

Estimation des dimensions de certaines variétés de Kisin

Xavier Caruso

Mai 2010

Résumé

Dans cet article, nous nous intéressons aux dimensions de certaines variétés qui ont été introduites récemment par Kisin pour démontrer la modularité de certaines représentations galoisiennes. Nous étudions plus spécialement un cas particulier pour lequel nous obtenons une estimation de la dimension qui nous intéresse, puis, en nous basant sur ce résultat, nous énonçons une conjecture dans le cas général.

Abstract

In this paper, we study dimensions of some varieties, that were introduced recently by Kisin in order to prove modularity of some Galois representations. In fact, we mainly consider a special case for which we obtain an estimation of the dimension we are interested in. Then, based on this result, we state a conjecture for the general case.

Table des matières

| | | |
|----------|--|-----------|
| 1 | Une stratification utile | 5 |
| 1.1 | Donnée combinatoire associée à un réseau | 5 |
| 1.2 | Paramétrisation de l'espace des fonctions φ | 11 |
| 1.3 | Les variétés \mathcal{X}_φ et leurs dimensions | 16 |
| 2 | Mise en place de la méthode | 21 |
| 2.1 | Préliminaires de programmation linéaire | 21 |
| 2.2 | Étude du cône convexe Φ | 24 |
| 2.3 | Un premier exemple d'application | 27 |
| 3 | Dimension des variétés $\mathcal{X}_{\leq e}$, \mathcal{X}_μ et $\mathcal{X}_{\leq \mu}$ | 30 |
| 3.1 | Les points extrémaux de $A_{Q_{\max}, g, \ell}$ | 30 |
| 3.2 | Le calcul de $A_{Q, g, \ell}$ | 34 |
| 3.3 | Démonstration des théorèmes 2, 4 et 5 | 38 |
| 3.4 | Points extrémaux de $A_{Q, g, \ell} \cap C$: quelques exemples | 42 |
| 4 | Perspectives et conjectures | 43 |
| 4.1 | Peut-on espérer une formule exacte pour la dimension ? | 43 |
| 4.2 | Généralisations envisageables | 49 |

Motivé par l'étude de certains problèmes de modularité et poursuivant des travaux de Breuil, Kisin a introduit et étudié dans [6] un certain nombre de variétés, notées $\mathcal{GR}_{V_{\mathbb{F}}}$, $\mathcal{GR}_{V_{\mathbb{F}}, 0}$ et $\mathcal{GR}_{V_{\mathbb{F}}, 0}^{\text{v,loc}}$ dans *loc. cit.*, paramétrant certains types de schémas en groupes définis sur l'anneau des entiers d'un corps local. S'inspirant de cela, Pappas et Rapoport ont ensuite défini dans [14] un champ sur \mathbb{Z}_p dont certaines fibres s'interprètent comme les variétés que Kisin avait définies, et en ont profité pour nommer ces dernières *variétés de Kisin*. Le fil directeur de cet article est le calcul de la dimension de certaines de ces variétés.

Commençons par rappeler la définition des variétés de Kisin que nous allons considérer. On considère p un nombre premier et k un corps de caractéristique p . On pose $K = k((u))$ et on appelle ϕ l'unique morphisme de k -algèbres $\phi : K \rightarrow K$ qui est continu pour la topologie u -adique et qui envoie u sur u^p .

Pour tout l'article, on fixe d un nombre entier supérieur ou égal à 1 et on pose $M = K^d$. Le Frobenius ϕ s'étend naturellement en un opérateur sur M , encore noté ϕ , en agissant coordonnée par coordonnée¹. Un réseau L de M est, par définition, un sous- $k[[u]]$ -module $L \subset M$ engendré par une $k((u))$ -base de M . On note $\mathcal{L}_{\leq e}$ l'ensemble des réseaux L de M satisfaisant la condition

$$u^e L \subset \phi(k[[u^{1/p}]] \otimes_{k[[u]]} L) \subset L \quad (1)$$

où ϕ est étendu à $k[[u^{1/p}]] \otimes_{k[[u]]} L$ de façon évidente. Kisin démontre que $\mathcal{L}_{\leq e}$ apparaît naturellement comme les k -points d'une variété algébrique que nous noterons simplement $\mathcal{X}_{\leq e}$ dans la suite de cet article. Lorsque $d = 2$, la géométrie de $\mathcal{X}_{\leq e}$ (et de certains de ses analogues) a déjà été étudiée par Kisin lui-même ([6]), Hellmann ([5]) et Imai ([8], [9], [10]). Par contre, pour les d plus grands, peu de choses sont connues. Dans cet article, nous démontrons le théorème suivant.

Théorème 1. *Avec les notations précédentes, on a :*

$$\left\lfloor \frac{d^2}{4} \right\rfloor \cdot \left\lfloor \frac{e-p+2}{p+1} \right\rfloor \leq \dim_k \mathcal{X}_{\leq e} \leq \frac{d(d-1)}{2} + \left\lfloor \frac{d^2}{4} \right\rfloor \cdot \frac{e}{p+1}.$$

Remarquez que la différence entre le majorant et le minorant que nous obtenons n'excède jamais d^2 . Insistons quand même sur le fait que l'on n'affirme en aucune façon que les variétés $\dim_k \mathcal{X}_{\leq e}$ sont équidimensionnelles, ni même que l'inégalité du théorème vaut pour toutes les composantes irréductibles. Le nombre $\dim_k \mathcal{X}_{\leq e}$ désigne bien uniquement la plus grande dimension d'une composante irréductible.

En réalité, nous allons démontrer un théorème légèrement plus général que celui que nous venons de décrire. Plus précisément, nous nous donnons σ une puissance entière du Frobenius agissant sur k et b un entier supérieur ou égal à 2 et nous considérons l'opérateur $\phi : k((u)) \rightarrow k((u))$ plus général donné par la formule que voici :

$$\phi : K \rightarrow K, \quad \sum_{i \gg -\infty} a_i u^i \mapsto \sum_{i \gg -\infty} \sigma(a_i) u^{bi}. \quad (2)$$

Lorsque $\sigma = \text{id}$ et $b = p$, on retrouve la situation précédente. Un autre cas qui semble intéressant est celui où $b = p$ et σ est l'élévation à la puissance p , c'est-à-dire si l'on préfère celui où ϕ lui-même est l'élévation à la puissance p . En effet, un théorème de Breuil ([1]) dit alors que les éléments de $\mathcal{X}_{\leq e}(k)$ sont en bijection avec l'ensemble des classes d'isomorphisme de modèles entiers du schéma en groupes $(\mathbb{Z}/p\mathbb{Z})_K^d$ où K est une extension totalement ramifiée fixée de degré e de $\text{Frac } W(k)$ (où $W(k)$ désigne l'anneau des vecteurs de Witt à coefficients dans k). Quoi qu'il en soit, dans la situation générale que nous considérons, nous démontrons le théorème suivant.

Théorème 2. *Si $\sigma \neq \text{id}$, on a :*

$$\left\lfloor \frac{d^2}{4} \right\rfloor \cdot \left\lfloor \frac{e-b+2}{b+1} \right\rfloor \leq \dim_k \mathcal{X}_{\leq e} \leq \left\lfloor \frac{d^2}{4} \right\rfloor \cdot \frac{e}{b+1}.$$

Si $\sigma = \text{id}$, on a :

$$\left\lfloor \frac{d^2}{4} \right\rfloor \cdot \left\lfloor \frac{e-b+2}{b+1} \right\rfloor \leq \dim_k \mathcal{X}_{\leq e} \leq \frac{d(d-1)}{2} + \left\lfloor \frac{d^2}{4} \right\rfloor \cdot \frac{e}{b+1}.$$

Notons que, dans ce qui précède, nous avons exclu le cas $b = 1$, mais celui-ci conduit en fait à une classe importante de variétés qui ont déjà été largement étudiées, à savoir un cas particulier simple de variétés de Deligne-Lusztig affines. En particulier, leurs dimensions ont déjà été déterminées (dans une plus grande généralité) dans les articles [4] et [15]. Soulignons à ce propos que la méthode que nous allons suivre dans cet article pour démontrer le théorème précédent est fortement inspirée de [15].

Dans leurs articles respectifs, Kisin d'une part et Pappas et Rapoport d'autre part définissent également des variantes des variétés $\mathcal{X}_{\leq e}$ qui ne sont plus paramétrées par un unique entier e mais par un d -uplet d'entiers relatifs (μ_1, \dots, μ_d) tels que $\mu_1 \geq \dots \geq \mu_d$. Dans la généralité que nous considérons — c'est-à-dire lorsque b et σ peut être quelconques — ces variantes ont encore un sens. Précisément, si $\mu = (\mu_1, \dots, \mu_d)$

¹L'auteur est conscient qu'il s'agit là d'une restriction importante, le cas général que l'on aimerait étudier étant celui où $\phi : M \rightarrow M$ est une application semi-linéaire quelconque. Nous discuterons rapidement dans le §4.2.1 de ce que l'on peut attendre dans cette généralité.

est un d -uplet comme précédemment, on peut construire des variétés \mathcal{X}_μ et $\mathcal{X}_{\leq \mu}$ dont les points k -rationnels sont respectivement :

$$\mathcal{L}_\mu = \left\{ \text{réseaux } L \text{ de } M \left| \begin{array}{l} \text{il existe une base } m_1, \dots, m_d \text{ de } L \text{ telle que} \\ u^{\mu_1} m_1, \dots, u^{\mu_d} m_d \text{ soit une base de } \phi(k[[u^{1/b}]] \otimes_{k[[u]]} L) \end{array} \right. \right\}$$

et

$$\mathcal{L}_{\geq \mu} = \bigcup_{\mu' \leq \mu} \mathcal{L}_{\mu'}$$

où l'on convient que $\mu' = (\mu'_1 \geq \dots \geq \mu'_d)$ est plus petit ou égal à μ si $\mu'_1 + \dots + \mu'_t \leq \mu_1 + \dots + \mu_t$ pour tout $t \in \{1, \dots, d\}$ avec égalité si $t = d$. Nous nous intéresserons également à la dimension de ces variétés. Pour énoncer les résultats obtenus, il est commode de munir \mathbb{R}^d du produit scalaire usuel $\langle \cdot | \cdot \rangle_d$, d'introduire le vecteur

$$\vec{\rho} = \left(\frac{d-1}{2}, \frac{d-3}{2}, \dots, \frac{1-d}{2} \right) \in \mathbb{R}^d$$

(la i -ième coordonnée est donnée par la formule $\frac{d+1}{2} - i$) ainsi que la définition suivante.

Définition 3. On dit qu'un d -uplet $\mu = (\mu_1, \dots, \mu_d) \in \mathbb{R}^d$ est :

- b -régulier si $\mu_i - \mu_{i+1} \leq b(\mu_{d-i} - \mu_{d-i+1})$ pour tout $i \in \{1, \dots, d-1\}$;
- *intégralement b -régulier* s'il est b -régulier, si tous les μ_i sont entiers et $b-1$ divise $\mu_1 + \dots + \mu_d$,
- *fortement intégralement b -régulier* s'il est intégralement b -régulier et vérifie en plus :

$$\mu_{d-1} - \mu_d \leq b(\mu_1 - \mu_2) - d(b^2 - 1).$$

Les définitions d'éléments b -réguliers et intégralement b -réguliers semblent s'imposer dans notre contexte. Par contre, l'inégalité renforcée qui apparaît dans la définition de fortement intégralement b -régulier n'est probablement pas optimale et devra sans doute être corrigée ultérieurement. Remarquons néanmoins que si $\mu = (\mu_1, \dots, \mu_d)$ est b -régulier, alors $\mu_1 \geq \dots \geq \mu_d$. Réciproquement si les μ_i sont rangés par ordre décroissant et deux à deux *distincts*, le d -uplet μ est b -régulier pour b suffisamment grand.

Théorème 4. Soit $\mu = (\mu_1, \dots, \mu_d) \in \mathbb{Z}^d$ tel que $\mu_1 \geq \mu_2 \geq \dots \geq \mu_d$. Si $b-1$ ne divise pas $\mu_1 + \dots + \mu_d$, alors la variété \mathcal{X}_μ est vide. On suppose donc tout au long du théorème que $b-1$ divise $\mu_1 + \dots + \mu_d$.

Posons $\varepsilon = 1$ si $\sigma = \text{id}$ et $\varepsilon = 0$ dans le cas contraire. Alors, il existe un entier $\delta \in \{0, 1, \dots, \varepsilon \cdot \frac{d(d-1)}{2}\}$ tel que l'on ait la congruence :

$$\dim_k \mathcal{X}_\mu \equiv \delta - \sum_{i=1}^d i \cdot \mu_i \pmod{b-1}.$$

En particulier, si $\sigma \neq \text{id}$, on a :

$$\dim_k \mathcal{X}_\mu \equiv - \sum_{i=1}^d i \cdot \mu_i \pmod{b-1}.$$

Supposons maintenant en plus $b > 1 + \frac{d^2}{4}$. Alors on a :

$$\dim_k \mathcal{X}_\mu \leq \varepsilon \cdot \frac{d(d-1)}{2} + (b-1) \cdot \min_{w \in \mathfrak{S}_d} \sum_{i=1}^d \sum_{n=1}^{\infty} \mu_i \cdot \frac{d+1-i-w^n(i)}{b^n}$$

où, bien entendu, \mathfrak{S}_d désigne le groupe des permutations de $\{1, \dots, d\}$ et $w^n = w \circ \dots \circ w$ (n fois). En outre, si μ est b -régulier, alors le minimum précédent est atteint pour $w = w_0 : i \mapsto d+1-i$ et vaut $\frac{1}{b+1} \cdot \langle 2\vec{\rho} | \mu \rangle_d$.

On suppose toujours $b > 1 + \frac{d^2}{4}$. Il existe des constantes positives c_1 et c_2 (qui ne dépendent que de d et b) telles que si les μ_i vérifient en plus $\mu_i \geq \mu_{i+1} + c_1$ pour tout i , alors :

$$\dim_k \mathcal{X}_\mu \geq -c_2 + (b-1) \cdot \min_{w \in \mathfrak{S}_d} \sum_{i=1}^d \sum_{n=1}^{\infty} \mu_i \cdot \frac{d+1-i-w^n(i)}{b^n}.$$

Encore une fois, on ne dit rien quant à l'équidimensionnalité des variétés \mathcal{X}_μ . Cependant, lorsque $\sigma \neq \text{id}$, on peut se demander s'il est vrai que toutes les composantes irréductibles de \mathcal{X}_μ ont des dimensions congrues à $-\sum_{i=1}^d i \cdot \mu_i$ modulo $(b-1)$. À part cela, il est clair que les sommes infinies qui apparaissent dans la formule du théorème précédent convergent. Étant donné que toute permutation w est d'ordre fini, on peut même facilement calculer leur limite qui s'exprime toujours comme le produit de μ_i par un nombre rationnel, ce dernier étant même la valeur en b d'une fraction rationnelle à coefficients entiers. On en vient maintenant aux variétés $\mathcal{X}_{\leq \mu}$.

Théorème 5. Soit $\mu = (\mu_1, \dots, \mu_d) \in \mathbb{R}^d$ tel que $\mu_1 \geq \mu_2 \geq \dots \geq \mu_d$. Posons $\varepsilon = 1$ si $\sigma = \text{id}$ et $\varepsilon = 0$ dans le cas contraire. Alors :

$$-(d-1)^2 - \frac{(d-2)^2}{4} + \sup_{\substack{\mu' \leq \mu \\ \mu' \text{ f.i. } b\text{-rég.}}} \frac{\langle 2\bar{\rho} | \mu' \rangle_d}{b+1} \leq \dim_k \mathcal{X}_{\leq \mu} \leq \varepsilon \cdot \frac{d(d-1)}{2} + \frac{\langle 2\bar{\rho} | \mu \rangle_d}{b+1}.$$

Si, en outre, $b \geq 1 + \frac{d^2}{4}$, alors la majoration peut être renforcée comme suit :

$$\dim_k \mathcal{X}_{\leq \mu} \leq \varepsilon \cdot \frac{d(d-1)}{2} + \sup_{\substack{\mu' \leq \mu \\ \mu' \text{ } b\text{-rég.}}} \frac{\langle 2\bar{\rho} | \mu' \rangle_d}{b+1}.$$

Commentons un peu le théorème. Pour la première assertion, remarquons que si μ est lui-même fortement intégralement b -régulier, alors la borne supérieure qui apparaît est atteinte pour $\mu' = \mu$. Ainsi le théorème dit, dans ce cas, que la quantité $\frac{\langle 2\bar{\rho} | \mu \rangle_d}{b+1}$ est une bonne approximation de la dimension de $\mathcal{X}_{\leq \mu}$. La deuxième assertion mérite, quant à elle, une discussion plus approfondie. Tout d'abord, signalons qu'il est facile de prouver que la borne supérieure qui apparaît est plus petite ou égale — et en général strictement plus petite, du moins si μ n'est pas lui-même b -régulier — que $\frac{\langle 2\bar{\rho} | \mu \rangle_d}{b+1}$; ainsi, comme nous le disions déjà dans l'énoncé du théorème, la majoration écrite est meilleure que la précédente. Notons également qu'on a clairement $\mathcal{X}_{\leq \mu} = \bigcup_{\mu' \leq \mu} \mathcal{X}_{\leq \mu'}$, d'où on déduit que :

$$\dim_k \mathcal{X}_{\leq \mu} = \sup_{\mu' \leq \mu} \dim_k \mathcal{X}_{\leq \mu'}.$$

L'inégalité du théorème dit donc *en substance* que, si $b \geq 1 + \frac{d^2}{4}$, les variétés $\mathcal{X}_{\leq \mu'}$, pour $\mu' \leq \mu$ non b -régulier, n'apportent pratiquement pas de nouvelles dimensions à $\mathcal{X}_{\leq \mu}$. Notamment, contrairement à ce qui se passe dans le cas des variétés de Deligne-Lusztig affines, il n'est pas clair — et ce n'est d'ailleurs en général pas vrai — que l'essentiel de la dimension de $\mathcal{X}_{\leq \mu}$ est concentré dans la variété \mathcal{X}_μ . Du fait que \mathcal{X}_μ est un ouvert dans $\mathcal{X}_{\leq \mu}$, il suit que $\mathcal{X}_{\leq \mu}$ n'est pas équidimensionnelle au moins lorsque μ n'est pas b -régulier.

Signalons enfin que la borne supérieure qui apparaît dans la dernière inégalité du théorème est aussi égale au minimum d'un nombre fini de formes linéaires sur \mathbb{R}^d , ce qui permet de la calculer efficacement. Malgré tout, bien que ces formes linéaires soient définies de façon plutôt explicite, leur nombre et leur complexité croît très rapidement lorsque d augmente. À titre d'exemple, le tableau 2 (page 44) les donne pour $d \leq 4$.

