Rapport de stage L3

Sous la supervision de Tristan Vaccon et Simone Naldi

Corentin Cornou

25 juillet 2023

Table des matières

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 $\mathbb{R}^s$ $S = \{(x_1, \dots, x_s) \in \mathbb{R}^s | A_0 + x_1A_1 + \dots + x_sA_s \succeq 0\}$.

image + exemple

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* (Figure 1). Le spectraèdre S est souvent appélé *samosa* et peut être obtenu comme *dérivée au sens de Renegar* du tetraèdre régulier [San13]. 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).

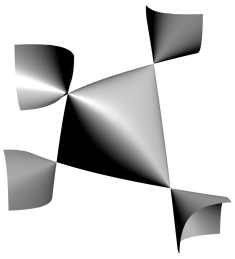

FIGURE 1 – Cubique de Cayley

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 appélé *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 coéfficients), 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 :

$$z = a_0 + a_1p + \ldots + a_np^n + \ldots$$

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.

exemple d'opérations dans $\mathbb{Q}_p$

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

les personne habitués pourrait y voir une analogie avec la contruction de R[[X]

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

Petit paragraphe introducif

On définit la valuation p-adique dans $\mathbb{Z}$ $\text{val}_p^{\mathbb{Z}} : \mathbb{Z} \to \mathbb{N} \cup \{+\infty\}$ 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 $\text{val}_p^{\mathbb{Q}} : \mathbb{Q} \to \mathbb{Z} \cup \{+\infty\}$ en définissant pour tout $r \in \mathbb{Q}$ $\text{val}_p^{\mathbb{Q}}(r) = \text{val}_p^{\mathbb{Z}}(a) - \text{val}_p^{\mathbb{Z}}(b)$ 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 $\text{val}_p : \mathbb{Q}_p \to \mathbb{Z} \cup \{+\infty\}$ 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, $\text{val}_p(\ldots 2413000) = 3$ et $\text{val}_p(\ldots 251, 24) = -2$.

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 . À cet effet on introduira la notation suivante :

i.e.

Notation. Pour tout élément $x \in \mathbb{Q}_p$, on dit que x est *positif* et on note $x \geq 0$ si $\text{val}_p(x) \geq 0$. 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 $x \geq y \Rightarrow x - y \geq 0$ [1].

1. Par exemple, $\text{val}_p(\ldots 11, 11) \geq \text{val}_p(\ldots 00, 01)$ mais $\text{val}_p(\ldots 11, 11 - \ldots 00, 01) = \text{val}_p(\ldots 11, 1) < 0$

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

1. $\mathrm{val}_p(x+y) \geq \min\left(\mathrm{val}_p\left(x\right), \mathrm{val}_p\left(y\right)\right)$
2. $\mathrm{val}_p\left(xy\right) = \mathrm{val}_p(x) + \mathrm{val}_p(y)$

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 [2] 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 $\mathbb{Q}_p$.

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

i. $x \in \mathbb{Z}_p$
ii. $\mathrm{val}_p\left(x\right) \geq 0$
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 $\mathrm{val}_p\left(x\right) \geq 0$ c'est-à-dire $i. \Leftrightarrow ii.$.

2. c'est-à-dire tel que $\mathbb{N}$ est borné dans $\left(\mathbb{Q}_p, |\cdot|_p\right)$

3 Polyèdres convexes p-adiques

Notation. Pour toute matrice M à coefficient dans $\mathbb{Q}_p$ on note $M \geq 0$ et on dit que M est *positive* si tous les coefficients de M sont positifs, c'est à dire si $M \in M_n(\mathbb{Z}_p)$. On infère également les notation $M \leq 0$, $M > 0$ et $M < 0$.

3.1 Matrices symétriques positive

Définition 8. On note $\mathcal{P}_n(\mathbb{Q}_p)$ l'ensemble des matrices symétriques dont tous les mineurs principaux ont une valuation positive.

Rappel. Un élément de $\mathbb{Q}_p$ a une valuation positive si et seulement si il est élément de $\mathbb{Z}_p$.

Propriété 5. $\mathcal{P}_n(\mathbb{Q}_p) = \{M \in S_n(\mathbb{Q}_p) \mid$ les mineurs principaux de M sont à valeur dans $\mathbb{Z}_p\}$.

Preuve : découle directement du rappel précédent.

