Vers les Spectraèdres p-adiques, définition et propriétés algorithmiques

Corentin Cornou

Sous la supervision de Tristan Vaccon et Simone Naldi

Abstract

Les spectraèdres sont une des généralisations les plus communes et utilisées des polyèdres. Ce sont des ensembles réels convexes définis comme les ensembles de matrices linéaires $A(x) = A_0 + x_1 A_1 + \ldots + x_s A_s$ qui sont symétriques définies positives, avec $x = (x_1, \ldots, x_s)$ parcourant $\in \mathbb{R}^s$ et $A_0, A_1, \ldots, A_s$ des matrices symétriques réelles fixées. Ils sont d'une grande importance en optimisation car au cœur de la programmation semi-définie, une généralisation de la programmation linéaire visant à minimiser une forme linéaire sur un spectraèdre au lieu et en place d'un polyèdre convexe. Ainsi, une large variété de problèmes peuvent se réduire à la programmation semi-définie. En effet, aux nombreuses applications de la programmation linéaire (problème de la coupe maximale, nombreuses applications en finance, médecine, dans l'industrie...) s'ajoutent des problèmes plus spécifiques dont un certain nombre est par exemple présentés dans [VB99]. Si les spectraèdres ont été largement étudiés dans le cas réel, en 2016 Allamigeon, Gaubert et Skomra ont ouvert la voie à l'étude des spéctraèdres sur les corps non-archimédien dans [AGS20] en définissant les spectraèdres tropicaux.

L'objectif de ce stage était alors d'essayer de trouver une définition de spectraèdre générale sur les corps non-archimédien. (Rappelons qu'un corps (valué) non-archimédien est un corps muni d'une valeur absolue [1] $|\cdot|$ vérifiant l'inégalité non-archimédienne : pour tous $x, y \in \mathbb{K}\, |x+y| \leq \max(|x|, |y|)$). En s'appuyant, pour ce faire, sur les corps p-adiques. Un corps p-adique $\mathbb{Q}_p$ étant un ensemble de nombres définis par les sommes formelles $x = \ldots + x_k p^k + \ldots + x_1 p + x_0 + x_{-1} p^{-1} + \ldots x_n p^n$ avec $n \in \mathbb{Z}$ et où les $(x_k)_{k \geq m}$ sont éléments de $\{0, \ldots, p-1\}$, pour p un nombre premier fixé. On peut munir ces corps de la valuation p-adique $\mathrm{val}_p(x) = \sup\{i \geq m | x_i \neq 0\}$ qui définit une valeur absolue non-archimédienne $|\cdot|_p : x \mapsto p^{-\mathrm{val}_p(x)}$.

Ce rapport propose une définition de spectraèdre sur les corps p-adiques. Pour ce faire, on introduira une nouvelle notion, celle de matrice semi-définie positive. Une matrice à coefficients p-adiques étant semi-définie positive si et seulement si les racines de son polynôme caractéristiques sont de valuation positive. Ce qui permet de définir les spéctraèdres comme les matrices linéaires $A(x) = A_0 + x_1 A_1 + \ldots x_s A_s$ semi-définies positives avec $x = (x_1, \ldots, x_s)$ parcourant $\mathbb{Q}_p^s$ et $A_0, \ldots, A_s$ quelconques fixées. On peut alors en déduire le principal résultat découvert lors de ce stage : les couronnes p-adiques sont des projections de spectraèdres. De plus, ce rapport définit les polyèdres p-adiques comme les ensembles de points $x \in \mathbb{Q}_p^s$ définis par inégalités de la forme $\mathrm{val}_p(\ell_1(x)) \geq 0, \ldots, \mathrm{val}_p(\ell_n(x)) \geq 0$ pour $\ell_1, \ldots, \ell_n$ des formes linéaires p-adiques. Ainsi, si le temps a manqué pour proposer des résultats sur la résolution de la programmation semi-définie positive p-adique, il sera toute fois présenté un algorithme résolvant la programmation linéaire en $O\left(\max(m,n)^2\right)$, où m et n sont les dimension de la matrice de contraintes. De plus, des pistes pour la résolution du problème LMI (*Linear Matrix Inequality*) p-adique visant à déterminer la vacuité ou non d'un spectraèdre sont également évoquées.

1. une valeur absolue sur un corps est une norme sur ce même corps compatible avec le produit.

Table des matières

1 Introduction

Les spectraèdres se présentent comme une généralisation des polyèdres, définis comme les points $x = (x_1, \ldots, x_s)$pour lesquels une matrice linéaire $A(x) = A_0 + x_1 A_1 + \ldots + x_s A_s$ est symétrique semi-définie positives, avec $A_0, \ldots, A_s$ des matrice symétriques. Ils sont d'une grand utilité en optimisation car ils permettent de résoudre non seulement des problèmes d'optimisation linéaire mais également d'autres plus spécifiques. En effet, une sur-classe des problèmes de programmation linéaire, les problèmes de programmation semi-définie consiste à maximiser une application linéaire sur un spectraèdre.

