Définition 5. Nombres p-adiques

On définit l'ensemble $\mathbb{Q}_p$ des nombres p-adiques comme $\mathbb{Z}_p\left[\frac{1}{p}\right]$ [a].

a. Le lecteur habitué à travailler dans $R[[X]]$ y verra dans la construction de $\mathbb{Q}_p$ à partir de $\mathbb{Z}_p$ une ressemblance avec celle de $R(X)$ à partir de $R[[X]]$. De nombreux autres similitudes entres ces ensemble peuvent être trouvées mais nos éviterons de les faire apparaître afin de rester à un niveau élémentaire (à reformuler bien).

Un nombre p-adique x s'écrit alors comme une somme de la forme $x = \sum_{i=k}^{\infty} x_i p^i$ avec $k \in \mathbb{Z}$ et les x_i compris entre 0 et $p-1$. Si $k < 0$ on écrira plus couramment $x = \overline{\ldots x_i \ldots x_1 x_0, x_{-1} \ldots x_k}^p$.

Propriété 3. $\mathbb{Q}_p$ est un corps qui étend les opérations de $\mathbb{Z}_p$.

Preuve : Voir annexe.

Corollaire 1. Le corps $\mathbb{Q}$ des rationnels est un sous-corps de $\mathbb{Q}_p$.

Ce dernier résultat permet de construire de manière assez élémentaire des éléments de $\mathbb{Q}_p$ qui ne sont pas des entiers p-adique.

2.3 Valuation et norme

On définit la valuation p-adique dans $\mathbb{Z}$ $\mathrm{val}_p^{\mathbb{Z}} : \mathbb{Z} \to \mathbb{N} \cup \{+\infty\}$ comme l'application qui à 0 associe $+\infty$ et à un entier a non nul associe le plus grand entier naturel k tel que $p^k | a$.

La valuation p-adique s'étend ensuite aux nombres rationnels en une application $\mathrm{val}_p^{\mathbb{Q}} : \mathbb{Q} \to \mathbb{Z} \cup \{+\infty\}$ en définissant pour tout $r \in \mathbb{Q}$ $\mathrm{val}_p^{\mathbb{Q}}(r) = \mathrm{val}_p^{\mathbb{Z}}(a) - \mathrm{val}_p^{\mathbb{Z}}(b)$ avec $a, b \in \mathbb{Z} \times \mathbb{N}^*$ tels que $r = \frac{a}{b}$.

La valuation p-adique s'étend alors également à $\mathbb{Q}_p$ depuis $\mathbb{Q}$ comme suit :

Définition 6. Valuation p-adique

On appelle valuation p-adique l'application $\mathrm{val}_p : \mathbb{Q}_p \to \mathbb{Z} \cup \{+\infty\}$ qui à un nombre p-adique x associe $\max\{k \in \mathbb{Z} \cup \{+\infty\} | x \in p^k \mathbb{Z}_p\}$.

Une manière simple de visualiser la valuation d'un nombre p-adique est de compter la "distance à la virgule".

En effet, la valuation d'un entier p-adique correspond au nombres de 0 à la fin de son écriture décimale et pour un nombre p-adique non entier il s'agit de l'opposé nombre de chiffres p-adiques après la virgule. Par exemple, $\mathrm{val}_p(\ldots 2413000) = 3$ et $\mathrm{val}_p(\ldots 251,24) = -2$.

Le principal intérêt qu'offre la notion de valuation pour le sujet développé ici est qu'elle permet de définir une notion de positivité dans un corps qui n'est pas

totalement ordonnable [1]. À cet effet on introduira la notation suivante :

Notation. Pour tout élément $x \in \mathbb{Q}_p$, on dit que x est *positif* et on note $x \geq 0$ si $\mathrm{val}_p(x) \geq 0$. On en induit alors les notations $x > 0$, $x \leq 0$ et $x < 0$.

On évitera la notation $x \geq y$ qui pourrait laisser penser de manière trompeuse que $x \geq y \Rightarrow x - y \geq 0$ [2].

Propriété 4. La valuation p-adique possède les propriétés suivantes, pour tous x et y appartenant à $\mathbb{Q}_p$:

1. $\mathrm{val}_p(x+y) \geq \min(\mathrm{val}_p(x), \mathrm{val}_p(y))$ avec égalité si $\mathrm{val}_p(x) \neq \mathrm{val}_p(y)$
2. $\mathrm{val}_p(xy) = \mathrm{val}_p(x) + \mathrm{val}_p(y)$

Preuve : Voir annexe.

Ces propriétés permettent alors de munir $\mathbb{Q}_p$ d'une valeur absolue que l'on définira comme suit :

Définition 7. Valeur absolue p-adique

On appelle valeur absolue p-adique l'application

$$\begin{aligned} |\cdot|_p : \mathbb{Q}_p &\longrightarrow \mathbb{R}_+^* \\ x &\longmapsto p^{-\mathrm{val}_p(x)} \end{aligned}$$

qui est une valeur absolue, c'est-à-dire, une norme compatible avec le produit.

Preuve : Découle directement de 4.

On observera en particulier que, d'après 4, pour tous x, y éléments de $\mathbb{Q}_p$ on a l'inégalité $|x+y|_p \leq \max\left(|x|_p, |y|_p\right)$. Ce qui en fait un corps non archimédien [3] et rend la géométrie p-adique très différente du cas réel peu et intuitive si l'on y est pas habituée. Ce qui explique le manque de figure et d'explications par le dessin dans la suite de ce rapport.

On terminera cette section en discutant la proposition suivante, qui est d'une importance cruciale puisqu'elle offre une caractérisation simple de la positivité dans $\mathbb{Q}_p$.