Proposition 1.

$$\mathcal{P}_n(\mathbb{Q}_p) = S_n(\mathbb{Z}_p).$$

Remarque. On remarque alors que l'ensemble $\mathcal{P}_n$ correspond aux matrices symétriques à coefficients positifs.

Preuve :

Le déterminant étant une fonction polynomiale en les coefficients de la matrice, toute matrice de à coefficient dans $\mathbb{Z}_p$ a un déterminant à valeur dans $\mathbb{Z}_p$. D'où, par la propriété 2, $S_n(\mathbb{Z}_p) \subset \mathcal{P}_n(\mathbb{Q}_p)$.

L'inclusion réciproque se montre par récurrence. On note pour tout $n \in \mathbf{N}$ $\mathcal{H}_n : \mathcal{P}_n(\mathbb{Q}_p) \subset S_n(\mathbb{Z}_p)$.

On notera $\Delta_{i_1,\ldots,i_n}(M)$ le mineur principal de M composé des lignes et des colonnes d'indices $i_1, \ldots, i_n \in \{1, \ldots, n\}$ pour tout matrice M. On notera d'ailleurs simplement $\Delta_{i_1,\ldots,i_n}$ lorsque le contexte est explicite.

Les cas $n = 0$ et $n = 1$ se démontrent sans difficultés aucunes. Montrons le cas $n = 2$ qui servira par la suite.

Soit $M \in \mathcal{P}_2(\mathbb{Q}_p)$, M s'écrit $M = \begin{pmatrix} \alpha & \gamma \\ \gamma & \beta \end{pmatrix}$, avec $\alpha, \beta, \gamma \in \mathbb{Q}_p^3$.

On sait alors que $\alpha = \Delta_1$ et $\beta = \Delta_j$ sont des entiers p-adiques, il suffit de montrer que γ en est également un. Pour ce faire supposons que $\mathrm{val}_p(\gamma) < 0$, on a alors $\mathrm{val}_p(\gamma^2) = 2\mathrm{val}_p(\gamma) < \mathrm{val}_p(\alpha\beta)$ et on en déduit $\mathrm{val}_p(\Delta_{1,2}) = \min(\mathrm{val}_p(\alpha\beta), 2\ \mathrm{val}_p(\gamma)) = 2\mathrm{val}_p(\gamma) < 0$ ce qui contredit la positivité de $\Delta_{1,2}$ et est donc absurde. On conclut alors que $\gamma \in \mathbb{Z}_p$ et $M \in S_n(\mathbb{Z}_p)$. On a montré $\mathcal{H}_2$.

Soit $n \in \mathbf{N}$ tel que la propriété $\mathcal{H}_n$ soit vérifiée et M une matrice de $\mathcal{P}_n(\mathbb{Q}_p)$.

M s'écrit

$$M = \left(\begin{array}{ccc|c} & & & \beta_1 \\ & M' & & \vdots \\ & & & \beta_n \\ \hline \beta_1 & \cdots & \alpha_n & \alpha_{n+1} \end{array}\right)$$

avec $M' \in S_n(\mathbb{Q}_p)$ et $\beta_1, \ldots, \beta_n, \alpha_{n+1} \in \mathbb{Q}_p$.

On note $\alpha_1, \ldots, \alpha_n$ les coefficients diagonaux de M' qui sont des entiers p-adique par hypothèse de récurrence.

Par définition $\alpha_{n+1} = \Delta_{n+1}$ est un entier p-adique. Puis on se ramène au cas $n = 2$ en utilisant le fait que pour i=1,..., n, $\Delta_{i,n+1} = \begin{vmatrix} \alpha_i & \beta_i \\ \beta_i & \alpha_{n+1} \end{vmatrix}$ et on en déduit que $\beta_i \in \mathbb{Z}_p$ pour $i = 1, \ldots, n$. On conclut en appliquant l'hypothèse de récurrence à M'.

□

Remarque. La preuve de la proposition précédente montre qu'il suffit en réalité que les mineurs principaux de taille au plus 2 aient une valuation positive (ou soient éléments de $\mathbb{Z}_p$) ce qui correspond à la définition de matrice semi-définie positive sur le semi-corps tropical développée par Allamigeon, Gaubert et Skorma dans [AGS20] . Ce n'est toutefois pas la définition qui sera choisie ici, pour des raisons développées en partie 1.2.