Si ces objets ont été largement étudiés dans le cadre réel, une voie vers leur étude dans des corps non archimédiens s'est récemment ouverte dans [AGS20]. C'est ce que ce rapport étudie dans le cadre des corps p-adiques, corps non-archimédiens qui peuvent être vus comme des extensions du coprs $\mathbb{Q}$ des rationnels autres que le corps des réels et dans lesquels les techniques traditionnelles ne marchent pas. Ainsi, le produit scalaire n'est en p-adique pas une forme bilinéaire particulièrement distinguée, ce qui annule tout bénéfice de la symétrie et le corps p-adique $\mathbb{Q}_p$ n'est de plus pas algébriquement clos. Il a donc fallu trouver une nouvelle définition de matrice semi-définie positive. Celle choisie ici est celle des matrices dont la valuation p-adique des valeurs propres est positive dans la clôture de $\mathbb{Q}_p$. On en déduit alors aisément une définition de spectraèdre p-adique et prouve qu'avec cette dernière les couronnes p-adiques sont des projetés de spectraèdre.

Ce rapport commence par décrire le déroulement du stage. Suite à quoi, les spectraèdres sont définis et quelques unes de leur propriétés décrites. Puis, suit une présentation élémentaire des corps p-adiques. Ensuite, les polyèdres seront définis dans le cas p-adique, et un algorithme résolvant le problème de la programmation linéaire sera décrit. Enfin, on y construira une définition des spectraèdre p-adiques, basé sur la nouvelle définition de matrice semi-définie positive après avoir brièvement discuté des clôtures algébriques des corps p-adiques. Ultimement, on prouvera que les couronnes p-adiques s'écrivent comme ombre de spectraèdre et y adjoindra d'éventuelle piste pour l'étude des propriétés algorithmiques des spectraèdre nouvellement définis.

2 Méta-informations

Cette courte section dévoile quelques informations non-scientifique sur le déroulement du stage.

Pour les activités non liées aux stage de façon immédiate, j'ai pu lors de mon séjour participer à 2 repas organisés respectivement par le laboratoire et par le département dans lequel je me trouvais et j'ai également assisté à deux conférences données sur place, une par mon encadrant Tristan Vaccon et une seconde par un intervenant extérieur. De plus, je mangeais régulièrement avec les chercheurs.

Je disposais d'un bureau dans une salle que je partageais avec 3 autres stagiaires [2]. Il était convenu d'un rendez-vous hebdomadaire afin de discuter des mes avancées ou de mes doutes et interrogations. Cependant, en cas de

2. tous fort sympathiques

questionnement je pouvais contacter directement mes encadrants qui étaient présents une majeure partie de la journée.

Le stage a approximativement suivie le déroulement suivant :

La première semaine a été passée à se documenter sur les corps p-adiques. La deuxième et la troisième ont été consacrées alternativement à essayer de trouver une définition pertinente de spectraèdre p-adique. La quatrième a principalement servie à commencer l'écriture du rapport ainsi qu'à se documenter sur les spectraèdres et l'optimisation convexe afin de dresser des similarités entre spectraèdres réels et p-adiques. La cinquième et la sixième ont été utilisées afin de continuer ce rapport démontrer que les couronnes p-adiques étaient des spectraèdres et concevoir l'algorithme présenté en 5.2. L'ultime semaine semaine a permis de peaufiner quelques détails (preuves plus formelles, légères erreurs corrigées, etc.) et de continuer mon rapport de stage. Cependant cette dernière a été peu productive car je devais préparer mon départ et je suis tombé malade (de manière totalement indépendante).

Enfin, je tiens à remercier chaleureusement mes encadrants Tristan Vaccon et Simone Naldi pour, entre autres, leur disponibilité, leurs conseils et leur patience. Mes camarades de bureaux Léo et Lucile qui ont su égayer le bureau ainsi que Abdu Razik pour sa participation à [Roz21].

3 Spectraèdres réels

Cette section consiste en une introduction très brève à la notion de spectraèdre réel. Elle n'offre au lecteur que l'outillage nécessaire à la bonne compréhension de l'objet en vue de son adaptation aux corps p-adiques, en insistant toutefois sur son usage en optimisation. On ne pourra que conseiller la lecture de [GPR12] pour des approfondissements.

3.1 Définition et premières propriétés

Définition 3.1.1. On appelle *matrice symétrique semi-définie positive* toute matrice réelle symétrique 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 permet de s'assurer d'obtenir des valeurs propres réelles grâce au théorème spectral, demander leur positivité fait alors sens.

Propriété 3.1.2. L'ensemble $\mathcal{S}_n^+(\mathbb{R})$ est un cône convexe fermé.