1. i.e. il n'y a pas relation d'ordre $\geq$ sur $\mathbb{Q}_p$ compatible avec l'addition et telle que $\forall s \geq 0$ $x \geq y \Rightarrow sx \geq sy$.
2. Par exemple, $\mathrm{val}_p(\ldots 11, 11) \geq \mathrm{val}_p(\ldots 00, 01)$ mais $\mathrm{val}_p(\ldots 11, 11 - \ldots 00, 01) = \mathrm{val}_p(\ldots 11, 1) < 0$
3. c'est-à-dire tel que $\mathbb{N}$ est borné dans $\left(\mathbb{Q}_p, |\cdot|_p\right)$

Proposition 1. Soit $x \in \mathbb{Q}_p$. Les trois propriétés suivantes sont équivalentes

i. $x \in \mathbb{Z}_p$

ii. $\mathrm{val}_p(x) \geq 0$

iii. $|x|_p \leq 1$

On dira alors indistinctement qu'un nombre x est un entier, est un élément de la boule unité ou est positif (conformément à la notation définie précédemment).

Preuve de la propriété : L'équivalence entre *ii.* et *iii.* découle directement de la définition de $|\cdot|_p$. Puis on conclut en remarquant que $x \in \mathbb{Z}_p = p^0\mathbb{Z}_p$ si et seulement si $\mathrm{val}_p(x) \geq 0$ c'est-à-dire $i. \Leftrightarrow ii.$.

2.4 Polyèdres convexes p-adiques

2.5 Polyèdres convexes p-adiques

Définition 8. (Matrice positive)

Une matrice M de $\mathcal{M}_n(\mathbb{Q}_p)$ est dite *positive* si tous ses coefficients sont positifs ou nuls, c'est-à-dire, par définition si elle est à coefficient dans $\mathbb{Z}_p$. On notera alors $M \geq 0$ le fait que $M \in \mathcal{M}_n(\mathbb{Z}_p)$

Propriété 5. L'ensemble $\mathcal{M}_n(\mathbb{Z}_p)$ est :

i. ouvert

ii. fermé

iii. borné

iv. compact

v. convexe au sens de [Mon58]

Preuve : i. et *ii.* se déduisent du fait que $\mathbb{Z}_p$ soit ouvert et fermé dans $\mathbb{Q}_p$, *ii.* découle directement du fait que $\|M\|_\infty = \sup |M_{i,j}|_p \leq 1$ et *iv.* se déduit de *ii.* et *iii.*. Quand à *v.* c'est une conséquence directe de la convexité de $\mathbb{Z}_p$.

$\mathcal{M}_n(\mathbb{Z}_p)$ est un cône p-adique pour la définition :Soit $\mathbb{E}$ un $\mathbb{Q}_p$ espace vectoriel $C \subset \mathbb{E}$ est un cône si pour tout $x \in C$ et $\lambda \geq 0$ $\lambda x \in C$. La preuve pour $\mathcal{M}_n(\mathbb{Z}_p)$ est assez triviale et pour $S_n^+(\mathbb{Q}_p)$ elle est laissée en exercice au lecteur

Définition 9. On définit un polyèdre convexe P comme l'intersection de $\mathcal{M}_n(\mathbb{Z}_p)$ avec un espace affine $\mathcal{L}$ de $\mathcal{M}_n(\mathbb{Q}_p)$.

Comme en **??** dans le cas réel on identifiera un polyèdre à sa préimage. Ce qui permet le résultat suivant :

Exemple. La boule unité de $\mathbb{Q}_p^n$ pour la norme infinie est un polyèdre. En effet, la boule infinie s'écrit comme l'ensemble des points $(x_1, \ldots, x_n)$ tels que $\begin{pmatrix} x_1 & & & \\ & x_2 & 0 & \\ & 0 & \ddots & \\ & & & x_n \end{pmatrix} \geq 0$. En effet, la boule unité de $\mathbb{Q}_p^n$ est $\mathbb{Z}_p^n$.

3 Optimisation

3.1 Programmation linéaire p-adique

Dans ce paragraphe, il sera étudié une forme équivalente du problème de programmation linéaire, appelée *programmation linéaire p-adique* (PLp) . Lequel consiste simplement à minimiser la norme p-adique d'une application linéaire sur un polyèdre p-adique.

Du fait des natures profondément différentes des polyèdres p-adiques et du cas réel, les techniques classiques de résolution sont mises à mal. Il est effet complexe d'appliquer la méthode du simplexe à un ensemble sans frontière ou des techniques d'analyse convexe dans un espace sans notion de convexité. Il convient donc alors de développer de nouvelles techniques pour résoudre ces problèmes. C'est ce qui est proposé dans cette section, qui présente un algorithme en $O(\max(m,n)^2)$, avec m, n les dimensions de la matrice de contrainte, pour résoudre le problème de la programmation linéaire en p-adique, dont une écriture en pseudo-code ainsi qu'une implémentation en SageMathsont disponible en C.

Cet algorithme est centré sur l'utilisation de la forme normale de Smith d'une matrice, dont seul la définition et quelques remarques sont présenté dans cette section, les preuves des résultats présentés ici ainsi que d'autres résultats sont disponible en B.

On appelle *programmation linéaire p-adique* le problème :

$$\begin{array}{c} \text{Minimiser } \mathrm{val}_p\left(\langle c, x\rangle\right) \text{ tel que} \\ Ax + b \geq 0 \end{array} \tag{PLp}$$

avec x un vecteur de taille n que l'on fait varier, c un vecteur de taille n représentant le coût, A une matrice de taille $m \times n$ et b un vecteur de taille m.