Détaillons à présent sommairement le plan de l'article. Dans un premier temps, en nous inspirant de la méthode de [15], nous associons à chaque réseau $L \subset M$ un d -uplet de fonctions. Nous montrons en outre que ces fonctions satisfont un certain nombre de contraintes combinatoires qui imposent une rigidité telle qu'elle nous permet de les paramétrer par les points d'un ensemble convexe dans un espace de dimension $\frac{d(d+1)}{2}$. Nous en venons ensuite à la géométrie : à l'aide de la construction précédente, nous définissons une stratification des variétés de Kisin et démontrons une formule essentielle pour notre propos donnant une estimation de la dimension des strates. Ceci nous permet de reformuler complètement le problème qui nous intéresse en termes de programmation linéaire. Les sections 2 et 3 sont consacrées à la résolution de ce nouveau problème dans chacun des cas que nous considérons. Comme corollaire, nous obtenons les théorèmes 2 (duquel découle directement, comme nous l'avons déjà dit, le théorème 1), 4 et 5. Enfin, dans une dernière section, nous analysons succinctement la méthode et discutons quelques autres situations auxquelles il est envisageable de l'étendre.

Remerciements C'est un plaisir de remercier Michael Rapoport pour m'avoir soumis le problème dont il est question dans cet article, et également pour ses encouragements constants. Je le remercie également de m'avoir plusieurs fois invité à l'Université de Bonn, qui est un lieu extraordinaire pour faire des mathématiques. Mes remerciements vont aussi à Eugen Hellmann pour d'intéressantes discussions et à Eva Viehmann pour m'avoir fait connaître son article [15], duquel tout ce travail est inspiré. Je remercie également David Monniaux pour m'avoir fait connaître son logiciel `mjollnir` [11] qui m'a été fort utile lors de l'élaboration de cet article.

Finalement, l'auteur remercie l'Agence Nationale de la Recherche (ANR) pour son soutien financier par l'intermédiaire du projet CETHop (Calculs Effectifs en Théorie de Hodge p -adique) référencé ANR-09-JCJC-0048-01.

1 Une stratification utile

Commençons par rappeler brièvement que les k -variétés $\mathcal{X}_{\leq e}$, \mathcal{X}_μ et $\mathcal{X}_{\leq \mu}$ sont définies par l'intermédiaire de leur « foncteur des points ». Par exemple, pour ce qui concerne $\mathcal{X}_{\leq e}$, étant donné R une k -algèbre, on note $\mathcal{X}_{\leq e}(R)$ l'ensemble des $R[[u]]$ -sous-modules L de $M \otimes_{k((u))} R((u)) = R((u))^d$ qui sont tels que :

- i) L est un réseau de $M \otimes_{k((u))} R((u)) = R((u))^d$, c'est-à-dire que L est un $R[[u]]$ -module localement libre de type fini (pour la topologie de Spec R) et le morphisme naturel $L \otimes_{R[[u]]} R((u)) \rightarrow M$ est un isomorphisme ;
- ii) la condition (1) est satisfaite (où ϕ opère encore par σ sur R et envoie u sur u^b et s'étend à $M \otimes_{k((u))} R((u)) = R((u))^d$ en agissant coordonnée par coordonnée).

On montre ensuite que le foncteur $R \mapsto \mathcal{X}_{\leq e}(R)$ ainsi défini est représentable par un schéma de type fini sur k . Des considérations analogues conduisent à une définition rigoureuse de \mathcal{X}_μ et $\mathcal{X}_{\leq \mu}$.

Le but de ce premier chapitre est de montrer que les variétés dont on souhaite estimer la dimension sont stratifiées par des variétés \mathcal{X}_φ (où φ est une donnée combinatoire qui dépend de $\frac{d(d+1)}{2}$ entiers) dont on sait calculer la dimension.

1.1 Donnée combinatoire associée à un réseau

Dans cette partie, on associe à chaque réseau L de M la donnée combinatoire que nous évoquions précédemment et qui s'avère être un ensemble de d fonctions soumises à un certain nombre de contraintes. Nous montrons ensuite que ces contraintes imposent une rigidité telle qu'elles réduisent la donnée des d fonctions à celle de seulement $\frac{d(d+1)}{2}$ nombres.

1.1.1 Définitions

Notons val la valuation naturelle sur $k((u))$: la valuation d'une somme $\sum_{i \gg -\infty} a_i u^i$ est le plus petit entier v tel que $a_v \neq 0$ et on convient que $\text{val}(0) = +\infty$. La valuation s'étend de manière unique à l'extension totalement ramifiée $k((u^{1/b}))$, et nous notons encore val ce prolongement ; on a donc $\text{val}(u^{1/b}) = \frac{1}{b}$.

On pose $M_{k((u^{1/b}))} = k((u^{1/b})) \otimes_{k((u))} M = k((u^{1/b}))^d$ et on note (e_1, \dots, e_d) la base canonique de $M = k((u))^d$. Les vecteurs $1 \otimes e_i$ forment une base de $M_{k((u^{1/b}))}$ sur le corps $k((u^{1/b}))$. La valuation val définit une application $\text{val}_M : M_{k((u^{1/b}))} \setminus \{0\} \rightarrow \frac{1}{b}\mathbb{Z} \times \{1, \dots, d\}$ par la formule :

$$\begin{aligned} \text{val}_M(x_1, \dots, x_d) &= (v, i) \quad \text{où} \quad v = \min \{ \text{val}(x_1), \dots, \text{val}(x_d) \} \\ &\quad \text{et} \quad i = \min \{ j \mid v = \text{val}(x_j) \} \end{aligned}$$

On prolonge val_M à $M_{k((u^{1/b}))}$ tout entier en convenant que $\text{val}_M(0) = \infty$ où ∞ est nouvel élément que l'on ajoute au produit $\frac{1}{b}\mathbb{Z} \times \{1, \dots, d\}$. On vérifie immédiatement que si $\lambda \in k((u^{1/b}))$ et $M \in M_{k((u^{1/b}))}$, on a $\text{val}_M(\lambda x) = \text{val}(\lambda) + \text{val}_M(x)$ avec la convention évidente que $\infty + x = \infty$ lorsque x est un nombre rationnel ou un couple $(v, i) \in \frac{1}{b}\mathbb{Z} \times \{1, \dots, d\}$. De plus, si l'on munit l'ensemble $\frac{1}{b}\mathbb{Z} \times \{1, \dots, d\}$ de l'ordre lexicographique² et que l'on convient que ∞ est strictement plus grand que tous les couples (v, i) , alors, pour tous x et y dans M , on a $\text{val}_M(x + y) \geq \min \{ \text{val}_M(x), \text{val}_M(y) \}$ et l'égalité a lieu dès que $\text{val}_M(x) \neq \text{val}_M(y)$.

²Cela signifie que $(v, i) < (v', i')$ si, et seulement si soit $v < v'$, soit $v = v'$ et $i < i'$.

Définition 1.1. Soit L un réseau de M . Pour tout $v \in \frac{1}{b}\mathbb{Z}$ et tout $i \in \{1, \dots, d\}$, on pose

$$\tilde{\varphi}_i(L)(v) = \sup_{\substack{x \in k[[u^{1/b}]] \otimes_{k[[u]]} L \\ \text{val}_M(x) = (v, i)}} \left(\inf \{ n \in \mathbb{Z} \mid \phi(x) \in u^n L \} \right) \quad (1.1)$$

où, par convention, la borne supérieure de l'ensemble vide est $-\infty$.

La définition ci-dessus n'est en fait rien d'autre qu'une adaptation de la définition des fonctions φ qui apparaissent dans [15]. Le lemme 4.1 de *loc. cit.* se transpose également à notre situation et donne la proposition suivante.

Proposition 1.2. Soit L un réseau de M . Les fonctions $\tilde{\varphi}_i(L) : \frac{1}{b}\mathbb{Z} \rightarrow \mathbb{Z} \cup \{-\infty\}$, $v \mapsto \varphi_i(L)(v)$ vérifient les propriétés suivantes.

1. Pour tout i , la fonction $\tilde{\varphi}_i(L)$ est strictement croissante où, par un léger abus d'écriture, l'on entend pas là³ que $\tilde{\varphi}_i(L)$ est croissante et qu'elle est strictement croissante sur l'ensemble où elle prend des valeurs finies.
2. Pour tout i , il existe un entier $\tilde{q}_i(L)$ tel que
 - la fonction $\tilde{\varphi}_i(L)$ prend des valeurs finies exactement sur l'intervalle $[\tilde{q}_i(L), +\infty[$, et
 - pour v suffisamment grand, on a $\tilde{\varphi}_i(L)(v) = bv - \tilde{q}_i(L)$.
3. Pour $j \in \{1, \dots, d\}$, il existe des fonctions croissantes $\psi_j(L) : \mathbb{Z} \rightarrow \frac{1}{b}\mathbb{Z} \cup \{-\infty\}$ telles que $\psi_1(L) \leq \psi_2(L) \leq \dots \leq \psi_d(L)$ et pour tout couple $(v, \mu) \in \frac{1}{b}\mathbb{Z} \times \mathbb{Z}$, il y a autant d'indices $i \in \{1, \dots, d\}$ tels que $\mu = \tilde{\varphi}_i(L)(v)$ que d'indices $j \in \{1, \dots, d\}$ tels que $v = \psi_j(L)(\mu)$. Ces fonctions sont en outre uniquement déterminées.
4. Si $u^{\mu_1(L)}, \dots, u^{\mu_d(L)}$, avec $\mu_1(L) \geq \dots \geq \mu_d(L)$, sont les exposants des diviseurs élémentaires du $k[[u]]$ -module engendré par $\phi(L)$ par rapport à L , alors, pour tout i , la fonction ψ_i prend des valeurs finies exactement sur l'intervalle $[\mu_i(L), +\infty[$.

Si L est un réseau de M , on définit aussi des fonctions $\varphi_1(L), \dots, \varphi_d(L) : \frac{1}{b}\mathbb{Z} \rightarrow \mathbb{Z} \cup \{-\infty\}$ en convenant simplement que pour tout $v \in \frac{1}{b}\mathbb{Z}$, les nombres $\varphi_1(L)(v), \dots, \varphi_d(L)(v)$ sont les mêmes que $\tilde{\varphi}_1(L)(v), \dots, \tilde{\varphi}_d(L)(v)$ mais triés par ordre décroissant. Les fonctions précédentes vérifient donc tautologiquement l'inégalité $\varphi_1(L) \geq \varphi_2(L) \geq \dots \geq \varphi_d(L)$ et on montre sans peine qu'elles satisfont encore aux quatre alinéas de la proposition 1.2 : les entiers $\mu_j(L)$ restent inchangés tandis que les $\tilde{q}_i(L)$ sont *a priori* permutés. Dans la suite, nous noterons simplement $q_i(L)$ l'entier correspondant à la fonction $\varphi_i(L)$.

1.1.2 Un exemple en dimension 2

Pour illustrer la proposition 1.2, examinons un exemple en dimension 2 (*i.e.* avec $d = 2$). Si L est un réseau de M , il existe des entiers relatifs α, δ et un élément $c \in k((u))$ de valuation γ tels que L soit engendré sur $k[[u]]$ par les vecteurs $f_1 = (u^\alpha, 0)$ et $f_2 = (c, u^\delta)$. Par ailleurs, quitte à retirer à c un multiple de u^α , on peut supposer que soit $c = 0$, soit $\gamma < \alpha$. Remarquons tout de suite qu'un vecteur $(x_1, x_2) \in k((u^{1/b})) \otimes_{k((u))} M$ se décompose sur la base (f_1, f_2) sous la forme :

$$(x_1, x_2) = (x_1 u^{-\alpha} - x_2 c u^{-(\alpha+\delta)}) f_1 + x_2 u^{-\delta} f_2.$$

Ainsi il appartient à M si, et seulement si les deux coefficients que l'on voit apparaître dans l'écriture précédente sont de valuation positive ou nulle, c'est-à-dire si, et seulement si $\text{val}(x_1 - x_2 c u^{-\delta}) \geq \alpha$ et $\text{val}(x_2) \geq \delta$. On en déduit notamment que le plus petit n tel que $(x_1, x_2) \in u^n k[[u^{1/b}]] \otimes_{k[[u]]} L$ est le plus petit des deux nombres $\text{val}(x_2) - \delta$ et $\text{val}(x_1 - x_2 c u^{-\delta}) - \alpha$.

À partir de maintenant, nous supposons que $c = u^\gamma$ avec $\gamma < \delta < \alpha$, les autres cas se traitent au moyen de calculs analogues que nous laissons au lecteur. Déterminons tout d'abord la fonction $\tilde{\varphi}_1(L)$. Soit $v \in \frac{1}{b}\mathbb{Z}$. Considérons un vecteur $x \in k[[u^{1/b}]] \otimes_{k[[u]]} L$ tel que $\text{val}(x) = (v, 1)$. Quitte à multiplier x par un élément inversible de $k[[u^{1/b}]]$, ce qui ne change pas la valeur de la borne inférieure dans la formule (1.1), on peut supposer que x s'écrit $u^v \otimes e_1 + u^v y \otimes e_2$ où $y \in k[[u^{1/b}]]$. Comme nous l'avons déjà expliqué, le

³Et ce sera aussi le cas dans tout l'article.

fait que x appartienne par L se traduit par les inégalités $\text{val}(u^v y) \geq \delta$ et $\text{val}(u^v - u^{v+\gamma-\delta} y) \geq \alpha$, ce qui se réécrit encore :

$$\text{val}(y) \geq \delta - v \quad \text{et} \quad y \equiv u^{\delta-\gamma} \pmod{u^{\delta-\gamma+(\alpha-v)}} \quad (1.2)$$

Supposons pour commencer $v < \alpha$. Dans ce cas, la dernière congruence implique que y est de valuation $\delta - \gamma$, d'où on déduit $\delta - \gamma \geq \delta - v$, c'est-à-dire $v \geq \gamma$. Autrement dit, si $v < \gamma$, aucun x ne satisfait les conditions requises et on a alors $\tilde{\varphi}_1(L)(v) = -\infty$. Si, au contraire, $\gamma \leq v < \alpha$, il existe des x convenables qui sont précisément les vecteurs de la forme

$$x = u^v \otimes e_1 + u^{v+\delta-\gamma}(1 + u^{\alpha-v} z) \otimes e_2$$

pour un certain élément $z \in k[[u^{1/b}]]$. On obtient ainsi :

$$\begin{aligned} \tilde{\varphi}_1(L)(v) &= \sup_{z \in k[[u^{1/b}]]} \left(\min\{b(v + \delta - \gamma) - \delta, bv - \alpha + \text{val}(1 - u^{(b-1)(\delta-\gamma)}(1 + u^{b(\alpha-v)}\phi(z)))\} \right) \\ &= \sup_{z \in k[[u^{1/b}]]} \left(\min\{b(v + \delta - \gamma) - \delta, bv - \alpha\} \right) \quad \text{car } \delta - \gamma > 0 \\ &= \min\{b(v + \delta - \gamma) - \delta, bv - \alpha\} \end{aligned}$$

Or, $b(\delta - \gamma) > 0 > \delta - \alpha$, d'où on obtient finalement $\tilde{\varphi}_1(L)(v) = bv - \alpha$ pour $v \in [\gamma, \alpha[$.

Supposons désormais $v \geq \alpha$. Dans ce cas, la première condition de la ligne (1.2) est automatiquement vérifiée (on rappelle que y est dans $k[[u^{1/b}]]$) tandis que la congruence qui suit se réduit à $\text{val}(y) \geq \delta - \gamma + \alpha - v$. On est ainsi amené à calculer

$$\sup_y \left(\min\{b(v + \text{val}(y)) - \delta, bv - \alpha + \text{val}(1 - u^{\gamma-\delta}\phi(y))\} \right)$$

où la borne supérieure est prise sur tous les y dont la valuation est à la fois supérieure ou égale à 0 et à $\delta - \gamma + \alpha - v$. Pour les y de valuation strictement plus petite (resp. strictement plus grande) que $\frac{\delta-\gamma}{b}$, la valuation de la différence $1 - u^{\gamma-\delta}\phi(y)$ vaut $\gamma - \delta + b\text{val}(y)$ (resp. 0), et un calcul simple montre que le minimum qui apparaît dans la formule précédente vaut à nouveau $bv - \alpha$. Par contre, pour les y qui ont la valuation critique $\frac{\delta-\gamma}{b}$, la borne supérieure est clairement atteinte lorsque $1 - u^{\gamma-\delta}\phi(y)$ s'annule, et il est égal à $b(v + \text{val}(y)) - \delta = bv - \gamma$. Du fait que $\gamma < \alpha$, on déduit que la valeur de $\tilde{\varphi}_1(L)(v)$ est $bv - \gamma$ dès que l'on peut choisir y de valuation $\frac{\delta-\gamma}{b}$, c'est-à-dire dès que $\frac{\delta-\gamma}{b} \geq \delta - \gamma + \alpha - v$ ou encore après simplification $v \geq \alpha + \frac{b-1}{b}(\delta - \gamma)$, et qu'elle est $bv - \alpha$ dans le cas contraire.

En résumé, la fonction $\tilde{\varphi}_1(L)$ prend la forme simple suivante :

$$\begin{aligned} \tilde{\varphi}_1(L) : \quad v &\mapsto -\infty && \text{si } v < \gamma \\ &\mapsto bv - \alpha && \text{si } \gamma \leq v < \alpha + \frac{b-1}{b}(\delta - \gamma) \\ &\mapsto bv - \gamma && \text{sinon.} \end{aligned}$$

Déterminons à présent la fonction $\tilde{\varphi}_2(L)$. Soit $x \in L$ tel que $\text{val}_M(x) = (v, 2)$. Comme dans le cas précédent, quitte à multiplier x par un élément inversible de $k[[u^{1/b}]]$, on peut supposer qu'il est de la forme $x = u^v y \otimes e_1 + u^v \otimes e_2$ où $y \in k((u^{1/b}))$ est un élément de valuation strictement positive. Du fait que x est élément de L , on déduit $\text{val}(y - u^{\gamma-\delta}) \geq \alpha - v$, soit encore $\gamma - \delta \geq \alpha - v$ car $\gamma - \delta < 0 < \text{val}(y)$, et donc la valuation de la différence $y - u^{\gamma-\delta}$ est $\gamma - \delta$. Ainsi si $v < \alpha + \delta - \gamma$, aucun élément y ne satisfait aux conditions requises, et donc $\tilde{\varphi}_2(L)(v) = -\infty$. Par contre, si $v \geq \alpha + \delta - \gamma$, tous les y de valuation strictement positive conviennent et un calcul analogue à celui mené pour $\tilde{\varphi}_1(L)$ conduit dans ce cas à $\tilde{\varphi}_2(L)(v) = bv - \alpha + \gamma - \delta$. En résumé, on a donc :

$$\begin{aligned} \tilde{\varphi}_2(L) : \quad v &\mapsto -\infty && \text{si } v < \alpha + \delta - \gamma \\ &\mapsto bv - \alpha + \gamma - \delta && \text{sinon.} \end{aligned}$$

On observe sans difficulté que $\tilde{\varphi}_1(L)(v) \geq \tilde{\varphi}_2(L)(v)$ pour tout $v \in \frac{1}{b}\mathbb{Z}$; ainsi obtient-on $\varphi_1(L) = \tilde{\varphi}_1(L)$ et $\varphi_2(L) = \tilde{\varphi}_2(L)$. Il est maintenant facile de vérifier la proposition 1.2 sur cet exemple et en particulier de

décrire les fonctions $\psi_1(L)$ et $\psi_2(L)$. On trouve :

$$\begin{aligned} \psi_1(L) : \quad & \mu \mapsto -\infty && \text{si } \mu < b(\alpha + \delta - \gamma) - \delta \\ & \mu \mapsto b^{-1}(\mu + \gamma) && \text{sinon} \\ \\ \psi_2(L) : \quad & \mu \mapsto -\infty && \text{si } \mu < b\gamma - \alpha \\ & \mu \mapsto b^{-1}(\mu + \alpha) && \text{si } b\gamma - \alpha \leq \mu < (b-1)(\alpha + \delta - \gamma) \\ & \mu \mapsto b^{-1}(\mu + \alpha + \delta - \gamma) && \text{sinon.} \end{aligned}$$

Les entiers $\mu_1(L)$ et $\mu_2(L)$ valent donc respectivement $b(\alpha + \delta - \gamma) - \delta$ et $b\gamma - \alpha$, et l'on peut vérifier par un calcul indépendant que ce sont bien les exposants des diviseurs élémentaires du $k[[u]]$ -module engendré par $\phi(L)$ par rapport à L .