Définition 3.1.3. On appelle *spectraèdre* l'intersection de $\mathcal{S}_n^+(\mathbb{R})$ avec un espace affine $\mathcal{L}$ de $\mathcal{S}_n(\mathbb{R})$, l'ensemble des matrices symétriques de taille n sur $\mathbb{R}$.

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 célèbre de spectraèdre est l'ensemble des matrices symétriques semi-définies 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 appelée *cubique de Cayley* (1). Les quatre 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 sur la frontière du spectraèdre, avec au moins une valeur propre négative autrement) ; enfin, les matrices à l'intérieur du spectraèdre sont définies positives (toutes valeurs singulières strictement positives).

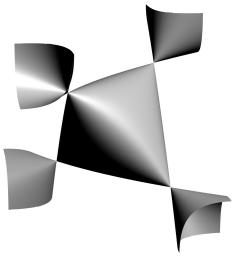

FIGURE 1 – Cubique de Cayley

3.2 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 $x \mapsto \langle c, x \rangle := c_1 x_1 + \cdots + c_s x_s$ le produit scalaire Euclidien. Le problème d'admissibilité associé au problème d'optimisation (PSD), c'est-à-dire, la question si le spectraèdre $S = \{(x_1, \ldots, x_s) \in \mathbb{R}^s | A_0 + x_1 A_1 + \ldots + x_s A_s \succeq 0\}$ 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 $D \succeq 0$.

4 Introduction aux nombres p-adiques

On se contentera dans cette section d'une description très élémentaire de 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 inspirée du cours de Xavier Caruso [Car17] que l'on invite d'ailleurs à aller consulter pour une vision plus complète mais très largement compréhensible des corps p-adiques.
Notation. On considère pour tout ce rapport p un nombre premier.

4.1 Entiers p-adique

Définition 4.1.1. Entier p-adique
On appelle *entier p-adique* la somme formelle :

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

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

Remarques.

- L'ensemble des entiers p-adiques est noté $\mathbb{Z}_p$.
- 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 $\sum_{i=0}^{\infty} (i \bmod p) p^i = \overline{\ldots 210(p-1)\ldots 210}^p$ sont des entiers p-adiques parfaitement définis bien que ne convergeant pas dans le cas réel.

Propriété 4.1.2. $\mathbb{Z}_p$ peut être muni d'une structure d'anneau commutatif intègre en lui adjoignant l'addition terme à terme avec retenue et la multiplication avec retenue.

Exemple. Par exemple dans $\mathbb{Z}_5$

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

FIGURE 2 – Exemples d'opérations dans $\mathbb{Z}_5$

Proposition 4.1.3. L'anneau $\mathbb{Z}$ des entiers relatifs s'identifie naturellement à un sous-anneau de $\mathbb{Z}_p$.

Remarque. Si l'on a vu les entiers relatifs sont des entiers p-adiques, certains entiers p-adiques 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 $\mathbb{Z}_p$.

4.2 Nombres p-adiques

Définition 4.2.1. Nombres p-adiques
On définit l'ensemble $\mathbb{Q}_p$ des *nombres p-adiques* comme $\mathbb{Z}_p\left[\frac{1}{p}\right]$.

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 courramment $x = \overline{\ldots x_i \ldots x_1 x_0, x_{-1} \ldots x_k}^p$.

Remarque. Le lecteur habitué à travailler dans $R[[X]]$ verra dans la construction de $\mathbb{Q}_p$ à partir de $\mathbb{Z}_p$ une ressemblance avec le passage de $R[[X]]$ à $\mathbb{R}(X)$. De nombreuses autres similitudes entres ces ensembles peuvent être trouvées mais nous éviterons de les évoquer afin de rester à un niveau élémentaire.

Propriété 4.2.2. $\mathbb{Q}_p$ est un corps qui étend les opérations de $\mathbb{Z}_p$.

Preuve : Voir annexe.

Remarque. $\mathbb{Q}_p$ est même le corps des fractions de $\mathbb{Z}_p$. Ce qui établit une analogie claire avec la construction de $\mathbb{Q}$ à partir de $\mathbb{Z}$ et explique en partie les notations $\mathbb{Z}_p$ et $\mathbb{Q}_p$.

Corollaire 4.2.3. 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.

4.3 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 4.3.1. 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 la positivité dans un corps qui n'est pas totalement ordonnable [3]. 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 infère 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 $x \geq y \Rightarrow x - y \geq 0$ [4].

Propriété 4.3.2. 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 4.3.3. 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 4.3.2.

On observera en particulier que, d'après 4.3.2, 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 fait de $\mathbb{Q}_p$ un corps non archimédien [5] et rend la géométrie p-adique très différente du cas réel et peu intuitive si l'on y est pas habitué. 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 4.3.4. 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 $i. \Leftrightarrow ii.$.

3. i.e. il n'y a pas relation d'ordre $\geq$ sur $\mathbb{Q}_p$ compatible avec l'addition et telle que $\forall s \geq 0$ $x \geq y \Rightarrow sx \geq sy$.