La méthode choisie ici consiste à mettre la matrice A sous forme normale de Smith, un factorisation classique en p-adique et qui permet de grandement simplifier le problème posé.

Définition 10. Forme Normale de Smith

On appelle forme normale de Smith d'une matrice $M \in \mathcal{M}_{m,n}(\mathbb{Q}_p)$ de rang r l'unique matrice S de la forme

$$S = \begin{pmatrix} p^{a_1} & & & & \\ & \ddots & & & \\ & & p^{ar} & & \\ & & & 0 & \\ & & & & \ddots \end{pmatrix}$$

telle que $a_1 \leq \ldots \leq a_r$ et $M = Q^{-1}SP$ avec $P \in \mathcal{G}L_n(\mathbb{Z}_p)$ et $Q \in \mathcal{G}L_m(\mathbb{Z}_p)$.

ner un exemple

Remarques. i. Les coefficients de la forme normale de Smith sont uniques à chaque matrice et sont appelés *facteurs invariants de Smith* ou, plus simplement, *invariants de Smith*.

ii. La valuation p-adique du premier coefficient de la forme normale de Smith d'une matrice $M \in \mathcal{M}_n(\mathbb{Q}_p)$ est égale au minimum des valuation des termes de M.

iii. En particulier, la forme normale de Smith d'une matrice de $\mathcal{M}_n(\mathbb{Z}_p)$ est à coefficients dans $\mathbb{Z}_p$.

iv. Les $r = \text{rang}M$ premiers coefficients diagonaux de S sont exactement ses coefficients non nuls.

Avant de pouvoir utiliser la forme de normale de Smith pour résoudre PLp, il nous faut démontrer le lemme suivant :

Lemme 1. Pour tous $z \in \mathbb{Q}_p^n$ et $M \in \mathcal{M}_{m,n}(\mathbb{Q}_p)$ si $z \geq 0$ et $M \geq 0$ alors $Mz \geq 0$.

Preuve : $\mathbb{Z}_p$ est un anneau. □

En mettant alors la matrice A de PLp sous sa forme normale normale de Smith il vient que résoudre PLp revient à résoudre :

$$\begin{array}{c} \text{Minimiser } \text{val}_p(\langle c', x\rangle) \text{ tel que} \\ Sy + b' \geq 0 \end{array} \qquad \text{(PLp')}$$

où $b' = Qb$, $c' = P^T c$, S est la forme normale de Smith de A et $A = Q^{-1}SP$ avec $P \in \mathcal{G}L_m(\mathbb{Z}_p)$ et $Q \in \mathcal{G}L_n(\mathbb{Z}_p)$.

Remarques. Il en vient immédiatement plusieurs résultats :

1. x^* est une solution admissible de PLp si et seulement si $y^* := Px^*$ est une solution admissible de PLp'
2. PLp' possède des solutions admissible si et seulement si les $m - r$ coefficients de b' sont non nuls, où r le rang de S.
3. Si les $n - r$ tous derniers coefficients de c' sont non nuls PLp' n'est pas borné et n'admet donc pas de solution.

Propriété 6.

- Si les $m - r$ coefficients de b' ne sont pas tous nuls alors il n'existe pas de $y \in \mathbb{Q}_p^n$ tel que $A'y + b' \geq 0$.
- Si les $n - r$ coefficients de c' ne sont pas tous nuls alors le problème n'est pas borné et n'admet donc pas de solution.

En ne considérant alors que les itérations du problème admettant des solutions on peut réduire le problème en ne considérant que les r premiers coefficients de y, b', c' et la sous matrice de S composée des r premières lignes et colonnes et dont les coefficients sont alors les exactement les facteurs invariants de Smith non

nuls. L'ensemble Adm des solutions admissible s'écrit alors comme l'ensemble des vecteurs $y \in \mathbb{Q}_p^n$ vérifiant $\forall 1 \leq i \leq r \ s_i y_i + b'_i \in \mathbb{Z}_p$ c'est-à-dire vérifiant :

$$\forall 1 \leq i \leq r y_i \in -\frac{b'_i}{s_i} + \frac{1}{s_i}\mathbb{Z}_p \tag{1}$$

Résoudre PLp' revient donc à minimiser $\mathrm{val}_p(\langle c', y\rangle)$ sur Adm. L'image de Adm par $y \mapsto \langle c', y\rangle$ est $\sum_{i=1}^r -c'_i.\frac{b'_i}{s_i} + \sum_{i=1}^r \left(\frac{c'_i}{s_i}\mathbb{Z}_p\right)$ qui se réécrit :

$$c' Adm = \lambda + p^v \mathbb{Z}_p$$

où $\lambda = \sum_{i=1}^{r} -c'_i.\frac{b'_i}{s_i}$ et $v = \min_{1\leq i\leq r} \mathrm{val}_p \frac{c'_i}{s_i}$. Ainsi, deux cas apparaissent.

— Soit $\mathrm{val}_p(\lambda) < v$ auquel cas le minimum de $y \mapsto \mathrm{val}_p(\langle c', y\rangle)$ sur Adm est atteint en n'importe quel point de Adm et vaut $\mathrm{val}_p(\lambda)$.