Propriété 6. $\mathcal{P}_n(\mathbb{Q}_p)$ est un anneau.

Preuve : Par la propriété précédente $\mathcal{P}_n(\mathbb{Q}_p) = S_n(\mathbb{Z}_p)$ comme intersection des anneaux $M_n(\mathbb{Q}_p)$ et $S_n(\mathbb{Q}_p)$.

Propriété 7. L'ensemble $\mathcal{P}_n(\mathbb{Q}_p)$ 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 $\mathbb{Z}_p$ et $S_n(\mathbb{Q}_p)$.

$\mathcal{P}_n(\mathbb{Q}_p)$ 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 $\mathcal{P}_n(\mathbb{Q}_p)$ est assez triviale et pour $S_n^+(\mathbb{Q}_p)$ elle est laissée en exercice au lecteur

3.2 Polyèdres convexes p-adiques

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

Soit P un polyèdre convexe et $\mathcal{L}$ un plan affine tel que $P = \mathcal{P}_n(\mathbb{Q}_p) \cap \mathcal{L}$, et dont on note s la dimension de l'espace vectoriel associé. On dispose de donc de $s+1$ matrices $M^0, M^1, \ldots, M^s$ telles que $\mathcal{L} = M^0 + \text{Vect}\left(M^1, \ldots, M^s\right)$. Le polyèdre P s'écrit alors $P = \left\{M^0 + x_1 M^1 + \ldots + x_s M^s \geq 0\right\}$. On identifie alors souvent P avec $\left\{(x_1, \ldots, x_s) \in \mathbb{Q}_p^s | M^0 + x_1 M^1 + \ldots + x_s M^s \geq 0\right\}$ ce qui permet d'écrire qu'un vecteur $x_1, \ldots, x_s$ de $\mathbb{Q}_p^s$ est élément de P si et seulement si il vérifie :

$$\forall i, j \ M^0_{i,j} + x_1 M^1_{i,j} + \ldots + M^s_{i,j} \geq 0 \tag{1}$$

On peut alors réécrire l'inégalité matricielle en $P = \left\{x \in \mathbb{Q}_p^s | Ax + b \geq 0\right\}$ avec

$$A = \begin{pmatrix} M^1_{1,1} & \ldots & M^s_{1,1} \\ \vdots & & \vdots \\ M^1_{n,n} & \ldots & M^s_{1,1} \end{pmatrix} \in M_{n^2,s}(\mathbb{Q}_p) \text{ et } b = \begin{pmatrix} M^0_{1,1} \\ \vdots \\ M^0_{n,n} \end{pmatrix} \in M_{n^2,1}(\mathbb{Q}_p).$$

Remarque. On peut réduire de moitié la tailles des matrices A et b en considérant que les coefficients diagonaux et supradigonaux des M^i pour $i = 0, 1, \ldots, n$. Ce qui permet de se ramener à des matrices équivalente [3] avec $\frac{n(n+1)}{2}$ lignes.

En mettant sous cette forme le polyèdre on reconnait alors aisément que le problème de minimiser une application linéaire sur un polyèdre correspond exactement à résoudre le problème de la *Programmation linéaire*.

Remarque. On se ramène au cas quelconque du problème de la *Programmation linéaire* (taille quelconque et non seulement avec un nombre de ligne en $\frac{n(n+1)}{2}$ ou n^2) en annulant des coefficients $M^k_{i,j}$ pour tout $i = 1, \ldots, n$.

Propriété 8. Un polyèdre p-adique convexe est convexe au sens de [Mon58].

Preuve : Provient immédiatement du fait qu'un polyèdre s'écrit comme intersection d'ensemble convexe.

Exemple. La boule unité pour la norme infinie est un polyèdre. En effet, considérons le polyèdre défini par l'intersection de $S_n(\mathbb{Q}_p)$ avec le plan linéaire induit par les matrices E_k, k=1...n, de $S_n(\mathbb{Z}_p)$ telles que le seul coefficient non nul de E_k soit le k-ième coefficient diagonal lequel est égal à 1 . On observe que pour tout $x_1, \ldots, x_n \in \mathbb{Q}_p^n$, $\sum x_k E_k \geq 0$ si et seulement si $x_1, \ldots, x_s \in \mathbb{Z}_p^n$ i.e. si et seulement si $\|(x_1, \ldots, x_n)\|_\infty \leq 1$.