1.1.3 Prolongement des fonctions φ_i

Pour la suite, il sera commode, afin de mieux visualiser les fonctions $\varphi_i(L)$ de les prolonger à tout \mathbb{R} en posant

$$\varphi_i(q) = \varphi_i(v) + b(q - v) \quad \text{pour tout } q \in [v, v + \frac{1}{b}[$$

et en convenant que $-\infty + x = -\infty$ pour tout nombre réel x . On prolonge de la même façon les fonctions $\tilde{\varphi}_i(L)$. Il est alors clair que pour tout réel q les nombres $\varphi_1(L)(q), \dots, \varphi_d(L)(q)$ sont les mêmes que $\tilde{\varphi}_1(L)(q), \dots, \tilde{\varphi}_d(L)(q)$ mais triés par ordre décroissant. Il est également évident que les fonctions $\tilde{\varphi}_i(L)$ et $\varphi_i(L)$ sont continues à droite et affines par morceaux, et que leurs dérivées valent b partout où elles sont définies. Les fonctions $\psi_j(L)$ données par la proposition 1.2 se prolongent elles aussi à \mathbb{R} tout entier en convenant qu'elles valent $-\infty$ sur l'intervalle $] - \infty, \mu_j(L)[$ et qu'elles sont affines de pente $\frac{1}{b}$ sur tout intervalle de la forme $[\mu, \mu + 1[$ où μ est un nombre entier supérieur ou égal à $\mu_j(L)$. Ces fonctions ainsi prolongées vérifient encore la condition de l'alinéa 3 da la proposition 1.2 lorsque v et μ sont des éléments de \mathbb{R} .

La méthode que nous avons employée pour prolonger les fonctions φ_i et ψ_j à tout \mathbb{R} peut sembler artificielle, mais en fait il n'en est rien comme le montre la proposition suivante.

Proposition 1.3. *On note $k[[u^{1/\infty}]] = \bigcup_{n \geq 1} k[[u^{1/n}]]$ (resp. $k((u^{1/\infty})) = \bigcup_{n \geq 1} k((u^{1/n}))$) l'anneau (resp. le corps) des séries de Puiseux à coefficients dans k . Alors pour tout $i \in \{1, \dots, d\}$ et tout nombre rationnel q , on a :*

$$\tilde{\varphi}_i(L)(q) = \sup_{\substack{x \in k[[u^{1/\infty}]] \otimes_{k[[u]]} L \\ \text{val}_{M, \mathbb{Q}}(x) = (q, i)}} \left(\inf \{ n \in \mathbb{Q} \mid \phi(x) \in u^n(k[[u^{1/\infty}]] \otimes_{k[[u]]} L) \} \right)$$

où $\text{val}_{M, \mathbb{Q}}$ désigne le prolongement naturel de val_M à $k((u^{1/\infty})) \otimes_{k[[u]]} M$.

Remarque 1.4. En d'autres termes, la proposition dit que la fonction

$$q \mapsto \sup_{\substack{x \in k[[u^{1/\infty}]] \otimes_{k[[u]]} L \\ \text{val}_{M, \mathbb{Q}}(x) = (q, i)}} \left(\inf \{ n \in \mathbb{Q} \mid \phi(x) \in u^n(k[[u^{1/\infty}]] \otimes_{k[[u]]} L) \} \right)$$

est entièrement déterminée par ses valeurs sur l'ensemble $\frac{1}{b}\mathbb{Z}$ et que, de surcroît, pour calculer les valeurs en ces points, on peut se contenter d'étendre les scalaires à $k((u^{1/b}))$ (sans aller, donc, jusqu'aux séries de Puiseux).

Démonstration. Étant donné que la proposition nous sera pas utilisée dans la suite, nous nous contentons de donner quelques indications sur sa preuve. L'idée directrice est de comprendre comment l'on peut calculer de façon algorithmique la borne supérieure qui apparaît dans l'énoncé de la proposition et que nous noterons $f_i(L)(q)$ dans le restant de la preuve. Dans la suite, on notera également (e_1, \dots, e_d) la base canonique de M . L'entier i restant fixé, concentrons-nous tout d'abord sur le calcul de la borne inférieure des q tels qu'il existe dans $k[[u^{1/\infty}]] \otimes_{k[[u]]} L$ des éléments de valuation (q, i) . Nous noterons cette q_i cette borne

inférieure. Dire que $k[[u^{1/\infty}]] \otimes_{k[[u]]} L$ contient un élément de valuation (q, i) signifie exactement qu'il existe un nombre rationnel $\varepsilon > 0$ tel que

$$u^q e_i \in L + \sum_{j=1}^i u^{q+\varepsilon} e_j + \sum_{j=i+1}^d u^q e_j.$$

Si l'on fixe m_1, \dots, m_d une base de L et que l'on note M_i (resp. E_i) le vecteur colonne des coordonnées de m_i (resp. e_i) dans la base canonique, la condition précédente signifie que le vecteur colonne $u^q E_i$ est dans l'image de la matrice par blocs

$$(M_1 \mid M_2 \mid \dots \mid M_d \mid u^{q+\varepsilon} E_1 \mid \dots \mid u^{q+\varepsilon} E_i \mid u^q E_{i+1} \mid \dots \mid u^q E_d).$$

On peut à présent effectuer des opérations sur les colonnes de la matrice précédente (ce qui ne modifie pas son image) pour se ramener à permutation des lignes près à une matrice de la forme

$$\begin{pmatrix} u^{n_1} & 0 & \dots & \dots & 0 \\ \star & \dots & \dots & \dots & \dots \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ \star & \dots & \star & u^{n_d} & 0 & \dots & 0 \end{pmatrix}$$

pour certains nombres rationnels n_j ($1 \leq j \leq d$) rangés par ordre croissant. En outre, un examen de l'algorithme classique de calcul de la forme normale précédente permet d'établir la dépendance en q et ε (pourvu que ce dernier reste suffisamment petit) des n_j : on trouve qu'il existe des entiers $v_1 < \dots < v_n$ et $c_0 < \dots < c_n$ tels que, en posant $v_0 = -\infty$ et $v_{n+1} = +\infty$, on ait sur chaque intervalle $[v_s, v_{s+1}[$, soit $n_j = c_s$, soit $n_j = q + c_s$, soit $n_j = q + \varepsilon + c_s$. Il est enfin possible d'exprimer q_i en fonction des c_s , à partir de quoi l'on déduit que q_i est entier. Il résulte également de ces considérations qu'il existe dans L (sans tensoriser par $k[[u^{1/\infty}]]$) un élément de valuation (q_i, i) puisque dans le cas où q est un nombre entier, toutes les opérations que nous avons effectuées peuvent se faire également dans $k[[u]]$.

Pour $q < q_i$, la proposition est clairement vraie puisque les deux nombres qui apparaissent dans l'égalité à établir valent tous deux $-\infty$. D'autre part, dans tous les cas, dire que $n \geq f_i(q)$ signifie que l'implication suivante est vraie :

$$(x \in k[[u^{1/\infty}]] \otimes_{k[[u]]} L \text{ et } \text{val}(x) = (q, i)) \implies \phi(x) \in u^n (k[[u^{1/\infty}]] \otimes_{k[[u]]} L). \quad (1.3)$$

Or, si $z_i \in L$ est un élément fixé de valuation (q_i, i) et si l'on suppose $q \geq q_i$, un élément x vérifie la prémisse de l'implication si, et seulement si

$$x - u^{q-q_i} z_i \in (k[[u^{1/\infty}]] \otimes_{k[[u]]} L) \cap \left(\sum_{j=1}^i u^{q+\varepsilon} e_j + \sum_{j=i+1}^d u^q e_j \right)$$

pour un certain $\varepsilon > 0$. On conclut alors de manière semblable à ce qui a été déjà fait : on commence par calculer l'intersection qui apparaît dans la formule précédente en effectuant des opérations sur les lignes d'une matrice, et réinjectant cela dans l'implication (1.3), on trouve qu'il existe des entiers $v_1 < \dots < v_n$ et $c_0 < \dots < c_n$ tel que sur chaque intervalle $[\frac{v_s}{b}, \frac{v_{s+1}}{b}[$, on ait $f_i(L)(q) = bq - c_s$. Ce faisant, on obtient également que $f_i(L)(q) = \tilde{\varphi}_i(L)(q)$ si $q \in \frac{1}{b}\mathbb{Z}$, d'où il résulte la proposition. \square

En s'autorisant à travailler dans des corps encore plus gros que $k((u^{1/\infty}))$, on peut aussi interpréter les nombres $\tilde{\varphi}_i(L)(q)$ pour $q \in \mathbb{R}$ comme des bornes supérieures du type précédent. Par exemple, on peut considérer l'anneau $k[[u^{\mathbb{R}^+}]]$ formé des séries formelles $\sum_{i \in I} a_i u^i$ où $I \subset \mathbb{R}^+$ est un monoïde de type fini. Celui-ci est encore muni d'une valuation naturelle qui permet de définir $\text{val}_{M, \mathbb{R}}$ sur $k[[u^{\mathbb{R}^+}]] \otimes_{k[[u]]} M$. On a alors pour tout nombre réel q :

$$\tilde{\varphi}_i(L)(q) = \sup_{\substack{x \in k[[u^{\mathbb{R}^+}]] \otimes_{k[[u]]} L \\ \text{val}_{M, \mathbb{R}}(x) = (q, i)}} \left(\inf \{ n \in \mathbb{R} \mid \phi(x) \in u^n (k[[u^{\mathbb{R}^+}]] \otimes_{k[[u]]} L) \} \right)$$

la démonstration étant en tout point analogue à celle de la proposition précédente.

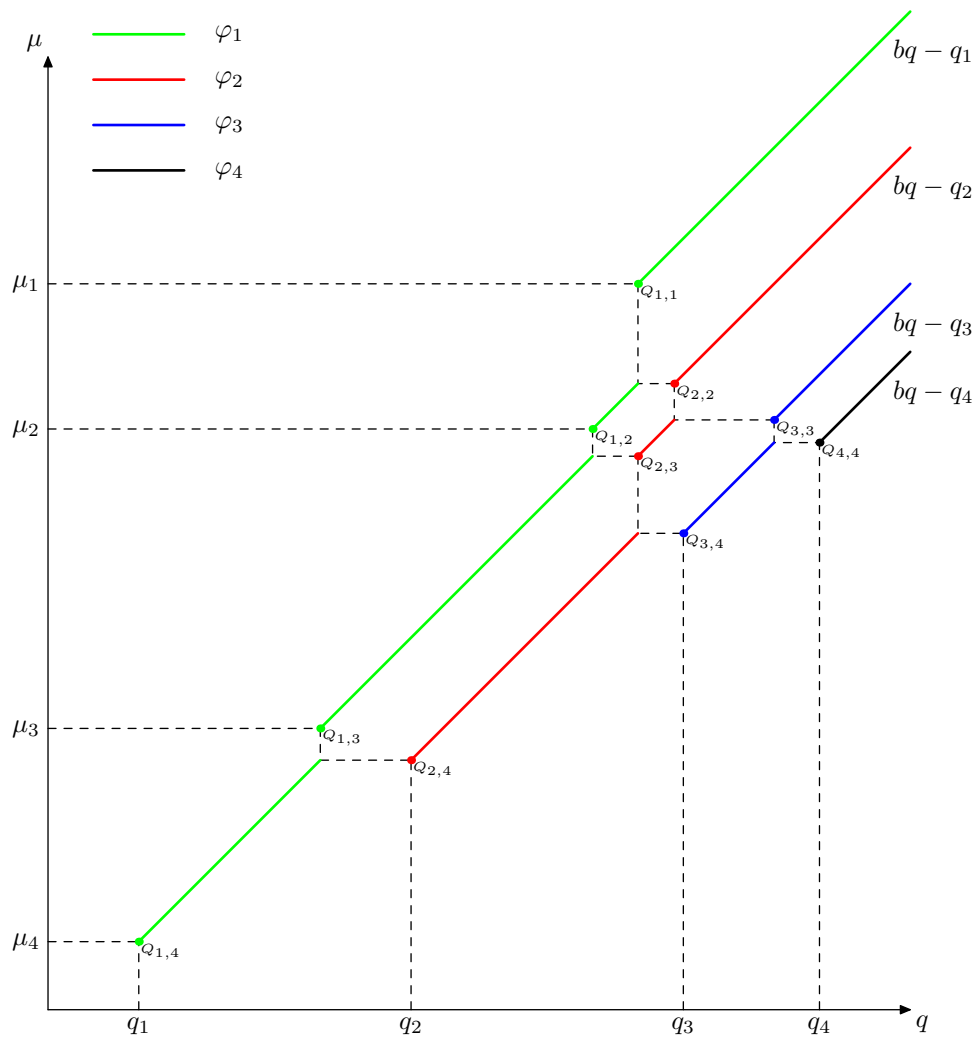


FIG. 1 – Un exemple de d -uplet $(\varphi_1, \dots, \varphi_d)$ appartenant à Φ avec $d = 4$

1.2 Paramétrisation de l'espace des fonctions φ

Nous nous proposons désormais de décrire complètement les d -uplets $\varphi = (\varphi_1, \dots, \varphi_d)$ où les φ_i sont des fonctions de \mathbb{R} dans $\mathbb{R} \cup \{-\infty\}$ qui satisfont aux conditions suivantes :

1. on a $\varphi_1 \geq \varphi_2 \geq \dots \geq \varphi_d$;
2. les fonctions φ_i sont strictement croissantes⁴ et continues à droite ;
3. pour tout i , il existe un nombre réel q_i (nécessairement unique) tel que
 - la fonction φ_i prend des valeurs finies exactement sur l'intervalle $[q_i, +\infty[$,
 - la fonction φ_i est affine par morceaux sur $[q_i, +\infty[$ et pour presque tout q dans cet intervalle, on a $\varphi_i'(q) = b$, et
 - pour q suffisamment grand, on a $\varphi_i(q) = bq - q_i$;
4. pour $j \in \{1, \dots, d\}$, il existe des fonctions strictement croissantes et continues à droites $\psi_j : \mathbb{R} \rightarrow \mathbb{R} \cup \{-\infty\}$ telles que $\psi_1 \leq \psi_2 \leq \dots \leq \psi_d$ et pour tout couple $(q, \mu) \in \mathbb{R}^2$, il y a autant d'indices $i \in \{1, \dots, d\}$ tels que $\mu = \varphi_i(q)$ que d'indices $j \in \{1, \dots, d\}$ tels que $q = \psi_j(\mu)$.

À partir de maintenant, nous notons Φ l'ensemble des d -uplets de fonctions $\varphi = (\varphi_1, \dots, \varphi_d)$ vérifiant les conditions précédentes. Notons que si, par la proposition 1.2, les $\varphi(L) = (\varphi_1(L), \dots, \varphi_d(L))$ provenant d'un réseau $L \subset M$ définissent bien des éléments de Φ , il n'est pas vrai que, réciproquement, tout élément de Φ s'obtient de cette manière. En effet, si φ provient d'un réseau, il vérifie en outre au moins les deux propriétés supplémentaires suivantes :

5. pour tout i , le réel q_i est un nombre entier ;
6. pour tout i , les réels en lesquels φ_i est discontinue appartiennent à $\frac{1}{b}\mathbb{Z}$.

Nous appelons *conditions d'intégrité* les deux conditions qui viennent d'être écrites, et nous notons $\Phi_{\mathbb{Z}}$ l'ensemble des éléments de Φ qui les satisfont.

1.2.1 Les réels $q_{i,j}$ et $\mu_{i,j}$

Soient $\varphi = (\varphi_1, \dots, \varphi_d) \in \Phi$ et $\psi = (\psi_1, \dots, \psi_d)$ le d -uplet de fonctions correspondant.

On suppose pour commencer — et il s'agit d'une hypothèse qui évitera bien des problèmes techniques — que $\varphi_1 < \dots < \varphi_d$ où, étant donné deux fonctions $f, g : \mathbb{R} \rightarrow \mathbb{R} \cup \{-\infty\}$, on convient que $f < g$ si $f(q) \leq g(q)$ pour tout réel q et que l'inégalité est stricte dès que $g(q) \neq -\infty$. Prolongeons les fonctions φ_i et ψ_j à $\mathbb{R} \cup \{-\infty\}$ en posant $\varphi_i(-\infty) = \psi_j(-\infty) = -\infty$. Pour tout couple (i, j) d'entiers vérifiant $1 \leq i \leq j \leq d$, définissons :

- le nombre $q_{i,j}$ comme la borne inférieure des nombres réels q tels que $\psi_j \circ \varphi_i(q) \geq q$;
- le nombre $\mu_{i,j}$ comme la borne inférieure des nombres réels μ tels que $\varphi_i \circ \psi_j(\mu) \geq \mu$.

Remarquons tout de suite que l'ordre dans lequel sont classés les φ_i et les ψ_j impose que les fonctions φ_i et ψ_j sont inverses l'une de l'autre sur des voisinages de $+\infty$. On en déduit qu'il existe toujours des q et des μ satisfaisant les inégalités précédentes. Par ailleurs si q (resp. μ) est suffisamment petit, on a $\varphi_i(q) = -\infty$ pour tout i (resp. $\psi_j(\mu) = -\infty$ pour tout j). On en déduit que les $q_{i,j}$ et $\mu_{i,j}$ sont bien des nombres réels. Par ailleurs, il est clair que $q_{i,j} \leq q_{i+1,j}$, $q_{i,j} \geq q_{i,j+1}$, $\mu_{i,j} \leq \mu_{i+1,j}$ et $\mu_{i,j} \geq \mu_{i,j+1}$ pour tout couple (i, j) pour lequel cela a un sens. Dans la suite, pour des raisons pratiques, nous poserons également $q_{i,i-1} = \mu_{j,j+1} = +\infty$.