— Soit $\mathrm{val}_p(\lambda) \geq v$, auquel cas $\lambda \in p^v\mathbb{Z}_p$ et le minimum vaut v et est atteint en tous les points y de Adm vérifiant

$$\mathrm{val}_p \sum_{\substack{1 \leq i \leq r \\ \mathrm{val}_p(c'_i/s_i) = v}} y_i = 0.$$

Remarque. Si l'on souhaite maximiser la valuation d'un application linéaire su un polyèdre p-adique au lieu de la minimiser (ce qui revient à maximiser la valeur absolue) on pourra utiliser un raisonnement similaire à celui présenté dans cette partie. La seule différence est que si $\mathrm{val}_p(\lambda) < v$ le problème n'est pas borné et n'admet donc pas de solution.

4 Spectraèdres p-adiques

Ce paragraphe tend à fournir un définition de la notion de matrice semi-définie positive sur les corps $p-$adiques pour en déduire une définition de spectraèdre qui serait pertinente sur un corps non-archimédien. La première étape pour définir un spectraèdre est de définir un équivalent des matrices symétriques définies positives. Sans théorème spectral et le produit scalaire n'étant qu'une forme bilinéaire "banale" (ni positive ni définie), la symétrie est en p-adique parfaitement inutile et ne sera pas exigé. De plus, du fait du manque cruel du théorème spectral la plupart des caractérisations des matrices symétriques semi-définies positives peinent à faire sens en p-adique. Il a donc été choisi de définir les matrices semi-définies positives [4]comme les matrices à valeurs propres positives. Or là un second problème se pose : $\mathbb{Q}_p$ n'est pas algébriquement clos et les matrices $\mathcal{M}_n(\mathbb{Q}_p)$ peuvent donc avoir des valeurs propres hors de $\mathbb{Q}_p$. Ce problème sera réglé en étendant la valuation p-adique aux extensions de $\mathbb{Q}_p$.

4. notez l'absence du mot symétrique

4.1 Clôture algébrique p-adique

Cette section présente quelques résultats élémentaires sur les extensions de corps p-adiques. La plupart des résultats présentés dans cette section étant soit classique et trouvable dans n'importe quel cours d'algèbre de niveau master soit élémentaires, peu de preuves y seront importés. On recommandera toutefois la lecture de la section 5 de [Gou03] pour plus d'information sur les extensions de corps p-adiques.

Définition 11. On appelle *extension de corps* d'un corps $\mathbb{K}$ tout corps $\mathbb{L}$ muni d'un morphisme de corps injectif de $\mathbb{K}$ dans $\mathbb{L}$. On note $\mathbb{L}/\mathbb{K}$ le fait que $\mathbb{L}$ soit une extension de $\mathbb{K}$.

Une extension d'un corps $\mathbb{K}$ est grossièrement un corps contenant une copie du corps $\mathbb{K}$.

Définition 12. Un corps $\mathbb{K}$ est dit algébriquement clos si tout polynôme $P \in \mathbb{K}[X]$ de degré au moins 1 possède une racine dans $\mathbb{K}$.

Proposition 2. $\mathbb{Q}_p$ n'est pas algébriquement clos.

Preuve : Le polynôme $X^2 - p$ n'a pas de racine dans $\mathbb{Q}_p$ □.

Définition 13. On appelle clôture algébrique l'unique (à isomorphisme près) corps $\mathbb{L}$ tel que tout élément de $\mathbb{L}$ est racine d'un polynôme de $\mathbb{K}[X]$ et $\mathbb{L}$ est algébriquement clos.

On notera $\overline{\mathbb{Q}_p}$ la clôture algébrique de $\mathbb{Q}_p$, il est alors possible d'y étendre la valuation p-adique comme suit :

Définition 14. On définit la valuation p-adique sur $\overline{\mathbb{Q}_p}$ comme

$$\begin{aligned} \mathrm{val}_p : \overline{\mathbb{Q}_p} &\longrightarrow \mathbb{Q} \cup \{+\infty\} \\ x &\longmapsto \mathrm{val}_p^{\mathbb{Q}_p}(a)/d \end{aligned}$$

où d et a sont respectivement le degré et le terme constant du polynôme minimal de x.

On retrouve alors une notion de positivité dans l'extension de corps et étendra à $\overline{\mathbb{Q}_p}$ la notation $x \geq 0$ si et seulement si $\mathrm{val}_p(x) \geq 0$. Il n'est cependant informatiquement pas très pratique de travailler dans $\overline{\mathbb{Q}_p}$ qui est n'est pas une extension finie de $\mathbb{Q}_p$ [5]. On cherchera donc des caractérisations plus simples pour savoir si un polynôme est à racines positives, ce qui sera fait dans la prochaine section.

5. c'est-à-dire $\overline{\mathbb{Q}_p}$ est un $\mathbb{Q}_p$-espace vectoriel de dimension infinie

4.2 Matrices semi-définies positives

Définition 15. On appelle matrice semi-définie positive toute matrice $M \in \mathcal{M}_n(\mathbb{Q}_p)$ dont toutes les valeurs propres sont de valuation positive ou nulle.

On note $\mathcal{M}_n^+(\mathbb{Q}_p)$ l'ensemble des matrices semi-définies positives .

Théorème 1. Caractérisation des matrices semi-définies positives

Une matrice est symétrique définie positive si et seulement si son polynôme caractéristique est à coefficient dans $\mathbb{Z}_p$.

Preuve : Voir annexe.

Conséquence 1. $\mathcal{M}_n(\mathbb{Z}_p) \subset \mathcal{M}_n^+(\mathbb{Q}_p)$

Preuve : $\mathbb{Z}_p$ étant un anneau, le polynôme caractéristique d'une matrice à coefficients dans $\mathbb{Z}_p$ est à coefficient dans $\mathbb{Z}_p$. Onconclut par 1 .