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

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

5 Polyèdres convexes p-adiques

Cette partie contient les premières contributions apportées lors de ce stage, c'est-à-dire la définition des polyèdres p-adiques et un algorithme qui résout le problème de la programmation linéaire en p-adique.

5.1 Définition

Définition 5.1.1. On appelle *polyèdre convexe p-adique* toute partie de $\mathbb{Q}_p^s$ définie par des inégalités linéaire $\mathrm{val}_p(\ell_1(x)) \geq 0, \ldots, \mathrm{val}_p(\ell_n(x)) \geq 0$ pour $\ell_1, \ldots, \ell_n$ des formes linéaires et x parcourant $\mathbb{Q}_p^s$.

Exemple. La boule unité de $\mathbb{Q}_p^s$ pour la norme infinie est un polyèdre. En effet, la boule infinie s'écrit comme l'ensemble des points $(x_1, \ldots, x_s)$ tels que

$$\begin{pmatrix} x_1 & & & \\ & x_2 & 0 & \\ & 0 & \ddots & \\ & & & x_s/ \end{pmatrix} \geq 0.$$

En effet, la boule unité de $\mathbb{Q}_p^s$ est $\mathbb{Z}_p^s$.

5.2 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 réels, les techniques classiques de résolution de la programmation linéaire sont mises à mal. Il est en 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 est 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 présentées dans cette section, les preuves des résultats sont disponible en B.

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

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

avec x un vecteur de taille n parcourant $\mathbb{Q}_p^n$, 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 5.2.1. 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 $Q \in \mathcal{G}L_m(\mathbb{Z}_p)$.

Remarques.
i. Les coefficients de la forme normale de Smith sont uniques 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 valuations 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 5.2.2. 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 de Smith il vient que résoudre PLp équivaut 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 admissibles si et seulement si les $m - r$ coefficients de b' sont non nuls, où r le rang de S.
3. Si au moins un des $n - r$ derniers coefficients de c' est non nul PLp' n'est pas borné et n'admet donc pas de solution.

Propriété 5.2.3.

- 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 exactement les facteurs invariants de Smith non nuls. L'ensemble Adm des solutions admissibles 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 :

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

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 sur un polyèdre p-adique au lieu de la minimiser (ce qui revient à maximiser la valeur absolue) on pourra appliquer le même raisonnement. La seule différence est que si $\mathrm{val}_p(\lambda) < v$ le problème n'est pas borné et n'admet donc pas de solution.

6 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. Il contient la majeur partie de la contribution apportée lors de ce stage : les notions de matrice semi-définie positive et les propriétés et définitions concernant les spectraèdres p-adiques étant nouveaux. 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

exigée. 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 [6] 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 $\mathbb{Q}_p$.

6.1 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 aporté. On recommandera toutefois la lecture de la section 5 de [Gou03] pour plus d'informations sur les extensions de corps p-adiques.

Définition 6.1.1. 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 $\mathbb{K}$. Par exemple le corps des nombres complexes $\mathbb{C}$ est une extension du corps des nombres réels $\mathbb{R}$ qui est lui même une extension du corps $\mathbb{Q}$ des rationnels.

Définition 6.1.2. 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 $\mathbb{K}$.

Exemple. Le corps $\mathbb{C}$ est algébriquement clos.

Proposition 6.1.3. $\mathbb{Q}_p$ n'est pas algébriquement clos.

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

Définition 6.1.4. 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.

Exemple. $\mathbb{C}$ est la clôture algébrique de $\mathbb{R}$.

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 6.1.5. 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 est cependant pour des usage pratique complexe de travailler dans $\overline{\mathbb{Q}_p}$ qui est n'est pas une

6. On notera l'absence du mot symétrique

extension finie de $\mathbb{Q}_p$ [7]. On cherchera donc des caractérisations plus simples pour savoir si un polynôme est à racines positives, ce qui sera fait dans la prochaine section.

6.2 Matrices semi-définies positives

Définition 6.2.1. 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 (dans $\overline{\mathbb{Q}_p}$) .

On note $\mathcal{M}_n^+(\mathbb{Q}_p)$ l'ensemble des matrices semi-définies positives et $M \succeq 0$ le fait que $M \in \mathcal{M}_n^+(\mathbb{Q}_p)$.

Théorème 6.2.2. Caractérisation des matrices semi-définies positives

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

Preuve : Voir annexe.

Conséquence 6.2.3. $\mathcal{M}_n(\mathbb{Z}_p) \subset \mathcal{M}_n^+(\mathbb{Q}_p)$

Preuve : $\mathbb{Z}_p$ étant un anneau, le polynôme caractéristique d'une matrice à coefficients dans $\mathbb{Z}_p$ est à coefficient dans $\mathbb{Z}_p$. On conclut par 6.2.2 .