Lemme 1.5. *Pour tout entiers i et j tels que $1 \leq i \leq j \leq d$, on a*

$$\mu_{i,j} \leq \varphi_i(q_{i,j}) \quad \text{et} \quad q_{i,j} \leq \psi_j(\mu_{i,j}).$$

De plus ces inégalités sont des égalités si, et seulement si, il existe q tel que $\psi_j \circ \varphi_i(q) = q$ si, et seulement si, il existe μ tel que $\varphi_i \circ \psi_j(\mu) = \mu$.

Démonstration. La croissance et la continuité à droite des fonctions φ_i et ψ_j impliquent que $\psi_j \circ \varphi_i$ est aussi continue à droite. On en déduit que $\psi_j \circ \varphi_i(q_{i,j}) \geq q_{i,j}$. À partir de là, en appliquant φ_i , on obtient $\varphi_i \circ \psi_j(\mu) \geq \mu$ avec $\mu = \varphi_i(q_{i,j})$. Par définition de la borne inférieure, il vient $\mu_{i,j} \leq \mu$ comme annoncé. On démontre de même l'autre inégalité.

⁴On rappelle que l'on entend par là que les φ_i sont croissantes et strictement croissantes sur l'intervalle où elles prennent des valeurs finies

Il est clair que si les inégalités sont des égalités, alors il existe q et μ satisfaisant la condition du lemme : il suffit de prendre $q = q_{i,j}$ et $\mu = \mu_{i,j}$. Supposons maintenant qu'il existe q tel que $\psi_j \circ \varphi_i(q) = q$. Du fait que la fonction $\psi_j \circ \varphi_i - \text{id}$ est en escalier (puisqu'elle est affine par morceaux et que sa dérivée s'annule partout où elle est définie), on déduit facilement que $\psi_j \circ \varphi_i(q_{i,j}) = q_{i,j}$. Appliquons maintenant ψ_j à la première égalité du lemme : cela donne $\psi_j(\mu_{i,j}) \leq q_{i,j}$ et donc finalement $\psi_j(\mu_{i,j}) = q_{i,j}$. L'autre égalité se démontre de même analogue en appliquant φ_i à la deuxième inégalité du lemme. Le cas où il existe μ tel que $\varphi_i \circ \psi_j(\mu) = \mu$ se traite pareillement. \square

Dans le cas où l'une des inégalités du lemme est stricte, nous dirons que le couple (i, j) est *dégénéré*. Notons que les couples de la forme (i, i) ne sont jamais dégénérés puisque l'on a dit que sur des voisinages de l'infini les fonctions φ_i et ψ_i étaient inverses l'une de l'autre. En particulier, on a toujours $\varphi_i(q_{i,i}) = \mu_{i,i}$ et $\psi_i(\mu_{i,i}) = q_{i,i}$.

Proposition 1.6. *Soit $\varphi = (\varphi_1, \dots, \varphi_d) \in \Phi$ tel que $\varphi_1 < \dots < \varphi_d$. Alors, pour tout couple (i, j) , les fonctions φ_i et ψ_j définissent par restriction des bijections*

$$\varphi_i|_{[q_{i,j}, q_{i,j-1}[} : [q_{i,j}, q_{i,j-1}[\rightarrow [\mu_{i,j}, \mu_{i+1,j}[\quad \text{et} \quad \psi_j|_{[\mu_{i,j}, \mu_{i+1,j}[} : [\mu_{i,j}, \mu_{i+1,j}[\rightarrow [q_{i,j}, q_{i,j-1}[$$

inverses l'une de l'autre. (On notera qu'il est possible que les intervalles précédents soient vides.)

De plus, pour tout i (resp. tout j), la fonction φ_i (resp. ψ_j) vaut $-\infty$ sur l'intervalle $] - \infty, q_{i,d}[$ (resp. l'intervalle $] - \infty, \mu_{1,j}[$).

Remarque 1.7. Telle quelle, la proposition est fausse sans l'hypothèse $\varphi_1 < \dots < \varphi_d$. Nous expliquerons sommairement au §1.2.3 comment modifier la définition des $q_{i,j}$ et $\mu_{i,j}$ pour que la proposition s'étende sans cette hypothèse.

Démonstration. On raisonne par récurrence sur j en commençant par traiter le cas $j = 1$. Puisque ψ_1 est strictement croissante, il est clair qu'elle prend des valeurs finies exactement sur un intervalle de la forme $[\mu_1, +\infty[$ pour $\mu_1 \in \mathbb{R}$. Du fait que ψ_1 est la plus petite des fonctions ψ_j , on déduit que la réunion des graphes des φ_i n'intersecte pas la région du plan suivante :

$$D_1 = \{ (q, \mu) \in \mathbb{R}^2 \mid q < \psi_1(\mu) \}.$$

Si μ est un réel plus grand ou égal à μ_1 , considérons $q = \psi_1(\mu)$ et μ' un réel strictement supérieur à μ . Alors, étant donné que ψ est croissante, le couple (q, μ') est dans D_1 , ce qui signifie que $\varphi_i(q) \neq \mu'$ pour tout i . Comme ceci est vrai pour tout $\mu' > \mu$, on obtient $\varphi_i(q) \leq \mu$, i.e $\varphi_i \circ \psi_1(\mu) \leq \mu$. Par ailleurs, on sait que cette inégalité doit être une inégalité pour au moins un i . Si i_0 est cet indice privilégié, on a $\mu = \varphi_{i_0} \circ \psi_1(\mu) \leq \varphi_1 \circ \psi_1(\mu) \leq \mu$ car les φ_i sont triés par ordre décroissant. Ainsi $\varphi_1 \circ \psi_1(\mu) = \mu$, et ce pour tout $\mu \geq \mu_1$. On en déduit que $\mu_{1,1} \leq \mu_1$. Mais comme ψ_1 vaut $-\infty$ sur les $\mu < \mu_1$, il vient $\mu_{1,1} = \mu_1$ et donc $q_{1,1} = \psi_1(\mu_1)$. En outre, sur l'intervalle $[\mu_{1,1}, +\infty[$ la fonction ψ_1 est inversible à gauche, et son inverse à gauche est la restriction de φ_1 à $[q_{1,1}, +\infty[$. Du fait que ces fonctions sont en outre affines par morceaux et strictement croissantes, on déduit facilement ce qui est énoncé dans la proposition.

Plutôt que de traiter l'hérédité de la récurrence dans le cas général — ce qui multiplierait encore les notations —, nous allons nous contenter d'expliquer comment le cas « $j = 2$ » se déduit de ce que l'on vient de faire, les arguments pour les j supérieurs étant similaires. Comme précédemment, on commence par remarquer que la fonction ψ_2 prend des valeurs finies exactement sur un intervalle de la forme $[\mu_2, +\infty[$ pour un certain nombre réel μ_2 . De $\psi_2(\mu_{1,1}) \geq \psi_1(\mu_{1,1}) > -\infty$, on tire $\mu_2 \leq \mu_{1,1}$. Considérons le domaine :

$$D_2 = \{ (q, \mu) \in \mathbb{R}^2 \mid q < \psi_2(\mu) \}.$$

Des résultats de l'étude menée pour $j = 1$, on déduit que D_2 intersecte la réunion des graphes de φ_i au plus selon le graphe de la restriction de φ_1 à l'intervalle $[q_{1,1}, +\infty[$. Soit $\mu \geq \mu_2$. Posons $q = \psi_2(\mu)$ et considérons un nombre réel $\mu' > \mu$. Le couple (q, μ) appartenant à D_2 , il en résulte que :

- si $q < q_{1,1}$, alors $\varphi_i(q) \neq \mu'$ pour tout $i \in \{1, \dots, d\}$;
- si $q \geq q_{1,1}$, alors $\varphi_i(q) \neq \mu'$ pour tout $i \in \{2, \dots, d\}$.

Les conclusions précédentes étant valables pour tout $\mu' > \mu$, on peut remplacer dans leurs énoncés « $\varphi_i(q) \neq \mu'$ » par « $\varphi_i(q) \leq \mu$ ». En utilisant le fait que les fonctions φ_i sont triées par ordre décroissant, et que la fonction φ_1 est connue sur $[q_{1,1}, +\infty[$, on obtient pour tout $\mu \geq \mu_2$:

- si $\psi_2(\mu) < q_{1,1}$, alors $\varphi_1 \circ \psi_2(\mu) = \mu$;

– si $\psi_2(\mu) \geq q_{1,1}$, alors $\varphi_2 \circ \psi_2(\mu) = \mu$, et donc $\varphi_1 \circ \psi_2(\mu) \geq \mu$.

On déduit déjà de cela que $\mu_{1,2} = \mu_2$ puisque $\varphi_1 \circ \psi_2(\mu)$ vaut $-\infty$ si $\mu < \mu_2$ et est supérieur ou égal à μ sinon. On a également $\psi_2(\mu_{2,2}) = q_{2,2}$ et $\varphi_2(q_{2,2}) = \mu_{2,2}$ étant donné que le couple $(2, 2)$ n'est pas dégénéré. Soit μ' l'infimum des nombres réels μ tels que $\psi_2(\mu) < q_{1,1}$. La restriction de ψ_2 à $[\mu_{1,2}, \mu'[,$ admet alors pour inverse φ_1 tandis que sa restriction à $[\mu', +\infty[$ admet pour inverse φ_2 . Pour conclure, il suffit donc de montrer que $\mu' = \mu_{2,2}$ et que si $\mu_{1,2} < \mu_{2,2}$ alors $\psi_2(\mu_{1,2}) = q_{1,2}$. Du fait que $\varphi_2 \circ \psi_2(\mu') = \mu'$, on déduit que $\mu_{2,2} \leq \mu'$. Mais si l'inégalité était stricte, on aurait $\varphi_1 = \varphi_2$ sur l'intervalle de la forme $[q_{1,1} - \varepsilon, q_{1,1}[,$ (pour $\varepsilon > 0$), ce que l'on a exclu au départ. L'autre point résulte maintenant aisément des descriptions que l'on vient d'obtenir. \square

Étant donné qu'une fonction définie sur un intervalle à valeurs dans un autre intervalle, qui est à la fois affine par morceaux et bijective est affine, on déduit facilement de la proposition la description suivante des fonctions φ_i et ψ_j :

$$\begin{aligned} \varphi_i : \quad q &\mapsto -\infty && \text{si } q < q_{i,d} \\ &q \mapsto b(q - q_{i,j}) + \mu_{i,j} && \text{si } q_{i,j} \leq q < q_{i,j-1}, \quad \text{et ce pour tout } j \in \{i, \dots, d\} \\ \psi_j : \quad \mu &\mapsto -\infty && \text{si } \mu < \mu_{1,j} \\ &\mu \mapsto b^{-1}(\mu - \mu_{i,j}) + q_{i,j} && \text{si } \mu_{i,j} \leq \mu < \mu_{i+1,j}, \quad \text{et ce pour tout } i \in \{1, \dots, j\} \end{aligned} \quad (1.4)$$

Il résulte en particulier de cette écriture que les fonctions φ_i sont entièrement déterminées par la donnée des $q_{i,j}$ et $\mu_{i,j}$.

1.2.2 Relations entre les $q_{i,j}$ et $\mu_{i,j}$

On sait déjà que les nombres $q_{i,j}$ et $\mu_{i,j}$ ne peuvent être quelconques puisque ceux-ci vérifient les inégalités $q_{i,j} \leq q_{i+1,j}$, $q_{i,j} \geq q_{i,j+1}$, $\mu_{i,j} \leq \mu_{i+1,j}$ et $\mu_{i,j} \geq \mu_{i,j+1}$. En réalité, ces nombres sont soumis à un certain nombre d'autres contraintes que nous nous proposons d'étudier maintenant.

Relations égalitaires On considère $\varphi = (\varphi_1, \dots, \varphi_d) \in \Phi$ et on suppose encore $\varphi_1 < \dots < \varphi_d$. Par définition, au voisinage de $+\infty$, la fonction φ_i est donnée par $q \mapsto bq - q_{i,d}$ (puisque la fonction φ_i prend des valeurs finis à partir de $q_{i,d}$). En comparant avec la forme de φ_i que nous avons obtenu ci-dessus, on trouve :

$$\mu_{i,i} = bq_{i,i} - q_{i,d} \quad (1.5)$$

pour tout $i \in \{1, \dots, d\}$. D'autre part, par la proposition 1.6, la fonction φ_i réalise une bijection de l'intervalle $[q_{i,j}, q_{i,j-1}[,$ sur l'intervalle $[\mu_{i,j}, \mu_{i+1,j}[,$. Comme on sait que cette fonction dilate la mesure de Lebesgue d'un facteur b , il vient :

$$\mu_{i+1,j} - \mu_{i,j} = b(q_{i,j-1} - q_{i,j}) \quad (1.6)$$

pour tout $i, j \in \{1, \dots, d\}$ tels que $1 \leq i < j \leq d$. À partir des deux relations que nous venons d'écrire, on voit facilement que les $\mu_{i,j}$ s'expriment en fonction des $q_{i,j}$:

$$\mu_{i,j} = bq_{j,j} - q_{j,d} + b \cdot \sum_{s=i}^{j-1} (q_{s,j} - q_{s,j-1}) \quad (1.7)$$

pour tout couple (i, j) tel que $1 \leq i \leq j \leq d$. En fait, la formule (1.7) implique réciproquement les formules (1.5) et (1.6). Ainsi, on peut décider d'oublier ces deux dernières relations et de ne travailler qu'avec les $q_{i,j}$. On peut également inverser les formules (1.7) et exprimer les $q_{i,j}$ en fonction des $\mu_{i,j}$; on obtient pour $1 \leq i \leq j \leq d$

$$q_{i,j} = \frac{1}{b-1} \cdot \left(\mu_{i,i} + \sum_{s=i+1}^j (\mu_{i,s} - \mu_{i+1,s}) + \sum_{s=j+1}^d \frac{\mu_{i,s} - \mu_{i+1,s}}{b} \right). \quad (1.8)$$

Il est donc également possible de décider d'oublier les $q_{i,j}$ et de travailler uniquement avec les $\mu_{i,j}$. L'avantage, néanmoins, de continuer à considérer simultanément les $q_{i,j}$ et les $\mu_{i,j}$ est que les formules qui apparaîtront pourront s'écrire manière plus agréable.

Relations inégales Rappelons que nous avons déjà vu les inégalités

$$q_{i,j} \geq q_{i,j+1} \quad ; \quad \mu_{i,j} \leq \mu_{i+1,j} \quad (1.9)$$

$$q_{i,j} \leq q_{i+1,j} \quad ; \quad \mu_{i,j} \geq \mu_{i,j+1} \quad (1.10)$$

pour tout couple (i, j) pour lequel cela a un sens.

Lemme 1.8. Avec les notations précédentes, on a les relations supplémentaires :

$$q_{i,j} \leq q_{i+1,j+1} \quad \text{et} \quad \mu_{i,j} \geq \mu_{i+1,j+1} \quad (1.11)$$

pour tout couple (i, j) tel que $1 \leq i < j \leq d$.

Démonstration. On démontre seulement la première inégalité, la seconde étant complètement analogue. Si $q_{i,j} = q_{i,j+1}$ ou $q_{i+1,j+1} = q_{i+1,j}$, l'inégalité résulte de (1.10). On peut donc supposer $q_{i,j} < q_{i,j+1}$ et $q_{i+1,j+1} < q_{i+1,j}$. Dans ce cas, on applique la proposition 1.6 qui nous assure que la fonction ψ_{j+1} réalise une bijection croissante de $[\mu_{i,j+1}, \mu_{i+1,j+1}[$ dans $[q_{i,j+1}, q_{i,j}[$, et également de $[\mu_{i+1,j+1}, \mu_{i+2,j+1}[$ dans $[q_{i+1,j+1}, q_{i+1,j}[$. Notons que d'après notre hypothèse, tous ces intervalles sont non vides. On en déduit que $\lim_{\mu \rightarrow \mu_{i+1,j+1}^-} \psi_{j+1}(\mu) = q_{i,j}$ et que $\psi_{j+1}(\mu_{i+1,j+1}) = q_{i+1,j+1}$. En utilisant la croissance de ψ_{j+1} , on obtient finalement $q_{i,j} \leq q_{i+1,j+1}$ comme voulu. \square

Remarquons que les inégalités (1.10) résultent de (1.9) et (1.11). En outre, en vertu de l'égalité (1.6), les deux inégalités de la ligne (1.9) se déduisent mutuellement l'une de l'autre. Ainsi, les six jeux d'inégalités que nous avons obtenues se résument finalement aux trois suivants :

$$q_{i,j} \geq q_{i,j+1} \quad ; \quad q_{i,j} \leq q_{i+1,j+1} \quad ; \quad \mu_{i,j} \geq \mu_{i+1,j+1}. \quad (1.12)$$

où (i, j) parcourt l'ensemble des couples d'entiers tels que $1 \leq i \leq j < d$. Signalons finalement que, bien entendu, les inégalités portant sur les $\mu_{i,j}$ peuvent se réécrire en termes de $q_{i,j}$ en utilisant la formule (1.7), et réciproquement en utilisant la formule (1.8).

1.2.3 Un mot sur la gestion des multiplicités

Dans ce qui précède, on a supposé pour simplifier que $\varphi_1 < \dots < \varphi_d$, c'est-à-dire si l'on préfère qu'il n'y a aucun point (q, μ) qui appartient simultanément aux graphes de plusieurs fonctions φ_i . Dans le cas où cette condition n'est pas réalisée, des complications techniques apparaissent. En particulier, la définition des $q_{i,j}$ et $\mu_{i,j}$ n'est plus correcte et doit être remplacée par :

- le nombre $q_{i,j}$ est la borne inférieure des nombres réels q tels que soit $\psi_j \circ \varphi_i(q) < q$, soit $\psi_j \circ \varphi_i(q) = q$ et

$$\text{Card} \{ i' \leq i \mid \varphi_{i'}(q) = \mu \} \leq \text{Card} \{ j' \leq j \mid \psi_{j'}(\mu) = q \} \quad (1.13)$$

où on a posé $\mu = \varphi_i(q)$;

- le nombre $\mu_{i,j}$ est la borne inférieure des nombres réels μ tels que soit $\varphi_i \circ \psi_j(\mu) < \mu$, soit $\varphi_i \circ \psi_j(\mu) = \mu$ et l'inégalité (1.13) est vérifiée avec $q = \psi_j(\mu)$.

Dans le cas où $\varphi_1 < \dots < \varphi_d$, on retrouve bien la définition donnée auparavant. En effet, il y a alors un unique indice i' (resp. j') tel que $\mu = \varphi_{i'}(q)$ (resp. $q = \psi_{j'}(\mu)$) à savoir $i' = i$ (resp. $j' = j$), et donc la condition supplémentaire est toujours vérifiée. L'idée dans cette définition est que si, étant donné un couple (q, μ) , on note $i_1 < i_2 < \dots < i_k$ et $j_1 < j_2 < \dots < j_k$ les entiers tels que :

$$\varphi_{i_1}(q) = \varphi_{i_2}(q) = \dots = \varphi_{i_k}(q) = \mu \quad \text{et} \quad \psi_{j_1}(\mu) = \psi_{j_2}(\mu) = \dots = \psi_{j_k}(\mu) = q,$$

alors on a bien $\psi_{j_s} \circ \varphi_{i_s}(q) = q$ mais, si $t < s$ le nombre $\psi_{j_t} \circ \varphi_{i_s}(q)$ doit être considéré comme infinitésimalement plus petit que q et, en tout cas, ne doit pas être pris en compte dans la définition de q_{i_s, j_t} .