Remarque. En général l'inclusion réciproque est fausse. Ainsi pour $M = \begin{pmatrix} 5+\frac{3}{5} & \frac{4}{5} \\ \frac{4}{5} & -\frac{3}{5} \end{pmatrix}$, on a $\chi_M = X^2 - 5X - 4$. Or une fois M plongé dans $\mathbb{Q}_5$ on a $\chi_M \in \mathbb{Z}_5[X]$ donc $M \in S_2^+(\mathbb{Q}_5)$ or aucun des coefficients de M n'est dans $\mathbb{Z}_5$

probablement pas nécessaire ira peut-être en annexe

Propriété 7. L'ensemble $\mathcal{M}_n^+(\mathbb{Q}_p)$ est :

i. ouvert

ii. fermé

iii. un cône

Preuve : Montrons tout d'abord que $\mathbb{Z}_p[X]$ est fermé et ouvert dans $\mathbb{Q}_p[X]$ muni de la norme infinie $\|.\|_\infty : P = \sum_{k=1}^n a_k X^k \to \sup |a_k|_p$. Il suffit pour cela de remarquer que $\|\cdot\|_\infty$ définit une distance discrète pour laquelle les boules fermées sont également ouvertes. Or, $\mathbb{Z}_p$ est la boule ouverte de centre 0 et de rayon 1 donc est fermée et ouverte. On montre alors *i.* et *ii.* par $\mathcal{M}_n^+(\mathbb{Q}_p) = \chi^{-1}(\mathbb{Z}_p[X])$ ou χ est l'application qui a une matrice associe son polynôme caractéristique qui est continue car polynomiale en les coefficients de la matrice.

Le *iii.* est laissé en exercice au lecteur.

Remarque. L'ensemble $S_n^+(\mathbb{Q}_p)$ n'est pas convexe en général.

Par exemple pour $p = 5$, si on considère les matrices $M_1 = \begin{pmatrix} 5+\frac{3}{5} & \frac{4}{5} \\ \frac{4}{5} & -\frac{3}{5} \end{pmatrix}$ et $M_2 = \begin{pmatrix} 25+\frac{7}{25} & \frac{24}{25} \\ \frac{24}{25} & -\frac{7}{25} \end{pmatrix}$, on a $\chi_{M_1} = X^2 - 5X - 4$ et $\chi_{M_2} = X^2 - 25X - 8$ donc en plongeant ces matrices dans $\mathbb{Q}_5$ il vient que $\chi_{M_1}, \chi_{M_2} \in \mathbf{Z}_5[X]$ i.e. $M_1, M_2 \in S_2^+(\mathbb{Q}_5)$. Or $\chi_{M_1+M_2} = X^2 - 150X - \frac{3784}{5}$ qui une fois plongé dans $\mathbb{Q}_5$ n'est pas à coefficient dans $\mathbb{Z}_5$, donc $S_2^+(\mathbb{Q}_5)$ n'est pas convexe. Ce résultat se généralise

pour tout n en considérant les matrice par blocs $M_i' = \text{diag}\,(M_i, 0, \ldots, 0)$.

4.3 Zoologie Spectraèdrique

Dans le cas réel de nombreux ensembles convexes peuvent être représentés comme des spectraèdres ou des projections de spectraèdres, il a même été conjecturé que tous les ensembles semialgébriques[6] convexes soient des ombres de spéctraèdres . Bien que cette conjecture ait ensuite été prouvée fausse , il n'en reste pas loin qu'un nombre important d'ensemble admettant une telle représentation garantisse sa flexibilité

lien machin

le lien

Définition 16. Couronnes

On appelle couronne tout ensemble C défini par $C = \{x \in \mathbb{Q}_p | a \leq \text{val}_p\,(x) \leq b\}$ pour $a < b$ deux réels positifs fixés.

Les couronnes sont un objet fondamentale de l'étude des espaces p-adique. .

expliquer pourquoi

Proposition 3. Les couronnes sont des projections de spectraèdres.

Preuve : Soit C la couronne de paramètres $a < b \in R_+^*$.

On considère pourtout $x, y \in \mathbb{Q}_p$ la matrice $M(x,y) := \begin{pmatrix} p^a x & 0 & 0 & 0 \\ 0 & p^{-b} y & 0 & 0 \\ 0 & 0 & p^{-1} & p^{-1} x \\ 0 & 0 & p^{-1} y & -p^{-1} \end{pmatrix}$

et le spectraèdre $\mathcal{S} = \{(x,y) \in \mathbb{Q}_p : M(x,y) \succeq 0\}$

Soient $x, y \in \mathbb{Q}_p$. Montrons que $x \in C$ si et seulement si $\exists y \in \mathbb{Q}_p\,(x,y) \in \mathcal{S}$.

Soient $x, y \in \mathbb{Q}_p$. En décomposant $M(x,y)$ en trois blocs : $p^a x$, $p^{-b} y$ et $M'(x,y) = \begin{pmatrix} p^{-1} & p^{-1} x \\ p^{-1} y & p^{-1} \end{pmatrix}$ et en utilisant 1 on a que $M(x,y)$ est semi-définie positive si et seulement si $\begin{cases} p^a x \geq 0 \\ p^{-b} y \geq 0 \\ \text{Tr} M'\,(x,y) = 0 \geq 0 \\ \det M'(x,y) = p^{-2}\,(xy - 1) \geq 0 \end{cases}$ c'est à dire si et seulement si

$$\begin{cases} \text{val}_p\,(x) \geq a \\ \text{val}_p\,(y) \geq -b \\ p^{-2}\,(xy - 1) \geq 0 \end{cases} \tag{2}$$

Or $x \in C$ si et seulement si il existe $y \in \mathbb{Q}_p$ tel que (x,y) vérifient 2. En effet, si x, y vérifient 1alors $\text{val}_p\,(x) \geq a$, $\text{val}_p\,(y) \geq -b$ et $p^{-2}\,(xy-1) \geq 0$ implique que $\text{val}_p\,(x) + \text{val}_p\,(y) = \text{val}_p\,(xy) = \text{val}_p\,(-1) = 0$ et donc que $\text{val}_p\,(x) = -\text{val}_p\,(y) \leq -(-b) = b$, donc $x \in$. Puis réciproquement si $x \in C$ alors (x, x^{-1}) vérifient 2 .