3.3 Résolution p-adique de la programmation linéaire

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.

3. puisque les inéquations de 1 impliquant le couple (i, j) $i > j$ sont redondantes avec les équations impliquant (j, i)

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 $O(n^3)$ 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.

vérifier que c'est améliorable

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 :

$$\begin{array}{c}\text{Minimiser } |c.x|_p \text{ tel que} \\ Ax + b \geq 0\end{array} \tag{PLp}$$

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

Pour toute matrice $M \in \mathcal{M}_{m,n}(\mathbb{Q}_p)$ il existe une unique matrice S de $\mathcal{M}_{m,n}(\mathbb{Q}_p)$ diagonale, dont les coefficients sont triés par valuation croissante et telle que

$$M = P^{-1}SQ$$

avec $P \in \mathcal{GL}_m(\mathbb{Z}_p)$ et $Q \in \mathcal{GL}_n(\mathbb{Z}_p)$. La matrice S est appelée forme normale de Smith de M.

donner 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 :

$$\begin{array}{c} \text{Minimiser } |c'.y|p \text{ tel que} \\ Sy + b' \geq 0 \end{array} \qquad \text{(PLp')}$$

où $b' = Pb$, $c' = cQ$, S est la forme normale de Smith de A et $A = PSQ$ 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 $y^* := Q^{-1}x$ est une solution admissible de PLp'
2. PLp' possède des solutions admissible si et seulement si les $m - r$ coefficients de Pb 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 9.

- 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 :

$$\forall 1 \leq i \leq r y_i \in -\frac{b'_i}{s_i} + \frac{1}{s_i}\mathbb{Z}_p \qquad (2)$$

Résoudre PLp' revient donc à minimiser $|c'.y|_p$ sur Adm. L'image de Adm par $y \mapsto c'y$ 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 :

$$c'Adm = \lambda_0 + p^{v_0}\mathbb{Z}_p$$

où $\lambda_0 = \sum_{i=1}^{r} -c'_i.\frac{b'_i}{s_i}$ et $v_0 = \min_{1\leq i\leq r} \mathrm{val}_p \frac{c'_i}{s_i}$.

Ainsi, deux cas apparaissent. Soit $\mathrm{val}_p(\lambda_0) < v_0$ auquel cas le minimum de $y \mapsto |c'.y|_p$ sur Adm est atteint en n'importe quel point de Adm et vaut $|\lambda_0|_p$.

Soit $\mathrm{val}_p(\lambda_0) \geq v_0$, auquel cas $\lambda_0 \in p^{v_0}\mathbb{Z}_p$ et le minimum vaut p^{-v_0} et est atteint en tous les points y de Adm tels que $\mathrm{val}_p\left(\sum_{1\leq i\leq r} y_i\right) = v_0$.

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 spectrale 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, se par le 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 $\mathbb{Q}_p$.

4.1 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 $\mathbb{Q}_p$ □.

4. notez l'absence du mot symétrique

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.

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 .

Propriété 10. 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 le LIEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEN0

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

Preuve : Le polynôme caractéristique d'une matrice à coefficients dans $\mathbb{Z}_p$ étant à coefficient dans $\mathbb{Z}_p$ on obtient le résultat par la propriété 10 .

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

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

Propriété 11. L'ensemble $S_n^+(\mathbb{Q}_p)$ 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 $\|.\|_\infty : P = \sum_{k=1}^n a_k X^k \to \sup |a_k|_p$.

Soit $P \in \mathbb{Z}_p[X]$. On peut alors montrer que la boule ouverte de centre P et de rayon 1 est incluse dans $\mathbb{Z}_p[X]$. Pour ce faire on considère $Q \in B_o(P,1)_\infty$ et on remarque que cela signifie que $\|Q-P\|_\infty \leq 1$ c'est-à-dire $Q-P \in \mathbb{Z}_p[X]$. On a donc $Q = P + P - Q \in \mathbb{Z}_p[X]$. $\mathbb{Z}_p[X]$ est donc ouvert.

Maintenant soit $P \in \mathbb{Q}_p[X]^c$ et $Q \in B_o(P,1)$. On note $P = \sum_{k=1}^n a_k X^k$ et $Q = \sum_{k=1}^n a_k X^k$. On dispose alors de $iin\{1,\dots,n\}$ tel que $|a_i|_p > 1$ et $a_i + b_i \in \mathbb{Z}_p$ (car $P - Q \in \mathbb{Z}_p$). Donc on a nécessairement $|b_i|_p = |a_i|_p > 1$ et $Q \in Z_p[X]^c$. Donc $\mathbb{Z}_p[X]^c$ est ouvert et $\mathbb{Z}_p[X]$ est fermé.