Quoi qu'il en soit, on peut montrer en reprenant les arguments développés précédemment que la proposition 1.6 est encore vraie pour tous les $\varphi \in \Phi$ à condition de prendre la définition modifiée précédente. De même, la formule (1.4) demeure, ainsi que les relations (1.5), (1.6) et (1.12).

1.2.4 Une bijection

À partir de maintenant, nous allons faire varier les éléments φ dans Φ . C'est pourquoi, afin de lever tout risque d'ambiguïté, nous noterons dans la suite $q_{i,j}(\varphi)$ et $\mu_{i,j}(\varphi)$ respectivement à la place de $q_{i,j}$ et $\mu_{i,j}$.

Notons I l'ensemble des couples (i, j) tels que $1 \leq i \leq j \leq d$ et considérons l'espace vectoriel $(\mathbb{R}^2)^I$ des suites $(q_{i,j}, \mu_{i,j})$ indicées par les éléments de I . Soit K le sous-ensemble convexe de $(\mathbb{R}^2)^I$ définis par les relations (1.5), (1.6) et (1.12).

Théorème 1.9. *L'application*

$$\Phi \rightarrow K, \quad \varphi \mapsto (q_{i,j}(\varphi), \mu_{i,j}(\varphi))_{(i,j) \in I}$$

est une bijection et son inverse est donné par la formule (1.4).

Démonstration. Il s'agit de démontrer qu'étant donné $(q_{i,j}, \mu_{i,j}) \in K$, la formule (1.4) définit un d -uplet $\varphi = (\varphi_1, \dots, \varphi_d)$ qui appartient à Φ et tel que pour tout $(i, j) \in I$, on a $q_{i,j}(\varphi) = q_{i,j}$ et $\mu_{i,j}(\varphi) = \mu_{i,j}$. Les conditions 2 et 3 qui définissent l'ensemble Φ (voir page 11) ne posent aucun problème à part peut-être en ce qui concerne la croissance des φ_i , mais celle-ci résulte directement des égalités et des inégalités supposées sur les $q_{i,j}$ et $\mu_{i,j}$. Notons en outre que l'on a :

$$\forall q < q_{i,j}, \quad \varphi_i(q) \leq b(q - q_{i,j}) + \mu_{i+1,j+1} \quad (1.14)$$

$$\forall q \geq q_{i,j}, \quad \varphi_i(q) \geq b(q - q_{i,j}) + \mu_{i,j} \quad (1.15)$$

Montrons à présent la condition 1, c'est-à-dire que pour tout indice $i \in \{1, \dots, d-1\}$, on a $\varphi_i \geq \varphi_{i+1}$. Soit $q \in \mathbb{R}$. Si $q < q_{i+1,d}$, on a bien $\varphi_i(q) \geq \varphi_{i+1}(q) = -\infty$. Sinon, il existe j tel que $q_{i+1,j} \leq q < q_{i+1,j-1}$. On a alors $\varphi_{i+1}(q) = b(q - q_{i+1,j}) + \mu_{i+1,j} \leq b(q - q_{i,j-1}) + \mu_{i,j-1} \leq \varphi_i(q)$ la première inégalité résultant des hypothèses $q_{i+1,j} \geq q_{i,j-1}$ et $\mu_{i+1,j} \leq \mu_{i,j-1}$, et la seconde résultant de (1.15) après avoir remarqué que $q \geq q_{i+1,j} \geq q_{i,j-1}$.

Vérifions maintenant la condition 4. Bien sûr, on prend les fonctions ψ_j définies par la formule (1.4). Les inégalités supposées impliquent de même que précédemment qu'elles sont strictement croissantes et rangées par ordre croissant. Soit (q, μ) un couple de nombres réels. Par définition, un indice $i \in \{1, \dots, d\}$ vérifie $\mu = \varphi_i(q)$ si, et seulement si il existe $j \in \{1, \dots, d\}$ tel que

$$q_{i,j} \leq q < q_{i,j-1} \quad \text{et} \quad \mu - \mu_{i,j} = b(q - q_{i,j}) \quad (1.16)$$

De plus, si un tel indice j existe, il est clair qu'il est unique. Ainsi, il existe autant d'indices i satisfaisant $\mu = \varphi_i(q)$ que de couples (i, j) satisfaisant (1.16). De même, on démontre qu'il existe autant d'indices j satisfaisant $q = \psi_j(\mu)$ que de couples (i, j) satisfaisant :

$$\mu_{i,j} \leq \mu < \mu_{i+1,j} \quad \text{et} \quad \mu - \mu_{i,j} = b(q - q_{i,j}). \quad (1.17)$$

Il suffit donc de montrer que les conditions (1.16) et (1.17) sont équivalentes, ce qui résulte sans peine de l'égalité (1.6).

Montrons à présent que $q_{i,j}(\varphi) = q_{i,j}$ et $\mu_{i,j}(\varphi) = \mu_{i,j}$. La relation (1.7) nous dit qu'il suffit de démontrer l'égalité pour les $q_{i,j}$. Comme précédemment, nous nous restreignons au cas où $\varphi_1 > \dots > \varphi_d$ pour écrire la preuve. Il faut alors montrer que pour tout $(i, j) \in I$, on a $\psi_j \circ \varphi_i(q_{i,j}) \geq q_{i,j}$ et $\psi_j \circ \varphi_i(q) < q$ pour tout $q < q_{i,j}$. La formule (1.14) montre que $\varphi_i(q_{i,j}) \geq \mu_{i,j}$, tandis que, de manière analogue, on démontre $\psi_j(\mu_{i,j}) \geq q_{i,j}$. Il en résulte, en utilisant la croissance, que $\psi_j \circ \varphi_i(q_{i,j}) \geq \psi_j(\mu_{i,j}) \geq q_{i,j}$. Soit $q < q_{i,j}$. Si $\varphi_i(q) = -\infty$, il n'y a rien à démontrer; on suppose donc que ce n'est pas le cas. À partir de (1.14) et d'une formule analogue donnant une majoration de ψ_j sur l'intervalle $] -\infty, \mu_{i,j}[$, on obtient

$$\psi_j \circ \varphi_i(q) \leq q - (q_{i,j} - q_{i-1,j-1}) - \frac{\mu_{i,j} - \mu_{i+1,j+1}}{b}.$$

Ainsi, le résultat est acquis dès lors que $q_{i,j} - q_{i-1,j-1} > 0$ ou $\mu_{i,j} - \mu_{i+1,j+1} > 0$ puisque, par hypothèse, les deux différences sont positives ou nulles, ce qui nous permet de supposer que ce n'est pas le cas. Mais alors en appliquant (1.14) au couple $(i-1, j-1)$, on trouve $\varphi_{i-1}(q) \leq b(q - q_{i-1,j-1}) + \mu_{i,j} = b(q - q_{i,j}) + \mu_{i,j}$ puis, avec (1.15), $\varphi_{i-1}(q) \leq \varphi_i(q)$, ce qui contredit notre hypothèse. \square

Rappelons que l'on avait défini un sous-ensemble $\Phi_{\mathbb{Z}}$ de Φ caractérisé par certaines conditions dites d'intégrité (les conditions 5 et 6, page 11). La proposition suivante montre que ce sous-ensemble est facilement caractérisable à l'aide de la bijection du théorème précédent.

Proposition 1.10. *Pour tout $\varphi \in \Phi$, les trois conditions suivantes sont équivalentes :*

- i) $\varphi \in \Phi_{\mathbb{Z}}$
- ii) pour tout $(i, j) \in I$, $q_{i,j}(\varphi) \in \frac{1}{b}\mathbb{Z}$, et pour tout $i \in \{1, \dots, d\}$, $q_{i,d}(\varphi) \in \mathbb{Z}$;
- iii) pour tout $(i, j) \in I$, $\mu_{i,j}(\varphi) \in \mathbb{Z}$ et pour tout $i \in \{1, \dots, d\}$, la somme $\mu_{i,i}(\varphi) + \mu_{i,i+1}(\varphi) + \dots + \mu_{i,d}(\varphi)$ est divisible par $b - 1$.

Démonstration. L'équivalence entre les conditions ii) et iii) résulte directement des formules (1.7) et (1.8) qui permettent d'exprimer les $\mu_{i,j}$ en fonction des $q_{i,j}$ et réciproquement. Reste donc à montrer l'équivalence entre i) et ii). À partir de la proposition 1.6, on déduit que ii) implique i). Si l'on suppose maintenant que $\varphi \in \Phi_{\mathbb{Z}}$, alors toutes les composées $\psi_j \circ \varphi_i$ sont constantes sur les intervalles de la forme $[v, v + \frac{1}{b}[$ pour $v \in \frac{1}{b}\mathbb{Z}$ et de là, en revenant à la définition, on déduit que les $q_{i,j}(\varphi)$ appartiennent tous à $\frac{1}{b}\mathbb{Z}$. Finalement, il est clair que $q_{i,d}(\varphi)$ est entier pour tout i , puisque celui-ci est égal à q_i qui est justement supposé entier. \square

1.3 Les variétés \mathcal{X}_{φ} et leurs dimensions

Étant donné un d -uplet $\tilde{\varphi} = (\tilde{\varphi}_1, \dots, \tilde{\varphi}_d)$ définissons $\tilde{\mathcal{X}}_{\tilde{\varphi}}(k)$ comme l'ensemble des réseaux $L \subset M$ tels que $\tilde{\varphi}_i(L) = \tilde{\varphi}_i$ pour tout i . Si l'on note φ le d -uplet de fonctions $\varphi_i : \mathbb{R} \rightarrow \mathbb{R} \cup \{-\infty\}$ obtenu à partir de $\tilde{\varphi}$ après réordonnement et prolongement, les propositions 1.2 et 1.6 montrent ensemble que $\tilde{\mathcal{X}}_{\tilde{\varphi}}(k)$ est inclus dans $\mathcal{X}_{\mu}(k)$ pour $\mu = (\mu_{1,1}(\varphi), \mu_{1,2}(\varphi), \dots, \mu_{1,d}(\varphi))$. De façon plus précise, on démontre comme dans le lemme 4.2 de [15] que l'on obtient ce faisant une sous-variété $\tilde{\mathcal{X}}_{\tilde{\varphi}}$ de \mathcal{X}_{μ} qui est localement fermée.

De façon similaire à ce que l'on vient de faire, étant donné $\varphi \in \Phi_{\mathbb{Z}}$, on note $\mathcal{X}_{\varphi}(k)$ l'ensemble des réseaux $L \subset M$ tels que $\varphi(L) = \varphi$; il s'écrit manifestement comme une union de $\tilde{\mathcal{X}}_{\tilde{\varphi}}(k)$. Le lemme suivant montre qu'il s'agit même d'une union finie et, par voie de conséquence, que $\mathcal{X}_{\varphi}(k)$ est aussi l'ensemble des k -points d'une sous-variété algébrique localement fermée de \mathcal{X}_{μ} pour le même μ que précédemment.

Lemme 1.11. *Fixons un élément $\varphi \in \Phi_{\mathbb{Z}}$. Alors, il n'existe qu'un nombre fini de d -uplets de fonctions $(\tilde{\varphi}_1, \dots, \tilde{\varphi}_d)$ qui satisfont les conditions de la proposition 1.2 et qui redonnent le d -uplet φ après réordonnement.*

Démonstration. Si $(\tilde{\varphi}_1, \dots, \tilde{\varphi}_d)$ est un tel d -uplet, alors il existe une permutation $w \in \mathfrak{S}_d$ telle que, pour tout i , on ait $\tilde{\varphi}_i(v) = -\infty$ pour $v < q_{w(i),d}(\varphi)$ et $\tilde{\varphi}_i(v) = bv - q_{w(i),d}(\varphi)$ pour v suffisamment grand. Du fait que les fonctions $\tilde{\varphi}_i$ doivent en outre être croissantes, on déduit que l'égalité $\tilde{\varphi}_i(v) = bv - q_{w(i),d}(\varphi)$ vaut pour tout $v \geq q_{d,d}(\varphi)$. Après cela, il ne reste plus qu'un nombre fini de v et donc qu'un nombre fini de possibilités pour attribuer les valeurs manquantes aux $\tilde{\varphi}_i$ puisque pour chaque v , on ne peut que permuter les nombres $\varphi_i(v)$ et on a donc au maximum $d!$ possibilités. \square

1.3.1 La fonction dimension sur Φ

Définition 1.12. Notons Leb la mesure de Lebesgue sur \mathbb{R} . Si $\varphi = (\varphi_1, \dots, \varphi_d) \in \Phi$, on pose :

$$\dim(\varphi) = \sum_{1 \leq i < i' \leq d} \text{Leb}(\varphi_i(\mathbb{R}) \setminus \varphi_{i'}(\mathbb{R}))$$

où, si E et E' sont des ensembles, on note $E \setminus E'$ l'ensemble des éléments qui appartiennent à E mais pas à E' .

Remarque 1.13. Pour $\varphi = (\varphi_1, \dots, \varphi_d) \in \Phi$, il est clair qu'il existe des constantes A et B telles que $[A, +\infty[\subset \varphi_i(\mathbb{R}) \subset [B, +\infty[$ pour tout i . On en déduit que les différences $\varphi_i(\mathbb{R}) \setminus \varphi_{i'}(\mathbb{R})$ sont toutes incluses dans l'intervalle $[A, B]$ et donc, en particulier, qu'elles ont une mesure finie. Ainsi $\dim(\varphi)$ est toujours fini.

Via la bijection de la proposition 1.2, un élément $\varphi \in \Phi$ est entièrement déterminé par la donnée des $q_{i,j}(\varphi)$ et $\mu_{i,j}(\varphi)$. Ainsi, le nombre $\dim(\varphi)$ que l'on vient de définir doit s'exprimer en fonction des $q_{i,j}(\varphi)$ et $\mu_{i,j}(\varphi)$. On a plusieurs possibilités pour cela, comme le montre le lemme suivant.

Lemme 1.14. Pour tout $\varphi \in \Phi$, on a :

$$\begin{aligned} \dim(\varphi) &= \sum_{j=1}^d (d+1-j) \cdot \mu_{1,j}(\varphi) - \sum_{(i,j) \in I} \mu_{i,j}(\varphi) \\ &= b \cdot \sum_{(i,j) \in I} q_{i,j}(\varphi) - \sum_{i=1}^d (2i-1-d-bi) \cdot q_{i,d}(\varphi). \end{aligned}$$

Remarque 1.15. On constate en particulier — et ce sera crucial dans la suite — que $\dim(\varphi)$ dépend de façon linéaire des $\mu_{i,j}(\varphi)$ et $q_{i,j}(\varphi)$.

Démonstration. Comme d'habitude, nous ne donnons la démonstration que dans le cas où $\varphi_1 > \dots > \varphi_d$. Fixons un indice $i \in \{1, \dots, d\}$. D'après la proposition 1.6, l'image de la fonction φ_i s'écrit :

$$\varphi_i(\mathbb{R}) = \bigsqcup_{i \leq j \leq d} [\mu_{i,j}, \mu_{i+1,j}[.$$

Comme on a en outre $\mu_{i+1,j+1} \leq \mu_{i,j}$, les intervalles qui apparaissent dans l'union précédente sont « rangés par ordre décroissant ». On en déduit que le réel μ n'est pas dans l'image de φ_i si, et seulement si, il existe $j \in \{i, \dots, d\}$ tel que $\mu_{i+1,j+1} \leq \mu < \mu_{i,j}$ où on a posé par convention $\mu_{i+1,d+1} = -\infty$. Comptons à présent le nombre d'indices $i' > i$ tels que μ appartienne à l'image de $\varphi_{i'}$ pour un indice $i' > i$. Comme les fonctions $\varphi_{i'}$ sont injectives sur l'intervalle où elles prennent des valeurs finies et que l'on a supposé $\varphi_1 > \dots > \varphi_d$, cela revient encore à compter le nombre de q pour lesquels il existe $i' > i$ tel que $\mu = \varphi_{i'}(q)$. Cette condition se réécrit encore :

$$\exists i' \in \{1, \dots, d\}, \quad \mu = \varphi_{i'}(q) \text{ et } \varphi_{i+1}(q) \geq \mu$$

puis, d'après la définition des ψ_j :

$$\exists j' \in \{1, \dots, d\}, \quad q = \psi_{j'}(\mu) \text{ et } \varphi_{i+1}(q) \geq \mu.$$

En remplaçant q par $\psi_{j'}(\mu)$, la dernière inégalité devient $\varphi_{i+1} \circ \psi_{j'}(\mu) \geq \mu$, ce qui équivaut encore à $\mu \geq \mu_{i+1,j'}$. Au final, on cherche donc à dénombrer les réels q s'écrivant sous la forme $\psi_{j'}(\mu)$ pour un indice j' tel que $\mu \geq \mu_{i+1,j'}$. De notre hypothèse supplémentaire $\varphi_1 > \dots > \varphi_d$, on déduit facilement que $\psi_1 < \dots < \psi_d$, d'où il suit que le nombre cherché est aussi le nombre d'indices j' tels que $\mu \geq \mu_{i+1,j'}$. Or, rappelons que μ a été pris dans l'intervalle $[\mu_{i+1,j+1}, \mu_{i,j}[$ et donc *a fortiori* dans $[\mu_{i+1,j+1}, \mu_{i+1,j}[$. À partir de la décroissance de la suite $j' \mapsto \mu_{i+1,j'}$, on déduit tout de suite que les j' convenables sont ceux de l'ensemble $\{j+1, \dots, d\}$. En particulier, il y en a $d-j$.

Récapitulons : nous avons montré que le complémentaire de l'image des φ_i est la réunion disjointe des intervalles $[\mu_{i+1,j+1}, \mu_{i,j}[$ pour j variant dans $\{i, \dots, d\}$, et que si $\mu \in [\mu_{i+1,j+1}, \mu_{i,j}[$ pour un certain j , il y a exactement $d-j$ indices $i' > i$ tels que $\mu \in \varphi_{i'}(\mathbb{R})$. Il en résulte que

$$\sum_{i'=i+1}^d \text{Leb}(\varphi_i(\mathbb{R}) \setminus \varphi_{i'}(\mathbb{R})) = \sum_{j=i}^{d-1} (d-j) \cdot (\mu_{i,j} - \mu_{i+1,j+1}).$$

En sommant ces égalités pour tout i , il vient :

$$\dim(\varphi) = \sum_{1 \leq i \leq j < d} (d-j) \cdot (\mu_{i,j} - \mu_{i+1,j+1}).$$

Les formules annoncées dans la proposition s'en déduisent (avec un peu de calcul) à partir de la relation (1.7). \square

Corollaire 1.16. Pour tout $\varphi \in \Phi_{\mathbb{Z}}$, on a la congruence :

$$\dim(\varphi) \equiv - \sum_{j=1}^d j \cdot \mu_{1,j}(\varphi) \pmod{b-1}.$$

Démonstration. C'est une conséquence immédiate de la première égalité de la proposition précédente et de la proposition 1.10. \square

Le corollaire est intéressant car nous avons vu que dans le cas où φ provient d'un réseau L , les nombres $\mu_{1,j}(\varphi)$ s'interprètent comme les exposants des diviseurs élémentaires du module engendré par $\phi(L)$ par rapport à L . Par ailleurs, comme on peut s'y attendre, la fonction \dim que nous avons défini est liée de près à la dimension des variétés \mathcal{X}_φ . Plus précisément, nous allons démontrer le théorème suivant.