6. *i.e.* les ensembles définis par des inégalités polynomiales

A Complément sur les corps p-adique

Cette section de l'appendice présente la plupart des preuves qui n'ont pas été traitées en section 2 ainsi que quelques compléments sur les nombres p-adique pour en avoir une meilleur appréhension.

Représentation sous forme d'arbre

Un façon intuitive de se représenter les nombres p-adiques est de les écrire comme les feuilles d'un arbre infini.

On considère l'arbre $\mathcal{T}(\mathbb{Z}_p)$ dont les nœuds sont les suites finies à coefficients dans $\{1, \dots, p\}$ et tels que deux sommets sont reliés entre eux si et seulement si

Démonstration. Proposition 3 En réalité on dispose même d'un résultat plus précis : $\mathbb{Q}_p$ est le corps des fractions de $\mathbb{Z}_p$. Pour prouver ce résultat on utilisera le lemme suivant :

Lemme 2. Les inversibles de $\mathbb{Z}_p$ sont exactement les entiers p-adique $\overline{\dots x_n \dots x_1 x_0}$ tels que x_0 est non nul.

Preuve du lemme : Un entier p-adique $x = \overline{\dots x_n \dots x_1 x_0}$ est inversible si et seulement si il est inversible dans $\mathbb{Z}/p^n\mathbb{Z}$ pour tout $n \in \mathbb{N}$, c'est-à-dire si et seulement si $\sum_{i=0}^{n} p^i x_i$ est premier avec p^n pour tout $n \in \mathbb{N}$ ce qui est équivalent à x_0 premier avec p et donc $x_0 \neq 0$.

Ensuite il suffit de remarquer que tout entier p-adique non nul $x = \overline{\dots x_n \dots x_1 x_0}$ s'écrit $p^n \tilde{x}$ avec $\tilde{x} \in \mathbb{Z}_p^\times$ et n un entier naturel. On a de plus unicité par 2.

En effet, si on pose n le plus petit entier naturel tel que $x_n \neq 0$ [7] et $\tilde{x} := \overline{\dots x_n}$ on a immédiatement $x = p^n \tilde{x}$ et $\tilde{x} \in \mathbb{Z}_p^\times$. Il est alors immédiat que $\mathbb{Q}_p = \mathbb{Z}_p[\frac{1}{p}]$ est le plus petit corps contenant $\mathbb{Z}_p$

□

Démonstration. Propriété 4 Soient x, y deux entiers naturels de valuation $n := \mathrm{val}_p(x)$ et $m := \mathrm{val}_p(y)$. On peut alors écrire $x = p^n \tilde{x}$ et $y = p^m \tilde{y}$ avec $\tilde{x}, \tilde{y} \in \mathbb{Z}_p^\times$, comme vu On a alors tout d'abord $xy = (\tilde{x}\tilde{y})p^{n+m}$ et donc par unicité de la décomposition $\mathrm{val}_p(xy) = \mathrm{val}_p(x) + \mathrm{val}_p(y)$.

Ensuite, on trouve que $x + y \in p^n\mathbb{Z}_p + p^m\mathbb{Z}_p = p^{\min(m,n)}\mathbb{Z}_p$ ce qui signifie que $\mathrm{val}_p(x+y) \geq \min(\mathrm{val}_p(x), \mathrm{val}_p(y))$. Puis si $m \neq n$ on peut supposer sans perte de généralité que $m > n$ et $x + y$ s'écrit alors $p^n(p^{m-n}\tilde{x} + \tilde{y})$ et par 2, $p^{m-n}\tilde{x} + \tilde{y} \in \mathbb{Z}_p^\times$. □

Démonstration. Théorème 1

□

7. c'est-à-dire la valuation de x

B Forme normale de Smith

On revient dans cette partie sur la construction de la forme normale de Smith d'une matrice ainsi que sur les principaux résultats sur cette dernière. Ces résultats sont utilisé dans l'algorithme présenté en section 3.1. Les preuves de cette section ont étés tirées de puis rapportées au cas p-adique, là ou le cours original se place dans le cadre plus général des anneaux euclidiens.

le lien

Rappel. On appelle forme normale de Smith d'une matrice $M \in \mathcal{M}_{m,n}(\mathbb{Q}_p)$ de rang r l'unique matrice S de la forme

$$S = \begin{pmatrix} p^{a_1} & & & & \\ & \ddots & & & \\ & & p^{ar} & & \\ & & & 0 & \\ & & & & \ddots \end{pmatrix}$$

telle que $a_1 \leq \ldots \leq a_r$ et $M = Q^{-1}SP$ avec $P \in \mathcal{G}L_n(\mathbb{Z}_p)$ et $Q \in \mathcal{G}L_m(\mathbb{Z}_p)$.