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 $M \in \mathcal{M}_2^+(\mathbb{Q}_5)$ or aucun des coefficients de M n'est dans $\mathbb{Z}_5$

Propriété 6.2.4. L'ensemble $\mathcal{M}_n^+(\mathbb{Q}_p)$ est :

i. ouvert

ii. fermé

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.

6.3 Spectraèdres p-adiques

Définition 6.3.1. On appelle *spectraèdre p-adique* l'intersection de $\mathcal{M}_n^+(\mathbb{Q}_p)$ avec un hyperplan affine $\mathcal{L}$ de $\mathcal{M}_n(\mathbb{Q}_p)$.

Remarque. De même que dans le cas réel on identifiera communément le spectraèdre engendré par l'hyperplan $\mathcal{L}$ avec sa préimage dans $\mathbb{Q}_p^s$ (i.e. l'ensemble des vecteurs $x \in \mathbb{Q}_p^s$ tels que la matrice linéaire $A(x) = A_0 + x_1 A_1 + \ldots + x_s A_s$ soit semi-définie positive avec $A_0, A_1, \ldots, A_s$ lui engendrent $\mathcal{L}$).

On peut alors en déduire la propriété suivante :

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

Propriété 6.3.2. Les polyèdres p-adique sont des spectraèdres p-adiques.

Preuve : La preuve est identique à celle du cas réel présentée en 3.2.

6.4 Couronnes p-adiques

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 semi-algébriques [8] convexes soient des ombres de spéctraèdres [HN08]. Bien que cette conjecture ait ensuite été réfutée par Schreider dans [Sch17] dans le cas réel elle a été prouvée vraie pour les spectraèdres tropicaux [AGS19], il n'en reste pas loin qu'un nombre important d'ensemble admettant une telle représentation garantisse sa flexibilité. Le cas p-adique est lui assez différent du cas réel puisque, sans notion de convexité la conjecture d'Helton-Nie n'a pas vraiment de sens. On trouve au contraire des résultats très différents du cas réel. L'exemple développé ici est celui des couronnes p-adique qui peuvent s'écrire comme projections de spectraèdres bien que les couronnes réelles soient des objets non convexes.

Définition 6.4.1. 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.

Les couronnes sont un objet fondamental de l'étude des espaces p-adique. En effet, ces dernières sont à l'origine de la géométrie rigide qui sert de base une partie non négligeable de l'analyse p-adique.

Théorème 6.4.2. Les couronnes sont des projections de spectraèdres.

Preuve : Soit C la couronne de paramètres $a < b \in R_+^*$.
On considère pour tous $x, y \in \mathbb{Q}_p$ 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 associé $\mathcal{S} = \{(x,y) \in \mathbb{Q}_p : M(x,y) \succeq 0\}$

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 6.2.2 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

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

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

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 6.2.2alors $\mathrm{val}_p(x) \geq a$, $\mathrm{val}_p(y) \geq -b$ 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 2 .

6.5 Vers la résolution du problème *(LMI)*

Cette dernière section présente des résultats qui bien qu'ils n'ont pas permis d'aboutir à une résolution concrète peuvent servir de bases a de futures réflexion.

On rappelle que le problème *(LMI)* consiste à déterminer si un spectraèdre est vide. On y développe ici quelques pistes.

Comme vu précédemment, d'après 6.2.2 le fait qu'une matrice soit semi-définie positive est caractérisé par le fait que son polynôme soit à coefficient dans $\mathbb{Z}_p$. Pour obtenir une représentation claire des spectraèdres, qui permettrait de résoude (LMI) on est en droit de se demander : à quelles conditions le polynôme caractéristique d'une matrice linéaire $A(x) := A_0 + x_1 A_1 + \ldots + x_s A_s$ est-il à coefficient dans $\mathbb{Z}_p$? Les coefficients du polynôme caractéristique de la matrice linéaire $A(x)$ étant polynomiaux en x se poser la question précédente revient alors à se demander pour quelles valeurs de $x = (x_1, \ldots x_s)$ un polynôme $P \in \mathbb{Q}_p[x_1, \ldots, x_s]$ est-il à valeur dans $\mathbb{Z}_p$?

Si je n'ai pu y répondre, on peut toutefois remarquer que dans le cas où le polynôme est univarié on retrouve le concept de discoïde développé par Rüth dans [Rüt15]. Ce qui signifie que pour un polynôme univarié P à coefficients dans $\mathbb{Q}_p$ fixé, l'ensemble des points x de $\overline{\mathbb{Q}_p}$ tels que $P(x) \geq 0$ correspond à une union disjointes de boules de $\overline{\mathbb{Q}_p}$ centrées en les racines de P et dont le rayon se déduit des coefficients de Taylor du polynôme en ses racines. Si trouver l'intersection d'un boule de $\overline{\mathbb{Q}_p}$ avec $\mathbb{Q}_p$ est aisé si cette dernière est centrée en un élément de $\mathbb{Q}_p$ (c'est alors le boule de même centre et de même rayon mais cette fois dans $\mathbb{Q}_p$) le cas où le centre donné n'est pas un nombre p-adique est lui plus délicat et je n'ai pas de résolution à y apporter dans ce rapport.