Théorème 1.17. Soit $\varphi = (\varphi_1, \dots, \varphi_d) \in \Phi_{\mathbb{Z}}$. Alors

- si $\sigma \neq \text{id}$, on a $\dim_k \mathcal{X}_\varphi = \dim(\varphi)$;
- si $\sigma = \text{id}$, on a $\dim(\varphi) \leq \dim_k \mathcal{X}_\varphi \leq \dim(\varphi) + \frac{d(d-1)}{2}$.

1.3.2 Démonstration du théorème 1.17

Fixons un élément $\varphi \in \Phi_{\mathbb{Z}}$. Puisque \mathcal{X}_φ s'écrit comme l'union finie des $\tilde{\mathcal{X}}_{\tilde{\varphi}}$ sur les d -uplets $\tilde{\varphi} = (\tilde{\varphi}_1, \dots, \tilde{\varphi}_d)$ vérifiant les conditions de la proposition 1.2 et redonnant φ après réordonnement, il suffit de démontrer

- d'une part, que la dimension de toutes les variétés $\tilde{\mathcal{X}}_{\tilde{\varphi}}$ est majorée par $\dim(\varphi)$ dans le cas où $\sigma \neq \text{id}$ et par $\dim(\varphi) + \frac{d(d-1)}{2}$ dans le cas contraire, et
- d'autre part, qu'il existe un d -uplet $\tilde{\varphi}$ particulier pour lequel $\dim_k \mathcal{X}_{\tilde{\varphi}} \geq \dim(\varphi)$.

Pour cela nous allons suivre, encore une fois, la méthode de [15].

Notion de famille correcte Fixons un d -uplet $\tilde{\varphi} = (\tilde{\varphi}_1, \dots, \tilde{\varphi}_d)$ comme précédemment et notons :

$$V = \left\{ (q, i) \in \frac{1}{b}\mathbb{Z} \times \mathbb{Z} \mid \varphi_i(q) \neq -\infty \right\}.$$

Posons aussi :

$$A = \left\{ (q, i, q', i') \in \frac{1}{b}\mathbb{Z} \times \mathbb{Z} \times \frac{1}{b}\mathbb{Z} \times \mathbb{Z} \mid (q', i') > (q, i) \text{ et } \varphi_i(q - \frac{1}{b}) < \varphi_{i'}(q') < \varphi_i(q) \right\}$$

et, pour tout $(q, i) \in V$:

$$A(q, i) = \left\{ (q', i') \in \frac{1}{b}\mathbb{Z} \times \mathbb{Z} \mid (q', i') > (q, i) \text{ et } \varphi_i(q - \frac{1}{b}) < \varphi_{i'}(q') < \varphi_i(q) \right\}.$$

On montre facilement que le cardinal de A est toujours majoré par $\dim(\varphi)$. Soient enfin \tilde{q}_i le nombre associé aux fonctions $\tilde{\varphi}_i$ et (e_1, \dots, e_d) la base canonique de M .

La première étape de la preuve consiste à démontrer qu'étant donné un réseau L de M tel que $\tilde{\varphi}_i(L) = \tilde{\varphi}_i$ pour tout i . Alors, il existe des éléments $v_{q,i} \in M_{k((u^{1/b}))}$ pour $(q, i) \in V$ et des éléments $a_{q,i,q',i'} \in k$ pour $(q, i, q', i') \in A$ qui vérifient :

- i) pour tout $(q, i) \in V$, on a $\text{val}(v_{q,i}) = (q, i)$ et $\text{val}(v_{q,i} - u^q e_i) > (q, i)$;
- ii) pour tout $(q, i) \in V$, on a $v_{q,i} \in k[[u^{1/b}]] \otimes_{k[[u]]} L$ et $w_{q,i} = u^{-\tilde{\varphi}_i(q)} \phi(v_{q,i}) \in L$;
- iii) pour tout $(q, i) \in V$ tel que $(q - \frac{1}{b}, i) \in V$, on a

$$v_{q,i} = u^{1/b} v_{q-\frac{1}{b},i} + \sum_{(q',i') \in A(q,i)} a_{q,i,q',i'} \cdot v_{q',i'} \quad (1.18)$$

- iv) pour tout $(q, i) \in V$ tel que $\tilde{\varphi}_i(q) = bq - \tilde{q}_i$ (ou de façon équivalente pour un tel (q, i)), on a

$$v_{\tilde{q}_i,i} = w_{q,i} + \sum_{(q',i') \in A(q,i)} a_{q,i,q',i'} \cdot v_{q',i'} - \sum_{\substack{(q',i') \in A(q,i) \\ q'=q}} \sigma(a_{q,i,q,i'}) \cdot u^{\tilde{q}_i} e_{i'} \quad (1.19)$$

où $w_{q,i} = u^{-\tilde{\varphi}_i(q)} \phi(v_{q,i})$ comme ci-dessus.

Nous dirons qu'une famille $(v_{q,i}, a_{q,i,q',i'})$ est *correcte* pour L si elle vérifie les conditions précédentes et, étant donné un entier n , qu'elle est *n-correcte* pour L si elle vérifie i), ii) et si les égalités iii) et iv) sont vraies respectivement modulo $u^{q+\frac{n}{b}}$ et $u^{\tilde{q}_i+\frac{n}{b}}$. Notre but est de construire une famille correcte, et pour cela nous allons procéder par approximations successives. Pour amorcer la construction, on se donne des

éléments $v_{q,i}$ vérifiant simplement les conditions i) et ii) (leur existence résulte de la définition des fonctions $\tilde{\varphi}_i(L)$) et on prend $a_{q,i,q',i'} = 0$ pour tout $(q, i, q', i') \in A$. La famille $(v_{q,i}, a_{q,i,q',i'})$ est alors 0-correcte. L'étape d'itération est donnée par le lemme suivant duquel il résulte directement l'existence souhaitée après un passage à la limite.

Lemme 1.18. *Soit $(v_{q,i}, a_{q,i,q',i'})$ une famille n -correcte pour L pour un certain entier $n \geq 0$. Posons $m = n + 1$. Alors, il existe $(v'_{q,i}, a'_{q,i,q',i'})$ une famille m -correcte pour L telle que*

- on ait $v'_{q,i} \equiv v_{q,i} \pmod{u^{q+\frac{n}{b}}}$ pour tout $(q, i) \in V$;
- si n est suffisamment grand, on ait aussi $a'_{q,i_0,q',i'} = a_{q,i_0,q',i'}$ pour tout $(q, i_0, q', i') \in A$.

Démonstration. On construit les $v'_{q,i}$ par récurrence sur q et à q fixé par récurrence descendante sur i . Autrement dit, on considère $(q, i) \in V$, on suppose que tous les $v'_{q',i'} \in V$ avec $q' < q$ ou $q' = q$ et $i' > i$ sont construits et on cherche à construire $v'_{q,i}$. Supposons d'abord que $(q - \frac{1}{b}, i)$ appartienne à V . On regarde dans ce cas l'équation (1.18) modulo $u^{q+\frac{m}{b}}$, i.e. la congruence

$$v'_{q,i} \equiv u^{1/b} v'_{q-\frac{1}{b},i} + \sum_{(q',i') \in A(q,i)} a'_{q,i,q',i'} \cdot v'_{q',i'} \pmod{u^{q+\frac{m}{b}}} \quad (1.20)$$

qui doit être satisfaite par l'élément $v'_{q,i}$ que l'on veut construire. Dans l'expression précédente, les $v'_{q-\frac{1}{b},i}$ ont déjà été construits de même que les $v'_{q',i'}$ pour $q = q'$ car on a alors nécessairement $i' > i$. Si $q' > q$, en revanche, on n'a pas encore construit $v'_{q',i'}$ mais on souhaite le faire de façon à ce que $v'_{q',i'} \equiv v_{q',i'} \pmod{u^{q'+\frac{n}{b}}}$ et donc *a fortiori* $v'_{q',i'} \equiv v_{q',i'} \pmod{u^{q+\frac{m}{b}}}$. On cherche donc à ce que $v'_{q',i'}$ satisfasse la congruence (1.20) où on a remplacé $v'_{q',i'}$ pour $q' > q$ par $v_{q',i'}$. Nous allons en fait trouver $v'_{q',i'}$ de sorte que cette nouvelle congruence soit une égalité, c'est-à-dire de sorte que :

$$v'_{q,i} = u^{1/b} v'_{q-\frac{1}{b},i} + \sum_{\substack{(q',i') \in A(q,i) \\ q'=q}} a'_{q,i,q',i'} \cdot v'_{q',i'} + \sum_{\substack{(q',i') \in A(q,i) \\ q'>q}} a'_{q,i,q',i'} \cdot v_{q',i'}. \quad (1.21)$$

Notons qu'en plus de cela, nous devons avoir $\phi(v'_{q,i}) \in u^{\tilde{\varphi}_i(q)} L$. En reportant la valeur désirée de $v'_{q,i}$ donnée par l'égalité précédente, on souhaite maintenant démontrer qu'il existe $a'_{q,i,q',i'} \in k$ tels que

$$u \cdot \phi(v'_{q-\frac{1}{b},i}) + \sum_{\substack{(q',i') \in A(q,i) \\ q'=q}} \sigma(a'_{q,i,q',i'}) \cdot \phi(v'_{q',i'}) + \sum_{\substack{(q',i') \in A(q,i) \\ q'>q}} \sigma(a'_{q,i,q',i'}) \cdot \phi(v_{q',i'}) \in u^{\tilde{\varphi}_i(q)} L. \quad (1.22)$$

Or, par définition de l'ensemble $A(q, i)$, il ne fait aucun doute que c'est le cas et même que les $a'_{q,i,q',i'}$ sont uniquement déterminés. Nous choisissons donc ces $a'_{q,i,q',i'}$ -ci et l'élément $v'_{q,i}$ donné par l'expression (1.21).

Si maintenant, au contraire, $(q - \frac{1}{b}, i) \notin V$, on raisonne de manière similaire sauf que l'on part désormais de l'équation (1.19) et comme précédemment on remplace $w'_{q,i} = u^{-\tilde{\varphi}_i(q)} \phi(v'_{q,i})$ par $w_{q,i} = u^{-\tilde{\varphi}_i(q)} \phi(v_{q,i})$. Après cela, il n'est plus difficile de vérifier que $v'_{q,i} \equiv v_{q,i} \pmod{u^{q+\frac{n}{b}}}$ pour tout $(q, i) \in V$ et que la famille $(v'_{q,i}, a'_{q,i,q',i'})$ que nous avons construite est bien m -correcte. Il reste à montrer que si n est suffisamment grand, on a $a_{q,i,q',i'} = a'_{q,i,q',i'}$ pour tout quadruplet $(q, i, q', i') \in A$. Mais cela résulte directement du fait que, en vertu des congruences $v'_{q,i} \equiv v_{q,i} \pmod{u^{q+\frac{n}{b}}}$ pour tout $(q, i) \in V$, l'assertion (1.22), de même que son analogue dans le cas où $(q - \frac{1}{b}, i) \notin V$, est vraie avec $a'_{q,i,q',i'} = a_{q,i,q',i'}$ si n est suffisamment grand. \square

Remarque 1.19. Comme nous l'avons déjà dit, il résulte du lemme l'existence d'une famille correcte pour L , mais la démonstration que nous en avons faite prouve également que les éléments $a_{q,i,q',i'}$ dans une famille correcte pour L sont entièrement déterminés par L .

Il est également possible à partir d'une famille correcte $(v_{q,i}, a_{q,i,q',i'})$ de retrouver le réseau L : en effet, à partir des conditions i) et ii), on démontre directement que L est le module engendré par les $v_{q,i}$ pour (q, i) parcourant V . Le lemme suivant montre qu'en fait L est déjà engendré par les d vecteurs $v_{\tilde{q}_i,i}$ (qui en forment donc une base).

Lemme 1.20. Soit $(v_{q,i}, a_{q,i,q',i'})$ une famille correcte pour L . Pour tout $(q, i) \in V$, il existe des $\lambda_s \in k[[u]]$ ($1 \leq s \leq d$) tels que :

$$v_{q,i} = \sum_{s=1}^d \lambda_s \cdot u^{q-\tilde{q}_s} v_{\tilde{q}_s,s}$$

et $\lambda_s = 0$ si $q < q_s$ ou si $q = q_s$ et $s < i$.

Démonstration. Si $(q - \frac{1}{b}, i) \notin V$, alors $q = \tilde{q}_i$ et le résultat est clair. Dans le cas contraire, la relation (1.18) nous dit que $v_{q,i}$ s'exprime en termes de $v_{q-\frac{1}{b},i}$ et des $v_{q',i'}$ pour $(q', i') \in A(q, i)$. Or, les nombres $\tilde{\varphi}_i(q - \frac{1}{b})$ et $\varphi_{i'}(q')$ sont tous strictement plus petit que $\varphi_i(q)$. Une récurrence sur le nombre $\tilde{\mu} = \tilde{\varphi}_i(q)$ permet donc de terminer la démonstration (on remarque que l'initialisation ne pose pas de problème car si $\tilde{\mu}$ est suffisamment petit, aucun couple (q, i) ne convient). \square

Remarque 1.21. De la démonstration précédente, il suit en outre que les λ_s s'expriment uniquement en fonction des $a_{q,i,q',i'}$ (et pas des $v_{q,i}$).

L'espace des familles correctes Nous souhaitons à présent montrer comment l'invariant « famille correcte » permet de paramétrer les réseaux L . À partir de maintenant, nous ne fixons donc plus un réseau L . Au contraire, nous considérons l'ensemble $\mathcal{C}(k)$ des familles $(v_{q,i}, a_{q,i,q',i'})$ satisfaisant les conditions i), iii) et iv) précédemment énoncées. Manifestement, $\mathcal{C}(k)$ est l'ensemble des k -points d'une variété algébrique définie sur k que nous noterons \mathcal{C} .

Lemme 1.22. On suppose que $(v_{q,i}, a_{q,i,q',i'})$ et $(v'_{q,i}, a_{q,i,q',i'})$ (avec les mêmes $a_{q,i,q',i'}$) vérifient les conditions i), iii) et iv), et que pour tout $i \in \{1, \dots, d\}$, on a $v_{\tilde{q}_i,i} \equiv v'_{\tilde{q}_i,i} \pmod{u^{\tilde{q}_i + \frac{1}{b}}}$. Alors $v_{q,i} = v'_{q,i}$ pour tout $(q, i) \in V$.

Démonstration. Posons, pour simplifier les écritures, $v_i = u^{-\tilde{q}_i} v_{\tilde{q}_i,i}$ et de même $v'_i = u^{-\tilde{q}_i} v'_{\tilde{q}_i,i}$. L'hypothèse s'écrit alors $v_i \equiv v'_i \pmod{u^{1/b}}$. En utilisant l'égalité (1.19), le lemme 1.20 ainsi que la remarque 1.21, on voit qu'il existe des matrices G et H à coefficients dans $k[[u]]$ de taille respectivement $d \times d$ et $1 \times d$ telles que

$$(\phi(v_1), \dots, \phi(v_d)) = (v_1, \dots, v_d)G + H \quad \text{et} \quad (\phi(v'_1), \dots, \phi(v'_d)) = (v'_1, \dots, v'_d)G + H.$$

De plus, on vérifie que la matrice G s'écrit $I_d + G'$ où G' est topologiquement nilpotente ; en particulier G est inversible. En posant $w_i = v_i - v'_i$, on a par hypothèse $w_i \equiv 0 \pmod{u^{1/b}}$ et, d'après ce qui précède, $(\phi(w_1), \dots, \phi(w_d)) = (w_1, \dots, w_d)G$. Comme G est inversible, cela implique que $w_i \equiv 0 \pmod{u}$. En répétant l'argument, on obtient $w_i \equiv 0 \pmod{u^{b^n}}$ pour tout n , c'est-à-dire $w_i = 0$. Finalement, $v_i = v'_i$ et une nouvelle application du lemme 1.20 permet de conclure. \square

Remarque 1.23. Le lemme précédent reste vrai si k est remplacé par une k -algèbre quelconque.

Notons $\mathcal{A} = \mathbb{A}_k^A$ l'espace affine standard sur k dont les coordonnées sont indicées par l'ensemble A ; c'est à l'évidence une variété algébrique de dimension $\text{Card } A$. On dispose par ailleurs d'un morphisme naturel $f : \mathcal{C} \rightarrow \mathcal{A}$ qui à une famille $(v_{q,i}, a_{q,i,q',i'})$ associe le vecteur de $a_{q,i,q',i'}$. Le lemme précédent et la remarque qui le suit montrent que les fibres de f sont de dimension inférieure ou égale à $\frac{d(d-1)}{2}$. En outre, lorsque $\sigma \neq \text{id}$, un examen de la preuve du lemme 1.22 montre même que f est étale. Ainsi, si l'on pose $\varepsilon = 1$ si $\sigma = \text{id}$ et $\varepsilon = 0$ dans le cas contraire, on obtient :

$$\dim_k \mathcal{C} \leq \dim_k \mathcal{A} + \varepsilon \cdot \frac{d(d-1)}{2} = \text{Card } A + \varepsilon \cdot \frac{d(d-1)}{2} \leq \dim(\varphi) + \varepsilon \cdot \frac{d(d-1)}{2}. \quad (1.23)$$

Par ailleurs, l'application qui à une famille $(v_{q,i}, a_{q,i,q',i'}) \in \mathcal{C}(k)$ associe le réseau engendré par les $v_{q,i}$ définit un morphisme algébrique g de \mathcal{C} dans la grassmannienne affine sur k . Le fait que tout réseau L appartenant à $\tilde{\mathcal{X}}_{\tilde{\varphi}}(k)$ admette une famille correcte signifie que l'image de g contient $\tilde{\mathcal{X}}_{\tilde{\varphi}}$. Ainsi trouve-t-on $\dim_k \tilde{\mathcal{X}}_{\tilde{\varphi}} \leq \dim_k \mathcal{C}$ et la majoration que l'on voulait suit alors de (1.23).

Démonstration de la minoration On se place ici dans le cas où $\tilde{\varphi}_1 \geq \tilde{\varphi}_2 \geq \dots \geq \tilde{\varphi}_d$ et on souhaite montrer qu'alors $\dim_k \tilde{\mathcal{X}}_{\tilde{\varphi}} \geq \dim(\varphi)$. Tout d'abord, on remarque que, dans ce cas, l'ensemble A que nous avons introduit précédemment est exactement de cardinal $\dim(\varphi)$.