Remarque préliminaire Soit M une matrice de $\mathcal{M}_{m,n}(\mathbb{Q}_p)$. Pour $k \in \mathbb{N}$ suffisamment grand $M_k := p^k M$ est à coefficient dans$\mathcal{M}_n(\mathbb{Z}_p)$. Il suffit donc de montrer l'existence et l'unicité de la forme normale de Smith sur les matrices de $\mathcal{M}_n(\mathbb{Z}_p)$ pour l'avoir sur toutes les matrices à coefficients dans $\mathbb{Q}_p$.

Démonstration. Existence de la forme normale de Smith.

On démontrera le résultat par récurrence sur $m+n$.

Les résultats dans les cas $n+m = 0, 1$ et 2 étant immédiats, on a l'initialisation.

Soit $k \in \mathbb{N}$ tel que tout matrice $M \in M_{m,n}(\mathbb{Z}_p)$ avec $m+n \leq k$ admettent une forme normale de Smith.

Soient $m, n \in \mathbb{N}$ tels que $m+n = k+1$ et $M \in \mathcal{M}_{m,n}(\mathbb{Z}_p)$.

Si M est nulle le résultat est immédiat. On supposera donc $M \neq 0$. On peut alors trouver un coefficient α de M de valuation minimale a_1. En multipliant M à droite et à gauche par des matrices de permutation on peut faire remonter ce coefficient en position $(1,1)$. M est alors équivalente à une matrice N de la forme :

$$N = \begin{pmatrix} \alpha & N_{1,2} & \ldots & N_{1,n} \\ N_{2,1} & * & \ldots & * \\ \vdots & \vdots & \ddots & \vdots \\ N_{m,1} & * & \ldots & * \end{pmatrix}.$$

On considère alors $\tilde{\alpha} := \alpha^{-1}p^{a_1}$ ainsi $\alpha\tilde{\alpha} = p^{a_1}$ et $\tilde{\alpha} \in \mathbb{Z}_p^\times$ conformément à 2. Multiplier à gauche N par la matrice $\mathrm{diag}(\tilde{\alpha}, 0, \ldots, 0)$ conserve l'équivalence

dans $\mathbb{Z}_p$ [8] et permet d'obtenir une matrice $\tilde{N}$:

$$\tilde{N} = \begin{pmatrix} p^{a_1} & \tilde{N}_{1,2} & \dots & \tilde{N}_{1,n} \\ N_{2,1} & * & \dots & * \\ \vdots & \vdots & \ddots & \vdots \\ N_{m,1} & * & \dots & * \end{pmatrix}.$$

On remarque en particulier que le passage de N à $\tilde{N}$ ne modifie pas la valuation de ses éléments. Or N s'écrivant comme permutation des coefficients de M p^{a_1} reste un coefficient de $\tilde{N}$ de valuation minimale. À ce titre pour tout $2 \leq i \leq m$ il existe $q_i \in \mathbb{Z}_p$ tel que $\tilde{N}_{i,1} = p^{a_1} q_i$ et de même pour tout $2 \leq j \leq n$ on dispose de $p_j \in \mathbb{Z}_p$ vérifiant $N_{1,j} = p^{a_1} p_j$. On fixe de tels q_i et p_j. En ajoutant à la i-ième ligne de $\tilde{N}$ q_i fois la première pour $2 \leq i \leq m$ on annule alors tous les coefficients de la première ligne sauf p^{a_1} en conservant l'équivalence.

$$\begin{pmatrix} p^{a_1} & \tilde{N}_{1,2} - p^{a_1} q_i & \dots & \tilde{N}_{1,n} - p^{a_1} q_i \\ N_{2,1} & * & \dots & * \\ \vdots & \vdots & \ddots & \vdots \\ N_{m,1} & * & \dots & * \end{pmatrix} = \begin{pmatrix} p^{a_1} & 0 & \dots & 0 \\ N_{2,1} & * & \dots & * \\ \vdots & \vdots & \ddots & \vdots \\ N_{m,1} & * & \dots & * \end{pmatrix}.$$

On procède alors pareillement pour les colonnes en ajoutant à la j-ième colonne de la matrice nouvellement obtenue p_j fois la première pour obtenir une matrice dont le seul coefficient non nul de la première ligne et colonne est p^{a_1}.

$$\begin{pmatrix} p^{a_1} & 0 & \dots & 0 \\ 0 & * & \dots & * \\ \vdots & \vdots & \ddots & \vdots \\ 0 & * & \dots & * \end{pmatrix}.$$

Dans les cas particuliers ou $m = 1$ ou $n = 1$ la preuve s'arrête ici, la matrice étant de la forme demandée. Sinon les coefficients de la matrice nouvellement obtenue s'écrive comme sommes et produits de coefficients de M et sont de valuation supérieure à a_1. On applique alors l'hypothèse de récurrence et obtient le résultat. □

Remarques. On observe que la preuve ci-dessus décrit en fait une procédure permettant de canuler la forme normale de Smith d'une matrice ainsi que des matrices de passages associées en $O\left(\max(m,n)^3\right)$ opérations. Il est cependant possible d'obtenir ce même résultats en $O(n^\omega)$.

comment je dis que Tristan a pas encore publié l'article

Démonstration. Unicité de la forme normale de Smith Soit $M \in \mathcal{M}_{m,n}(\mathbb{Z}_p)$ et

8. car on multiplie par une matrice de déterminant inversible dans $\mathbb{Z}_p$ et donc elle même inversible.

$S = \begin{pmatrix} p^{a_1} & & & & \\ & \ddots & & & \\ & & p^{ar} & & \\ & & & 0 & \\ & & & & \ddots \end{pmatrix}$ sa forme normale de Smith.