7 Conclusion

Il a été décrit au cours de ce rapport de nouvelles définitions pour les polyèdres et les spectraèdres sur les corps p-adiques. Les polyèdres sont définis par des inégalités de valuation linéaire. On leur a de plus adjoint un algorithme permettant de résoudre la programmation linéaire en $O(\max(m, n)^2)$. Afin de définir les spectraèdres sur les corps p-adiques il a été nécessaire de trouver une nouvelle définition de matrice semi-définie positive. Pour ce faire l'on s'est débarrassé de la symétrie, obligatoire dans le cas réel, en demandant à ce que les valeurs propres de la matrice soit de valuation positive dans la clôture de $\mathbb{Q}_p$. La définition de spectraèdre était alors immédiate et nous a permis de trouver que les couronnes p-adiques sont des ombres de spectraèdre, dressant un portrait bien différent du cas réel.

Ces résultats gagneraient toutefois à être d'avantage étudiés, en effet, si la définition des polyèdres dans le cadre choisi semble difficilement pouvoir varier, celle des spectraèdre peut toutefois être discutée. En effet, l'on peut par exemple se demander si l'on obtient de résultats similaires en demandant la symétrie aux

matrices semi définies positives, comme dans le cas réel en demandant des condition particulières sur les matrices de sortes à ce que leurs valeurs propres soit dans $\mathbb{Q}_p$. De plus, les problèmes informatiques comme la programmation semi-définie ou le problème (LMI) n'ont pas été résolus (loin s'en faut). Mais il peut toutefois être interessant d'explorer les pistes laissées en 6.5 dans d'éventuels travaux futurs.

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 4 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 $N_1 \to N_2$ sont reliés entre eux si et seulement si $N_1 \subset N_2$ et $|N_2| = |N_1| + 1$.

On encode alors les p-adique comme une suite de sommets reliés entre eux.

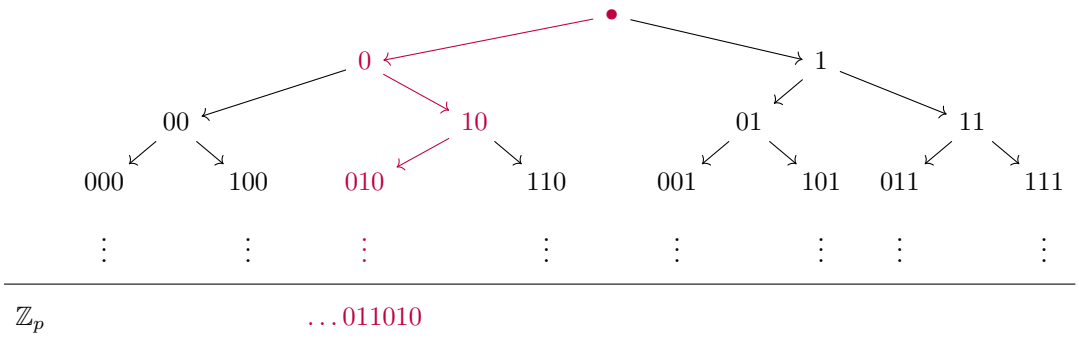

FIGURE 3 – $\mathcal{T}(\mathbb{Z}_p)$

Cette interprétation en arbre de $\mathbb{Z}_p$ est utile car permet de se figurer certaine propriétés géométriques des p-adiques, puisqu'en effet chaque sommet représente exactement une boule

Démonstration. Proposition 4.2.2 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 A.0.1. 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 A.0.1.

En effet, si on pose n le plus petit entier naturel tel que $x_n \neq 0$ [9] 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 $\mathbb{Z}_p$

9. c'est-à-dire la valuation de x

□

Démonstration. Propriété 4.3.2 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 A.0.1, $p^{m-n}\tilde{x} + \tilde{y} \in \mathbb{Z}_p^\times$. □

Démonstration. Théorème 6.2.2

Afin de prouver le théorème 6.2.2 nous allons reformuler ce dernier sous la forme équivalente suivante :

Propriété A.0.2. Un polynôme de $\mathbb{Q}_p[X]$ *unitaire et de terme constant entier* est a uniquement des racines de valuation positive ou nulle dans $\overline{\mathbb{Q}_p}$ si et seulement si il est à coefficients dans $\mathbb{Z}_p$.

Si prouver le sens réciproque de cette équivalence se fait sans difficulté, le sens direct est, lui plus complexe à démontrer. Pour ce faire, nous utiliserons un outil particulièrement utile pour l'étude des polynômes à coefficients p-adique : les polygones de Newton.