Lemme 1.24. *Le morphisme $f : \mathcal{C} \rightarrow \mathcal{A}$ défini précédemment est un isomorphisme.*

Démonstration. Considérons R une k -algèbre. Il s'agit de montrer que pour tout $(a_{q,i,q',i'}) \in \mathcal{A}(R)$. Il existe une unique famille $(v_{q,i})_{(q,i) \in V}$ d'éléments de $M \otimes_{k((u))} R((u^{1/b}))$ telle que $(v_{q,i}, a_{q,i,q',i'}) \in \mathcal{C}(R)$.

On construit les $v_{q,i}$ et on démontre leur unicité par récurrence descendante sur i . En reprenant la démonstration du lemme 1.22, on voit que l'élément $v_i = u^{-\tilde{q}_i} v_{\tilde{q}_i, i}$ doit satisfaire une équation de la forme

$$\phi(v_i) = v_i + \sum_{s=i+1}^d \lambda_s v_s$$

où les λ_s sont de valuation u -adique strictement positive (les éventuels termes de valuation 0 s'annulent avec le terme $\sum_{(q',i') \in A(q,i), q'=q} \sigma(a_{q,i,q',i'}) \cdot u^{\tilde{q}_i} e_{i'}$ de la formule (1.19)). Comme les v_s pour $s > i$ sont déjà connus, on a à résoudre une équation de la forme $\phi(v_i) = v_i - c$ où c est un élément connu de valuation strictement positive de $R[[u^{1/b}]]$. Une telle équation a bien une unique solution, à savoir $v_i = \sum_{n=0}^{\infty} \phi^n(c)$. Les $v_{q,i}$ pour $q > q_i$ s'obtiennent alors à partir d'une variante du lemme 1.20. \square

À présent, il est aisé de conclure. La remarque 1.19 montre que le morphisme $g : g^{-1}(\tilde{\mathcal{X}}_{\tilde{\varphi}}) \rightarrow \tilde{\mathcal{X}}_{\tilde{\varphi}}$ est également un isomorphisme. Il suffit donc de démontrer que $g^{-1}(\tilde{\mathcal{X}}_{\tilde{\varphi}})$ est un ouvert non vide de \mathcal{C} , ce qui se fait comme dans la preuve du *Claim 3* de [15].

2 Mise en place de la méthode

Les théorèmes 1.9 et 1.17 permettent de reformuler le problème de calculer — ou disons, plutôt d'estimer — la dimension de $\mathcal{X}_{\leq e}$ en un problème d'optimisation linéaire. Dans cette section, nous mettons en place les outils nécessaires à la résolution de ce dernier problème puis, en guise d'exemple, nous illustrons la méthode proposée en démontrant le théorème 2 de l'introduction sous une hypothèse additionnelle. La démonstration complète de ce théorème est reportée à la section suivante, §3.3.3.

2.1 Préliminaires de programmation linéaire

On considère un espace euclidien E dont on note $\langle \cdot | \cdot \rangle_E$ le produit scalaire. On se donne :

- un cône convexe $Q \subset E$, c'est-à-dire un sous-ensemble non vide de E stable par addition et par multiplication par les nombres réels positifs ou nuls ;
- une application linéaire $f : E \rightarrow \mathbb{R}^n$ où n est un certain entier naturel ;
- une forme linéaire $\ell : E \rightarrow \mathbb{R}$.

Étant donné que E est un espace euclidien, il existe des vecteurs $\vec{\ell}, \vec{f}_1, \dots, \vec{f}_n$ tels que $\ell(x) = \langle x | \vec{\ell} \rangle_E$ et $f(x) = (\langle x | \vec{f}_1 \rangle_E, \dots, \langle x | \vec{f}_n \rangle_E)$ pour tout $x \in E$. Nous souhaitons étudier la fonction $a_{Q,f,\ell} : \mathbb{R}^n \rightarrow \mathbb{R} \cup \{\pm\infty\}$ définie par :

$$a_{Q,f,\ell}(y) = \sup_{\substack{x \in Q \\ f(x)=y}} \ell(x) = \sup_{\substack{x \in Q \\ \langle x | \vec{f}_i \rangle_E = y_i}} \langle x | \vec{\ell} \rangle_E \quad \text{où } y = (y_1, \dots, y_n)$$

en convenant, comme d'habitude, que la borne supérieure de l'ensemble vide est $-\infty$ et celle d'un ensemble non majorée est $+\infty$. Notons Q^* le cône dual de Q :

$$Q^* = \{ x \in E \mid \langle x | x' \rangle_E \geq 0, \quad \forall x' \in Q \}.$$

Remarquons que si Q est défini par les inégalités $\langle x | \vec{v}_i \rangle_E \geq 0$ ($1 \leq i \leq N$), alors Q^* est le cône convexe engendré par les vecteurs v_i , c'est-à-dire l'ensemble des vecteurs de la forme $\lambda_1 \vec{v}_1 + \dots + \lambda_N \vec{v}_N$ pour des scalaires $\lambda_i \in \mathbb{R}^+$. Introduisons $A_{Q,f,\ell}$ l'ensemble convexe défini par :

$$A_{Q,f,\ell} = \{ y = (y_1, \dots, y_n) \in \mathbb{R}^n \mid (y_1 \vec{f}_1 + \dots + y_n \vec{f}_n) - \vec{\ell} \in Q^* \}. \quad (2.1)$$

Le théorème suivant établit un lien de dualité entre maximisation sur Q et minimisation sur $A_{Q,f,\ell}$.

Théorème 2.1. Avec les notations précédentes, on a :

$$a_{Q,f,\ell}(y) = \inf_{\alpha \in A_{Q,f,\ell}} \langle \alpha | y \rangle_n$$

où $\langle \cdot | \cdot \rangle_n$ désigne le produit scalaire usuel sur \mathbb{R}^n .

Démonstration. Il s'agit un résultat classique de dualité en programmation linéaire. Rappelons quand même brièvement comment on l'établit. On remarque tout d'abord que la fonction $a_{Q,f,\ell}$ est concave. Le théorème de Hahn Banach assure qu'elle s'écrit comme la borne inférieure des fonctions affines qui la majorent. Or un calcul immédiat montre que la fonction affine $\mathbb{R}^n \rightarrow \mathbb{R}$, $(y_1, \dots, y_n) \mapsto \alpha_1 y_1 + \dots + \alpha_n y_n + \beta$ ($\alpha_i, \beta \in \mathbb{R}$) majore $a_{f,K,\ell}$ si, et seulement si

$$\forall x \in Q, \quad \langle x | \vec{\ell} - (\alpha_1 \vec{f}_1 + \dots + \alpha_n \vec{f}_n) \rangle_E \leq \beta.$$

Comme Q est un cône convexe, ceci est encore équivalent à $\beta \geq 0$ et $(\alpha_1 \vec{f}_1 + \dots + \alpha_n \vec{f}_n) - \vec{\ell} \in Q^*$. Le théorème en résulte. \square

Pour ce que l'on veut faire, on aura besoin de travailler dans une situation légèrement plus générale que celle que nous venons d'étudier. Précisément, en plus de Q , f et ℓ , on se donne maintenant deux cônes convexes C et D inclus dans \mathbb{R}^n , et on considère la fonction $b_{Q,f,\ell,C,D} : \mathbb{R}^n \rightarrow \mathbb{R} \cup \{\pm\infty\}$ définie par :

$$\begin{aligned} b_{Q,f,\ell,C,D}(y) &= \sup_{x \in Q, f(x) \in y-C} \ell(x) && \text{si } y \in D \\ &= -\infty && \text{sinon} \end{aligned}$$

où par définition $y-C$ est l'ensemble des vecteurs y' $\in \mathbb{R}^n$ pour lesquels il existe $c \in C$ tel que $y - c = y'$, ou autrement dit $y - y' \in C$. Dans la suite, lorsque $D = \mathbb{R}^n$, on s'autorisera à ne pas le noter en indice. Comme pour Q , on note C^* et D^* les cônes duaux respectifs de C et D . On pose :

$$B_{Q,f,\ell,C,D} = (A_{Q,f,\ell} \cap C^*) + D^*$$

où la notation précédente signifie que les éléments de $B_{Q,f,\ell,C,D}$ sont ceux qui s'écrivent sous la forme $y_1 + y_2$ avec $y_1 \in A_{Q,f,\ell} \cap C^*$ et $y_2 \in D^*$.

Proposition 2.2. Avec les notations précédentes, on a :

$$b_{Q,f,\ell,C,D}(y) = \inf_{\alpha \in B_{Q,f,\ell,C,D}} \langle \alpha | y \rangle_n.$$

Démonstration. On commence par traiter le cas où $D = \mathbb{R}^n$. Alors $D^* = \{0\}$ et $B_{Q,f,\ell,C,D} = A_{Q,f,\ell} \cap C^*$. La démonstration suit les mêmes idées que celle du théorème 2.1. On commence par montrer que la fonction $b_{Q,f,\ell,C,D}$ est concave. Par le théorème de Hahn Banach, elle s'écrit donc comme la borne inférieure des fonctions affines qui la majorent. Or, la fonction affine $\mathbb{R}^n \rightarrow \mathbb{R}$, $(y_1, \dots, y_n) \mapsto \alpha_1 y_1 + \dots + \alpha_n y_n + \beta$ ($\alpha_i, \beta \in \mathbb{R}$) majore $b_{Q,f,\ell,C,D}$ si, et seulement si

$$\forall x \in Q, \forall c \in C, \quad \langle x | \vec{\ell} - (\alpha_1 \vec{f}_1 + \dots + \alpha_n \vec{f}_n) \rangle_E \leq \beta + \langle \alpha | c \rangle_n. \quad (2.2)$$

Si $\alpha \in C^*$, le produit scalaire $\langle \alpha | c \rangle_n$ est par définition toujours positif ou nul. La valeur minimale qu'il prend lorsque c décrit C est donc 0. Ainsi, la condition précédente est équivalente à celle qui apparaissait dans la démonstration du théorème 2.1, soit encore à $\beta \geq 0$ et $\alpha \in A_{Q,f,\ell}$. Si, au contraire, $\alpha \notin C^*$, alors il existe un vecteur $c_0 \in C$ tel que $\langle \alpha | c_0 \rangle_n < 0$. Comme C est supposé stable par multiplication par les éléments de \mathbb{R}^+ , la quantité $\langle \alpha | c \rangle_n$ est non minorée lorsque c décrit C et la condition (2.2) n'est jamais satisfaite dans ce cas. La proposition, dans le cas particulier $D = \mathbb{R}^n$, résulte de ces considérations.

On revient maintenant au cas général. D'après ce que l'on vient de faire, il suffit d'établir que :

$$\begin{aligned} \inf_{\alpha \in B_{Q,f,\ell,C,D}} \langle \alpha | y \rangle_n &= \inf_{\alpha \in A_{Q,f,\ell} \cap C^*} \langle \alpha | y \rangle_n && \text{si } y \in D \\ &= -\infty && \text{sinon.} \end{aligned}$$

Supposons d'abord $y \in D$. Alors, si α est un élément de $B_{Q,f,\ell,C,D}$, il s'écrit $\alpha = \alpha_1 + \alpha_2$ avec $\alpha_1 \in A_{Q,f,\ell} \cap C^*$ et $\alpha_2 \in D^*$, d'où il suit $\langle \alpha | y \rangle_n = \langle \alpha_1 | y \rangle_n + \langle \alpha_2 | y \rangle_n \geq \langle \alpha_1 | y \rangle_n$. En passant à la borne

inférieure, on obtient l'inégalité $\inf_{\alpha \in B_{Q,f,\ell,C,D}} \langle \alpha | y \rangle_n \geq \inf_{\alpha \in A_{Q,f,\ell} \cap C^*} \langle \alpha | y \rangle_n$. Mais l'inégalité dans l'autre sens est évidente puisque $B_{Q,f,\ell,C,D}$ contient $A_{Q,f,\ell} \cap C^*$. Si maintenant $y \notin D$, le théorème d'Hahn Banach assure qu'il existe $z \in D^*$ tel que $\langle z | y \rangle_n < 0$. Les vecteurs λz , pour $\lambda \in \mathbb{R}^+$ appartiennent alors tous à $B_{Q,f,\ell,C,D}$, ce qui assure que la quantité $\langle \alpha | y \rangle_n$ est non minorée lorsque α parcourt cet ensemble. On a donc bien démontré ce que l'on voulait dans tous les cas. \square

Un cas important est celui où le cône convexe Q est défini comme l'intersection d'un nombre fini de demi-espaces, ce qui est la situation que l'on considèrera dans la suite. L'ensemble $B_{Q,f,\ell,C,D}$ est alors un polytope (éventuellement non borné) qui n'a, en tout cas, qu'un nombre fini de sommets. En outre, si on note $\alpha_1, \dots, \alpha_N$ ceux qui restent à distance finie, il découle de la proposition précédente que :

$$\begin{aligned} b_{Q,f,\ell,C,D}(y) &= \inf_{1 \leq i \leq N} \langle \alpha_i | y \rangle_n \quad \text{si } y \in D \cap (f(Q) + C) \\ &= -\infty \quad \text{sinon.} \end{aligned} \quad (2.3)$$

Ainsi, déterminer la fonction $b_{Q,f,\ell,C,D}$ revient à déterminer les α_i .

Un peu de réseaux pour pimenter

On conserve les notations introduites précédemment, et on se donne en outre R un réseau de E , c'est-à-dire un sous-groupe additif de E engendré par une base de E . On définit une nouvelle fonction $b'_{Q,R,f,\ell,C,D} : \mathbb{R}^n \rightarrow \mathbb{R}$ par

$$\begin{aligned} b'_{Q,R,f,\ell,C,D}(y) &= \sup_{x \in Q \cap R, f(x) \in y - C} \ell(x) \quad \text{si } y \in D \\ &= -\infty \quad \text{sinon.} \end{aligned}$$

De même que précédemment, lorsque $D = \mathbb{R}^n$, on l'omettra dans la notation. Il est évident que la fonction $b'_{Q,R,f,\ell,C,D}$ est majorée par $b_{Q,f,\ell,C,D}$ puisque la borne supérieure pour définir cette dernière fonction est prise sur un ensemble plus gros.

Proposition 2.3. *On suppose que Q engendre E en tant qu'espace vectoriel, que l'application f est surjective, et finalement que $R \cap f^{-1}(C)$ et $f^{-1}(C)$ engendrent le même espace vectoriel dans E .*

Alors, il existe un vecteur $y_0 \in \mathbb{R}^n$ et une constante $c \in \mathbb{R}$ tels que, pour tout $y \in f(R) + C$, on ait :

$$b_{Q,f,\ell,C}(y - y_0) - c \leq b'_{Q,R,f,\ell,C}(y) \leq b_{Q,f,\ell,C}(y)$$

où, bien sûr, on convient que $-\infty - c = -\infty$ et $+\infty - c = +\infty$.

Remarque 2.4. Le fait que Q engendre E n'est évidemment pas vraiment contraignant puisque, dans le cas où cela ne serait pas vérifié, il suffit de remplacer E par le sous-espace vectoriel $Q_{\mathbb{R}}$ engendré par Q et le réseau R par $R \cap Q_{\mathbb{R}}$. On attire toutefois l'attention du lecteur sur le fait qu'il se peut que $R \cap Q_{\mathbb{R}}$ ne soit pas un réseau de $Q_{\mathbb{R}}$; il s'agit donc d'une question qu'il ne faudra pas oublier de se poser le cas échéant. Toutefois, dans le cas où le réseau R et le cône Q sont tous les deux définis sur le corps des nombres rationnels, il est facile de vérifier que $R \cap Q_{\mathbb{R}}$ est toujours un réseau dans R ; il n'y a donc dans cette situation-ci pas de vérification supplémentaire à faire. De la même façon, la troisième hypothèse de la proposition (à savoir que $R \cap f^{-1}(C)$ et $f^{-1}(C)$ engendrent le même espace vectoriel dans E) est automatiquement satisfaite dès que R , C et f sont définis sur \mathbb{Q} . Dans les applications que nous avons en vue, nous considèrerons uniquement cette situation, et c'est pourquoi nous nous dispenserons de vérifier la troisième hypothèse, et nous nous autoriserons à appliquer la proposition même si Q n'engendre pas E .

Un mot enfin en rapport avec l'hypothèse de surjectivité de f . Bien entendu, elle n'est pas véritablement contraignante car on peut toujours appliquer la proposition en remplaçant \mathbb{R}^n par l'image de f . La conclusion du théorème n'est alors bien sûr plus valable que pour les y qui appartiennent à l'intersection de $f(R) + C$ avec l'image de f .

Démonstration. Définissons $C' = f^{-1}(C)$ et de façon générale, si X est un sous-ensemble de E ou de \mathbb{R}^n , nous noterons $X_{\mathbb{R}}$ le sous-espace vectoriel qu'il engendre. Soit $M \subset C'_{\mathbb{R}}$ une maille du réseau $C'_{\mathbb{R}} \cap R$. C'est un ensemble compact qui vérifie la propriété suivante : pour tout $x \in C'_{\mathbb{R}}$, il existe $m \in M$ tel que $x + m \in R$. Du fait que C' est d'intérieur non vide dans $C'_{\mathbb{R}}$ et qu'il est stable par multiplication par les réels positifs, on déduit qu'il existe un translaté de M entièrement inclus dans $(-C')$. Notons K un tel translaté. C'est encore un ensemble compact qui vérifie une propriété analogue à celle satisfaite par M . De même que

précédemment, étant donné que K est compact et que Q est un cône convexe d'intérieur non vide dans $Q_{\mathbb{R}}$, il existe $x_0 \in Q_{\mathbb{R}}$ tel que $x_0 + K \subset Q$. Posons $y_0 = f(x_0)$.