La preuve de l'unicité repose sur le fait que la valuation minimale pour les sous-déterminants de taille $k \times k$ de M soit $a_1 + a_2 + \ldots + a_r$ si $k \leq r$ et 0 sinon pour $k = 1, \ldots, \min(m, n)$. Ce qui permet de conclure immédiatement à l'unicité de S.

On note pour toute matrice $A \in \mathcal{M}_{m,n}(\mathbb{Z}_p)$, $v_k(A)$ la valuation minimale des déterminants de taille $k \times k$ de A, pour $k = 1 \ldots \min(m, n)$.

Remarquons tout d'abord la propriété suivante : pour tous $A \in \mathcal{M}_{m,n}(\mathbb{Z}_p)$ et $Q \in \mathcal{M}_n(\mathbb{Z}_p), v_k(AQ) \leq v_k(A)$

Le résultat est une conséquence immédiate de 4.

On en déduit alors ce résultat plus fort : Pour toutes matrice $A \in \mathcal{M}_{m,n}(\mathbb{Z}_p)$, $P \in \mathcal{GL}_n(\mathbb{Z}_p)$ et $Q \in \mathcal{GL}_m(\mathbb{Z}_p)$ on a $v_k(A) = v_k(PAQ)$.

En effet, soient $A \in \mathcal{M}_{m,n}(\mathbb{Z}_p)$, $P \in \mathcal{M}_n(\mathbb{Z}_p)$ et $Q \in \mathcal{M}_m(\mathbb{Z}_p)$. On a l'inégalité suivante par invariance de v_k par transposition :

$$v_k(PAQ) \leq v_k(PA) = v_k\left((PA)^T\right) = v_k(A^T P^T) \leq v_k(A).$$

Puis de même $v_k(A) = v_k(P^{-1}(PAQ)Q^{-1}) \leq v_k(PAQ)$.

En appliquant ce résultat à M et S on a que pour tout $1 \leq k \leq \max(m, n)$ $v_k(M) = v_k(S)$, or par définition de S, $v_k(S) = a_1 + a_2 + \ldots + a_r$ si $k \leq r$ et 0 sinon. D'où le résultat.

□

C Résolution de la programmation linéaire p-adique

Cette section présente le pseudo-code ainsi qu'une implémentation en SageMathde l'algorithme de la section 3.1.

Ou FormeNormaleDeSmith renvoie la forme normale de Smith de la matrice A ainsi que les matrices P et Q telles que .

stick to a convention

L'algorithme s'exécute en $O\left(n^3\right)$

Références

[Mon58] A. F. Monna. « Ensembles convexes dans les espaces vectoriels sur un corps valué ». fr. In : *Indagationes Mathematicae (Proceedings)* 61 (jan. 1958), p. 528-539. ISSN : 1385-7258. DOI : 10.1016/S1385-7258(58)50076-6. URL : https://www.sciencedirect.com/science/article/pii/S1385725858500766 (visité le 12/07/2023).

Algorithm 1 Résolution de la programmation p-adique

Entrée : Une matrice A de taille $m \times n$, un vecteur b de taille m et un vecteur c de taille n.
Sortie : Le maximum des $\mathrm{val}_p(\langle c, x\rangle)$ tels que $Ax + b \geq 0$.

S, P, Q = FormeNormaleDeSmith(A)
r = rang(S)
$b' = Q \times b$
$c' = P^T \times c$
pour i allant de $r+1$ à m
  si $\mathrm{val}_p(b'[i]) < 0$ **alors**
    Échec : Pas de solution
  fin si
fin pour
pour i allant de $r+1$ à n
  si $c'[i] \neq 0$ **alors**
    Échec : Le problème n'est pas borné
  fin si
fin pour
$\tilde{c}$ =Projection($c', 1, r$) ▷ On réduit le problème à un problème de taille r
$\tilde{b}$ = Projection($b', 1, r$)
$\tilde{S}$ =SousMatrice($S, (1, r), (1, r)$)
$\lambda = \tilde{c}.S^{-1}.\tilde{b}$
$v = \min\left\{\mathrm{val}_p(z_i) \mid (z_1, \ldots, z_r) = \tilde{c}.S^{-1}\right\}$
si $\mathrm{val}_p(\lambda) < v$ **alors return** $\mathrm{val}_p(\lambda)$
sinonreturn v ▷ Si l'on cherche à calculer la valuation maximale à la place il suffit d'échouer au lieu de renvoyer v.
fin si

[PK97] Lorant Porkolab et Leonid Khachiyan. « On the complexity of semidefinite programs ». In : *Journal of Global Optimization* 10.4 (1997), p. 351-365.

[Ram97] Motakuri V Ramana. « An exact duality theory for semidefinite programming and its complexity implications ». In : *Mathematical Programming* 77 (1997), p. 129-162.

[Gou03] Fernando Q. Gouvêa. *P-adic numbers : an introduction*. eng. Second edition.. Universitext. Berlin, Heidelberg : Springer-Verlag, 2003. ISBN : 978-3-540-62911-5.

[De 06] Etienne De Klerk. *Aspects of semidefinite programming : interior point algorithms and selected applications*. T. 65. Springer Science & Business Media, 2006.

[HNE16] Didier Henrion, Simone Naldi et Mohab Safey El Din. « Exact algorithms for linear matrix inequalities ». In : *SIAM Journal on Optimization* 26.4 (2016), p. 2512-2539.

[Car17] Xavier Caruso. *Computations with p-adic numbers*. arXiv :1701.06794 [cs, math]. Jan. 2017. DOI : 10.48550/arXiv.1701.06794. URL : http://arxiv.org/abs/1701.06794 (visité le 06/07/2023).