Preuve du sens réciproque : Soit $P = X^n + \sum_{i=0}^{n-1} a_i X^i$ un polynôme à coefficients dans $\mathbb{Z}_p$. Montrons par l'absurde que toute racine de P est de valuation positive. Soit $\rho \in \overline{\mathbb{Q}_p}$ une racine de P, supposons $\mathrm{val}_p(\rho) < 0$. D'après la propriété 4.3.2, $\mathrm{val}_p(P(\rho)) = \min\left(\mathrm{val}_p(\rho^n), \mathrm{val}_p(a_{n-1}\rho^{n-1}), \ldots, \mathrm{val}_p(a_0)\right)$. Or on a l'inégalité $\mathrm{val}_p(\rho^n) = n\mathrm{val}_p(\rho) \leq \mathrm{val}_p\left(a_i p^i\right) = i\mathrm{val}_p(\rho) + \mathrm{val}_p(a_i)$ pour $i = 1, \ldots, n$, car $a_i \in \mathbb{Z}_p$. Ainsi $\mathrm{val}_p(P(\rho)) = n\mathrm{val}_p(\rho) < 0$, or ρ est une racine de P et donc $\mathrm{val}_p(P(\rho)) = \mathrm{val}_p(0) = +\infty$. Ce qui est absurde, donc $\mathrm{val}_p(\rho) \geq 0$.

Preuve du sens direct :

Pour la preuve du sens direct on utilisera les polygones de Newton, un outil permettant de relier très facilement les coefficient d'un polynôme à la valuation de ses racines. On ne prouvera pas le principal résultat sur les polygones de Newton dont la preuve peut se retrouver en section 6.4 de [Gou03] .

Définition A.0.3. Polygone de Newton

Soit $P = \sum_{i=0}^{n} a_i X^i$ un polynôme à coefficients dans $\mathbb{Q}_p$. On appelle *polygone de Newton* l'ensemble des points enveloppe convexe inférieure de l'ensemble $\mathcal{P} = \{(i, \mathrm{val}_p(a_i)) \,|\, 1 \leq i \leq n\}$.

On entend par enveloppe convexe inférieure le graphe de la plus grande fonction convexe f de $[0, n]$ étant "sous" les points de $\mathcal{P}$, i.e. telle que $f(i) > a_i$ pour $i = 1 \ldots n$.

Exemple. Par exemple au polynôme $P = 3 + \frac{5}{2}X + 32X^2 + \frac{9}{4}X^4 + 44X^5 + 2X^6$ on associe

On pourra alors prouver que l'enveloppe convexe inférieure ainsi définie est une ligne brisée constitués de segments de pentes deux à deux différentes. On appelle pentes du polygones les pentes des segments de la ligne brisée et longueur d'un segment de la ligne brisé la longueur du projeté du segment sur l'axe des abscisses.

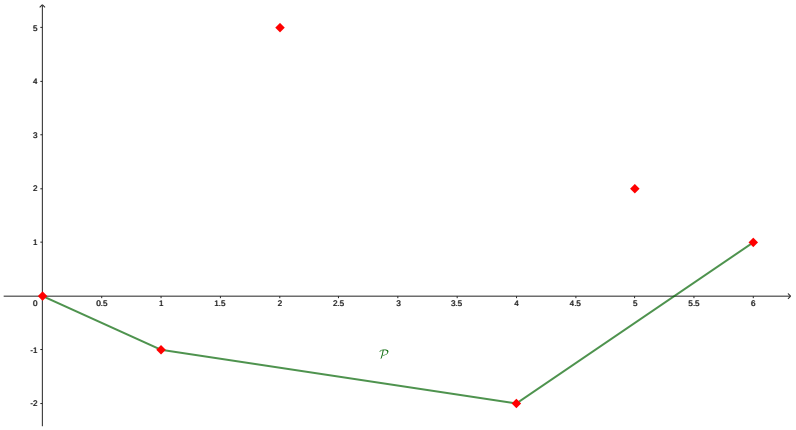

FIGURE 4 – Polygone de Newton $\mathcal{P}$ associé à P

Théorème A.0.4. Les pentes du polygone de Newton $\mathcal{P}$ sont exactement les opposés des valuations des racines de P (dans $\overline{\mathbb{Q}_p}$). De plus, le nombre de racines de valuation v est égal à la longueur du segment de pente $-v$.

On considère alors un polynôme $P = X^n \sum_{i=1}^{n-1} a_i X^i$ à coefficient dans $\mathbb{Q}_p$ unitaire. On remarque immédiatement que le point d'abscisse n du polygone de Newton $\mathcal{P}$ associé à P est d'ordonnée nulle. On en déduit alors que si un des coefficients $(a_i)_{0\leq i\leq n-1}$ est de valuation strictement négative, $\mathcal{P}$ admet une pente strictement positive et donc P admet une racine de valuation strictement négative.

Par contraposée, on en déduit que si polynôme unitaire à coefficient dans $\mathbb{Q}_p$ est à racine positive alors il est élément de $\mathbb{Z}_p[X]$.