On montre alors *i.* et *ii.* grâce à $\mathcal{P}_n(\mathbb{Q}_p) = \chi^{-1}(\mathbb{Z}_p[X])$ 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 $M_i' = \mathrm{diag}(M_i, 0, \dots, 0)$.

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 $C = \{x \in \mathbb{Q}_p | a \leq \mathrm{val}_p(x) \leq b\}$ pour $a < b$ deux réels positifs fixés.

expliquer pourquoi

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

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

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 10 on a que $M(x,y)$ est semi-définie positive si et seulement si $\begin{cases} p^a x \geq 0 \\ p^{-b} y \geq 0 \\ \mathrm{Tr} M'(x,y) = 0 \geq 0 \\ \det M'(x,y) = p^{-2}(xy-1) \geq 0 \end{cases}$ c'est à dire si et seulement si $beg \begin{cases} \mathrm{val}_p(x) \geq a \\ \mathrm{val}_p(y) \geq -b \\ p^{-2}(xy-1) \geq 0 \end{cases}$ Or $x \in C$ si et seulement si il existe $y \in \mathbb{Q}_p$ tel que (x,y) vérifient 4.3. En effet, si x, y vérifient 4.3alors $\mathrm{val}_p(x) \geq a$, $\mathrm{val}_p(y) \geq -b$ et $p^{-2}(xy-1) \geq 0$ implique que $\mathrm{val}_p(x) + \mathrm{val}_p(y) = \mathrm{val}_p(xy) = \mathrm{val}_p(-1) = 0$ et donc que $\mathrm{val}_p(x) = -\mathrm{val}_p(y) \leq -(-b) = b$, donc $x \in$. Puis réciproquement si $x \in C$ alors (x, x^{-1}) vérifient 4.3 .

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).

[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.

[San13] Raman SANYAL. « On the derivative cones of polyhedral cones ». In : *Advances in Geometry* 13.2 (2013), p. 315-321. DOI : doi:10.1515/advgeom-2011-051. URL : https://doi.org/10.1515/advgeom-2011-051.

[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).

[AGS20] Xavier ALLAMIGEON, Stéphane GAUBERT et Mateusz SKOMRA. « Tropical spectrahedra ». In : *Discrete & Computational Geometry* 63.3 (avr. 2020). arXiv :1610.06746 [math], p. 507-548. ISSN : 0179-5376, 1432-0444. DOI : 10.1007/s00454-020-00176-1. URL : http://arxiv.org/abs/1610.06746.

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.

Démonstration. Proposition 3 □

Démonstration. Propriété 4

□

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 3.3

Propriété 12. Il existe une unique matrice 0

Démonstration. i □

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 3.3.

stick to a convention

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

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

Algorithm 1 Résolution de la programmation p-adique

$S, P, Q = \text{FormeNormaleDeSmith}(A)$
$r = \text{rang}(S)$
$b' = P \times b$
$c' = c \times Q$
pour i allant de $r+1$ à m
  si $\text{val}_p(b'[i]) < 0$ **alors**
    Pas de solution
  fin si
fin pour
pour i allant de $r+1$ à n
  si $c'[i] \neq 0$ **alors**
    Le problème n'est pas borné
  fin si
fin pour
$\tilde{c} = \text{Projection}(c', 1, r)$ ▷ On réduit le problème à un problème de taille r
$\tilde{b} = \text{Projection}(b', 1, r)$
$\tilde{S} = \text{SousMatrice}(S, (1, r), (1, r))$
$\lambda_0 = \tilde{c}.S^{-1}.\tilde{b}$
$v_0 = \min\left\{\text{val}_p(z_i) \mid (z_1, \ldots, z_r) = \tilde{c}.S^{-1}\right\}$
si $\text{val}_p(\lambda_0) < v_0$ **alors return** $\text{val}_p(\lambda_0)$
sinonreturn v_0 ▷ Si l'on cherche à calculer la valuation maximale à la place il suffit de soulever une erreur au lieu de renvoyer v_0.
fin si