□

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 5.2. Les preuves de cette section ont étés tirées de [How] puis rapportées au cas p-adique, là ou le cours original se place dans le cadre plus général des anneaux euclidiens.

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 :

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

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 A.0.1. Multiplier à gauche N par la matrice $\mathrm{diag}(\tilde{\alpha}, 0, \dots, 0)$ conserve l'équivalence dans $\mathbb{Z}_p$ [10] 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}.

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

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

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 $\Omega(\max(m,n))$, résultat prouvé par Tristan Vaccon et son stagiaire dans un article encore non publié.

Démonstration. Unicité de la forme normale de Smith Soit $M \in \mathcal{M}_{m,n}(\mathbb{Z}_p)$ et $S = \begin{pmatrix} p^{a_1} & & & & \\ & \ddots & & & \\ & & p^{ar} & & \\ & & & 0 & \\ & & & & \ddots \end{pmatrix}$ 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 4.3.2.

On en déduit alors ce résultat plus fort : Pour toutes matrice $A \in \mathcal{M}_{m,n}(\mathbb{Z}_p)$, $P \in \mathcal{G}L_n(\mathbb{Z}_p)$ et $Q \in \mathcal{G}L_m(\mathbb{Z}_p)$ 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 de l'algorithme de la section 5.2.

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 $Ax + b \geq 0$.

$S, P, Q = \mathrm{FormeNormaleDeSmith}(A)$
$r = \mathrm{rang}(S)$
$b' = Q \times b$
$c' = P^T \times c$
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
$\tilde{c} = \mathrm{Projection}(c', 1, r)$ ▷ On réduit le problème à un problème de taille r
$\tilde{b} = \mathrm{Projection}(b', 1, r)$
$\tilde{S} = \mathrm{SousMatrice}(S, (1, r), (1, r))$
$\lambda = \tilde{c}.S^{-1}.\tilde{b}$
$v = \min\left\{\mathrm{val}_p(z_i) \mid (z_1, \ldots, z_r) = \tilde{c}.S^{-1}\right\}$
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

Ou FormeNormaleDeSmith renvoie la forme normale de Smith S de la matrice A ainsi que les matrices P et Q telles que $A = Q^{-1}SP$.

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

Références

[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.

[VB99] Lieven Vandenberghe et Stephen Boyd. « Applications of semidefinite programming ». In : *Applied Numerical Mathematics*. Proceedings of the Stieltjes Workshop on High Performance Optimization Techniques 29.3 (mar. 1999), p. 283-299. ISSN : 0168-9274. DOI : 10.1016/S0168-9274(98)00098-1. URL : https://www.sciencedirect.com/science/article/pii/S0168927498000981 (visité le 21/08/2023).

[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.

[HN08] J. William Helton et Jiawang Nie. *Sufficient and Necessary Conditions for Semidefinite Representability of Convex Hulls and Sets*. arXiv :0709.4017 [math]. Déc. 2008. DOI : 10.48550/arXiv.0709.4017. URL : http://arxiv.org/abs/0709.4017 (visité le 21/08/2023).

[GPR12] Blekherman Grigoriy, A. Parrilo Pablo et R. Thomas Rekha, éd. *Semidefinite Optimization and Convex Algebraic Geometry*. MOS-SIAM Series on Optimization. Society for Industrial et Applied Mathematics, déc. 2012. ISBN : 978-1-61197-228-3. DOI : 10.1137/1.9781611972290. URL : https://epubs.siam.org/doi/book/10.1137/1.9781611972290 (visité le 21/08/2023).

[Rüt15] Julian Rüth. « Models of curves and valuations ». en. In : Universität Ulm, 2015. DOI : 10.18725/OPARU-3275. URL : https://oparu.uni-ulm.de/xmlui/handle/123456789/3302.

[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).

[Sch17] Claus Scheiderer. *Spectrahedral shadows*. arXiv :1612.07048 [math]. Déc. 2017. DOI : 10.48550/arXiv.1612.07048. URL : http://arxiv.org/abs/1612.07048 (visité le 21/08/2023).

[AGS19] Xavier Allamigeon, Stéphane Gaubert et Mateusz Skomra. « The tropical analogue of the Helton–Nie conjecture is true ». en. In : *Journal of Symbolic Computation*. MEGA 2017, Effective Methods in Algebraic Geometry, Nice (France), June 12-16, 2017. 91 (mar. 2019), p. 129-148. ISSN : 0747-7171. DOI : 10.1016/j.jsc.2018.06.017. URL : https://www.sciencedirect.com/science/article/pii/S0747717118300828 (visité le 23/07/2023).

[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.

[Roz21] Abdu Rozik. *Borgir*. English. Mai 2021. URL : https://youtu.be/toZW65rksYY.

[How] Ralph Howard. « Rings, Determinants, the Smith Normal Form, and Canonical Forms for Similarity of Matrices. » en. In : ().