Si $y - y_0 \notin f(Q) + C$, on a $b_{Q,f,\ell,C}(y - y_0) = -\infty$ et la proposition est évidente dans ce cas. On suppose donc que $y - y_0 \in f(Q) + C$. Alors $b_{Q,f,\ell,C}(y - y_0)$ est fini, et pour tout $\varepsilon > 0$, il existe $x_1 \in Q$ tel que $f(x_1) \in (y - y_0) - C$ et $\ell(x_1) \geq b_{Q,f,\ell,C}(y - y_0) - \varepsilon$. On a alors $f(x_0 + x_1) \in y - C \subset f(R) + C_{\mathbb{R}}$, d'où on déduit, en utilisant la surjectivité de f , que $x_0 + x_1 \in R + C'_{\mathbb{R}}$ et, de là, qu'il existe $x_2 \in K$ tel que $x = x_0 + x_1 + x_2$ soit élément de R . Comme $x_1 \in Q$ et $x_0 + K \subset Q$, l'élément x appartient aussi à Q . Par ailleurs, $f(x) = y_0 + f(x_1) + f(x_2) \in y_0 + (y - y_0) - C + f(K) = y - C$ car $f(K)$ est inclus dans $(-C)$ par construction de K . Ainsi, trouve-t-on :

$$b'_{Q,R,f,\ell,C}(y) \geq \ell(x) \geq b_{Q,f,\ell,C}(y - y_0) - \varepsilon + \ell(x_0) + \inf_{x' \in K} \ell(x')$$

et la borne inférieure est finie étant donné que K est compact. \square

La minoration dans la proposition précédente fait intervenir la valeur de la fonction $b_{Q,f,\ell,C}$ en $y - y_0$, alors qu'il aurait été sans doute plus agréable d'avoir simplement $b_{Q,f,\ell,C}(y)$. En général, malheureusement, on ne peut pas remplacer $y - y_0$ par y , même en modifiant la constante c . Néanmoins dans le cas que nous avons déjà discuté précédemment où Q est défini comme l'intersection d'un nombre fini d'hyperplans, on peut être plus précis. Ainsi, il résulte de la formule (2.3) que la fonction $b_{Q,f,\ell,C}$ est uniformément continue sur l'ensemble $f(Q) + C$. En particulier, il existe une constante réelle c' telle que :

$$b_{Q,f,\ell,C}(y) - c' \leq b_{Q,f,\ell,C}(y - y_0)$$

pour tout $y \in (f(Q) + C) \cap (y_0 + f(Q) + C)$. En fait, l'inégalité est encore satisfaite si $y \notin f(Q) + C$ puisque dans ce cas, le minorant vaut $-\infty$. Enfin, en posant $c'' = c + c'$, il vient :

$$b_{Q,f,\ell,C,D}(y) - c'' \leq b'_{Q,R,f,\ell,C,D}(y) \leq b_{Q,f,\ell,C,D}(y) \quad (2.4)$$

pour tout y sauf éventuellement ceux qui appartiennent à $D \cap (f(Q) + C)$ mais pas à $y_0 + f(Q) + C$. Il existe donc, si l'on veut, une zone de trouble autour de la frontière de $f(Q) + C$ sur laquelle on ne sait pas contrôler le comportement de la fonction $b'_{Q,R,f,\ell,C,D}$.

2.2 Étude du cône convexe Φ

On reprend la situation du théorème 1.9 : on note I l'ensemble des couples d'entiers (i, j) tels que $1 \leq i \leq j \leq d$, et K le sous-ensemble convexe de $(\mathbb{R}^2)^I$ définis par les égalités (1.5) et (1.6) et les inégalités (1.12). En fait, comme nous l'avons déjà dit, la formule (1.7) nous permet de nous passer des $\mu_{i,j}$ ce que nous allons faire à partir de maintenant. On considère donc plutôt l'espace vectoriel $E = \mathbb{R}^I$ formés des suites $q = (q_{i,j})_{(i,j) \in I}$ indexées par les éléments de I , et à l'intérieur de celui-ci, le cône convexe Q défini par les inégalités

$$\text{(Jeu I) : } \quad \text{si } 1 \leq i \leq j < d, q_{i,j} \geq q_{i,j+1}$$

$$\text{(Jeu II) : } \quad \text{si } 1 \leq i \leq j < d, q_{i,j} \leq q_{i+1,j+1}$$

$$\text{(Jeu III) : } \quad \text{si } 1 \leq i \leq j < d,$$

$$bq_{j,j} - q_{j,d} + b \cdot \sum_{s=i}^{j-1} (q_{s,j} - q_{s,j-1}) \geq bq_{j+1,j+1} - q_{j+1,d} + b \cdot \sum_{s=i+1}^j (q_{s,j+1} - q_{s,j})$$

qui correspondent aux inégalités (1.12) dans lesquelles on a remplacé chaque apparition d'un $\mu_{i,j}$ par son expression en fonction des $q_{i,j}$. Le théorème 1.9 dit alors que l'application $\varphi \mapsto (q_{i,j}(\varphi))_{(i,j) \in I}$ définit une bijection entre Φ et Q .

Munissons E du produit scalaire usuel : si $v = (v_{i,j})$ et $w = (w_{i,j})$ sont deux éléments de E , on pose

$$\langle v|w \rangle_E = \sum_{(i,j) \in I} v_{i,j} w_{i,j}.$$

Les inégalités définissant Q se réécrivent alors sous la forme $\langle \vec{v}_m | q \rangle_E \geq 0$ pour certains vecteurs explicites $\vec{v}_m \in E$ ($1 \leq m \leq M$). Une étude attentive des formules montre en outre que tous les vecteurs \vec{v}_m appartiennent à l'hyperplan « somme des coordonnées égale 0 ».

Notons comme précédemment Q^* le cône dual de Q (par rapport au produit scalaire $\langle \cdot | \cdot \rangle_E$) ; c'est simplement le cône convexe engendré par les vecteurs \vec{v}_m . En particulier, il est lui aussi inclus dans l'hyperplan « somme des coordonnées égale 0 ». Cependant, la présentation à l'aide des \vec{v}_m ne nous permet pas vraiment d'exprimer simplement les ensembles $A_{Q,f,\ell}$ qui apparaissent en 2.1, et que nous aurons à manipuler dans la suite. Pour cela, nous aurons plutôt besoin d'écrire Q^* comme l'intersection d'un certain nombre de demi-espaces. Malheureusement, de part sa complexité, le jeu III d'inégalités rend la chose difficile à réaliser. C'est pourquoi, nous allons devoir travailler avec certaines approximations Q . Les deux plus simples que nous considérerons sont les cônes convexes Q_{\min} et Q_{\max} définis comme suit : Q_{\max} est le cône convexe défini par les jeux d'inégalité I et II, tandis Q_{\min} est celui défini par le jeu I et le jeu II' ci-dessous :

$$\text{(Jeu II')} : \quad \text{si } 1 \leq i \leq j < d, q_{i,j} = q_{i+1,j+1}$$

Il est clair que $Q \subset Q_{\max}$ et un calcul aisé montre que $Q_{\min} \subset Q$. Ainsi on a des inclusions renversées au niveau des duaux $Q_{\max}^* \subset Q^* \subset Q_{\min}^*$, d'où on déduit que, pour toute donnée (f, ℓ, C, D) , l'encadrement

$$b_{Q_{\min},f,\ell,C,D} \leq b_{Q,f,\ell,C,D} \leq b_{Q_{\max},f,\ell,C,D} \quad (2.5)$$

est vrai. Il est maintenant temps de donner les présentations annoncées des cônes duaux Q_{\min}^* et Q_{\max}^* . Pour cela, nous avons besoin de la définition suivante.

Définition 2.5. Une partie J de I est dite *admissible* si pour tout couple $(i, j) \in J$, les deux couples $(i, j + 1)$ et $(i - 1, j - 1)$ sont dans J , pour peu qu'ils appartiennent encore à I .

On peut remarquer que les parties admissibles dans le sens précédent sont naturellement en bijection avec les parties de $\{1, \dots, d\}$: à une telle partie J , on fait correspondre l'ensemble T des nombres non nuls qui sont de la forme :

$$\text{Card}\{j \geq i \mid (i, j) \in J\}$$

pour un $i \in \{1, \dots, d\}$. Réciproquement, si T est un sous-ensemble de $\{1, \dots, d\}$, on note $t_1 > \dots > t_{\text{Card } T}$ ses éléments et on lui associe l'ensemble $J \subset I$ formé des couples (i, j) tels que $i \leq \text{Card } T$ et $j > d - t_i$. Il n'est alors pas difficile de vérifier que J ainsi défini est admissible et que les deux applications que l'on vient de définir sont des bijections inverses l'une de l'autre entre l'ensemble des parties admissibles de I et l'ensemble des parties de $\{1, \dots, d\}$. Par exemple, si $s \in \{1, \dots, d\}$, la partie admissible correspondant à l'ensemble $\{1, \dots, s\}$ est l'ensemble $I_s = \{(i, j) \in I \mid j - i \geq d - s\}$.

Proposition 2.6. Une suite $v = (v_{i,j})$ de E appartient à Q_{\min}^* si, et seulement si :

$$\sum_{(i,j) \in I} v_{i,j} = 0 \quad \text{et} \quad \forall s \in \{1, \dots, d\}, \quad \sum_{(i,j) \in I_s} v_{i,j} \leq 0.$$

Une suite $v = (v_{i,j})$ de E appartient à Q_{\max}^* si, et seulement si :

$$\sum_{(i,j) \in I} v_{i,j} = 0 \quad \text{et} \quad \forall J \subset I \text{ admissible}, \quad \sum_{(i,j) \in J} v_{i,j} \leq 0.$$

En utilisant l'identification décrite précédemment entre parties admissibles de I et parties de $\{1, \dots, d\}$, on peut réécrire la condition d'appartenant à Q_{\max}^* comme suit :

$$\sum_{(i,j) \in I} v_{i,j} = 0 \quad \text{et} \quad \forall T \subset \{1, \dots, d\}, \quad \sum_{s=1}^d \sum_{j=s+1}^{t_s} v_{j-s,j-1} \leq 0 \quad (2.6)$$

où t_s est le s -ième plus petit élément de T si $s \leq \text{Card } T$ et $t_s = d + 1$ sinon.

Démonstration de la proposition 2.6 : un peu de théorie des flots

Il est possible de donner une démonstration « à la main » de la proposition 2.6 mais, comme me l'a signalé Bodo Lass, la proposition peut également se déduire du théorème Flot-Maximal-Coupe-Minimale, classique en théorie des graphes. Nous avons choisi de présenter cette dernière approche qui est à la fois plus générale et plus conceptuelle.

Rappelons tout d'abord l'énoncé du théorème Flot-Maximal-Coupe-Maximale. Soit G un graphe fini orienté dans lequel on a privilégié deux sommets D (comme départ) et A (comme arrivée) et on a attribué à chaque arête a un nombre positif ou nul, éventuellement égal à $+\infty$, appelé *capacité de a* , et noté $c(a)$. Si a est une arête dans G , on notera $s_1(a)$ (resp. $s_2(a)$) le sommet duquel elle part (resp. auquel elle aboutit). Un flot de D vers A est une fonction f à valeurs réelles définie sur les arêtes de G satisfaisant les propriétés suivantes :

- pour toute arête a , on a $0 \leq f(a) \leq c(a)$;
- pour tout sommet s différent de D et A , on a $\sum_{a|s_1(a)=s} f(a) = \sum_{a|s_2(a)=s} f(a)$.

La dernière propriété implique que :

$$\sum_{a|s_1(a)=D} f(a) - \sum_{a|s_2(a)=D} f(a) = \sum_{a|s_2(a)=A} f(a) - \sum_{a|s_1(a)=A} f(a).$$

Cette valeur commune s'appelle la *valeur* du flot f et est notée $|f|$. Une *coupe* C de G est la donnée d'une partition de l'ensemble des sommets de G en deux parties \mathcal{D} et \mathcal{A} telles que $D \in \mathcal{D}$ et $A \in \mathcal{A}$. La *capacité* de la coupe C , que l'on notera $|C|$, est la somme des $c(a)$ étendue à toutes les arêtes a qui ont leur origine dans \mathcal{D} et leur arrivée dans \mathcal{A} .

Il est facile de voir que si f est un flot et C est une coupe sur le graphe G précédemment fixé, alors $|f| \leq |C|$. Ainsi, en passant aux bornes supérieures et inférieures, on obtient $\sup_{f \text{ flot}} |f| \leq \min_{C \text{ coupe}} |C|$ (notez qu'il n'y a qu'un nombre fini de coupes possibles).

Théorème 2.7 (Flot-Maximal-Coupe-Minimale). *Avec les notations précédentes, on a :*

$$\sup_{f \text{ flot}} |f| = \min_{C \text{ coupe}} |C|$$

et la borne supérieure précédente est atteinte.

Démonstration. Voir par exemple [12]. □

On se place à présent dans une situation un peu différente. On considère toujours un graphe fini orienté G mais on ne se donne plus de décoration : on ne suppose plus que deux de ses sommets sont privilégiés, ni que les arêtes de G sont munies d'une capacité. On note S l'ensemble des sommets de G . À un tel graphe, on associe l'espace euclidien $E_G = \mathbb{R}^S$ muni du produit scalaire usuel $\langle \cdot | \cdot \rangle_G$ et Q_G le cône convexe regroupant les éléments $x = (x_s)_{s \in S} \in E_G$ vérifiant

$$x_{s_2(a)} \leq x_{s_1(a)}$$

pour toute arête a de G .

Définition 2.8. Un sous-ensemble S' de S est dit *admissible* si toute arête de G ayant son origine dans S' a aussi son but dans S' .

On a alors la proposition suivante, de laquelle il résulte facilement la proposition 2.6.

Proposition 2.9. *On conserve les notations précédentes, et on note Q_G^* le cône dual de Q_G par rapport au produit scalaire $\langle \cdot | \cdot \rangle_G$. Alors un élément $x = (x_s)_{s \in S} \in E_G$ appartient à Q_G^* si, et seulement si :*

$$\sum_{s \in S} x_s = 0 \quad \text{et} \quad \forall S' \subset S \text{ admissible, } \sum_{s \in S'} x_s \leq 0.$$

Démonstration. De la définition de Q_G , il résulte que Q_G^* est un cône convexe engendré par des vecteurs de l'hyperplan « somme des coordonnées égale 0 ». Ainsi Q_G^* est inclus dans cet hyperplan. Par ailleurs, si $S' \subset S$ un ensemble admissible de sommets, l'opposé de la fonction indicatrice de S' définit un vecteur $-\mathbb{1}_{S'} \in Q_G$, d'où on déduit que le produit scalaire $\langle x | \mathbb{1}_{S'} \rangle_G$ est négatif ou nul dès que $x \in Q_G^*$. Les éléments de Q_G^* vérifient donc bien les conditions de la proposition.

Réciproquement, considérons un vecteur $x = (x_s) \in E_G$ vérifiant ces conditions. Soit M un nombre réel positif assez grand pour que toutes les sommes $x_s + M$ (pour s décrivant S) soient positives ou nulles. Introduisons le graphe \tilde{G} obtenu à ajoutant à G deux nouveaux sommets notés D et A et, pour tout sommet s de G , une arête de D vers s et une arête de s vers A . On définit une capacité c sur \tilde{G} comme suit :

- si a est une arête de G , on pose $c(a) = +\infty$;

- si a part de D et arrive à un sommet s de G , on pose $c(a) = x_s + M$;
- si a part d'un sommet s de G et arrive à A , on pose $c(a) = M$.

Soit $C = (\mathcal{P}, \mathcal{A})$ une coupe de \tilde{G} . Posons $S' = \mathcal{P} \setminus \{P\}$; c' est un sous-ensemble de S . Si S' n'est pas admissible, cela signifie qu'il existe une arête reliant un sommet de S' à un sommet de $S \setminus S'$. Autrement dit, il existe une arête reliant un sommet de \mathcal{P} à un sommet de \mathcal{A} qui est dans G , c'est-à-dire qui est de capacité infinie. Dans ce cas, la capacité de la coupe C est donc infinie. Si, au contraire, l'ensemble des sommets S' est admissible, la capacité de la coupe C vérifie :

$$|C| = \sum_{s \in S'} M + \sum_{s \in S \setminus S'} (x_s + M) = nM - \sum_{s \in S'} x_s \geq nM$$

où on a noté n le nombre de sommets de G . Ainsi la capacité minimale d'une coupe, notée c_{\min} est, elle aussi, supérieure ou égale à nM . D'après le théorème Flot-Maximal-Coupe-Minimale, il existe un flot f sur \tilde{G} , de valeur c_{\min} . Comme la somme des capacités des arêtes sortant de D est nM , la capacité de ce flot est inférieure ou égale à nM . On en déduit qu'elle est égale à nM (et donc qu'il en est de même de c_{\min}) et que toute arête partant de D est saturée, c'est-à-dire que pour toute arête a partant de D , on a $f(a) = c(a) = M + x_{s_2(a)}$. De même, on démontre que, pour toute arête a partant d'un sommet $s \in S$ et aboutissant en D , on a $f(a) = c(a) = M$. Par la condition de flot, on a pour tout sommet $s \in S$:

$$\sum_{a|s_1(a)=s} f(a) - \sum_{a|s_2(a)=s} f(a) = x_s$$

où, dans les sommes précédentes, a désigne une arête de G . Ainsi, pour tout $y = (y_s) \in Q_G$, on a :

$$\langle x|y \rangle_E = \sum_{s \in S} y_s \cdot \left(\sum_{a|s_1(a)=s} f(a) - \sum_{a|s_2(a)=s} f(a) \right) = \sum_a (y_{s_1(a)} - y_{s_2(a)}) f(a) \geq 0$$

d'où on déduit finalement que $x \in Q_G^*$ comme voulu. \square

2.3 Un premier exemple d'application

À titre d'exemple, et afin de familiariser le lecteur avec les méthodes de cet article, nous aimerions montrer comment la machinerie que l'on vient d'introduire permet de démontrer la majoration du théorème 2 sous l'hypothèse supplémentaire $b \geq d-1$. Ce cas est intéressant car de nombreuses difficultés techniques s'évanouissent, mais il permet tout de même, selon nous, de donner une idée correcte de la nature des raisonnements que nous allons mener dans la section suivante.

Pour ne pas avoir, dans la suite, à distinguer systématiquement les cas selon que σ vaille ou non l'identité, on se restreint à partir de maintenant à $\sigma \neq \text{id}$, le cas contraire se traitant de façon complètement analogue en ajoutant $\frac{d(d-1)}{2}$ à tous les majorants.

2.3.1 Positionnement du problème

Un réseau L de M définit un k -point de la variété $\mathcal{X}_{\leq e}$ si, et seulement si les exposants des diviseurs élémentaires du $k[[u]]$ -module engendré par $\phi(L)$ par rapport à L sont tous compris entre 0 et e . Si on note ceux-ci $\mu_1(L) \geq \dots \geq \mu_d(L)$ comme dans la proposition 1.2, cela se réécrit $\mu_1(L) \leq e$ et $\mu_d(L) \geq 0$. Par ailleurs, si on note $q_{i,j}(L)$ et $\mu_{i,j}(L)$ les nombres réels associés au d -uplet de fonctions $\varphi(L) = (\varphi_1(L), \varphi_2(L), \dots, \varphi_d(L))$, l'assertion 4 de la proposition 1.2 combinée à la proposition 1.6 nous dit que $\mu_j(L) = \mu_{1,j}(L)$ pour tout indice $j \in \{1, \dots, d\}$. Ces observations nous donnent une décomposition de la variété $\mathcal{X}_{\leq e}$ en union disjointe comme suit :

$$\mathcal{X}_{\leq e} = \bigsqcup_{\varphi \in \Phi_{\leq e}} \mathcal{X}_{\varphi}$$

où l'ensemble $\Phi_{\leq e}$ réunit les $\varphi \in \Phi$ tels que $\mu_{1,1}(\varphi) \leq e$ et $\mu_{1,d}(\varphi) \geq 0$. On déduit directement de cette écriture, une formule au niveau des dimensions :

$$\dim_k \mathcal{X}_{\leq e} = \sup_{\varphi \in \Phi_{\leq e}} \dim_k \mathcal{X}_{\varphi}.$$

Comme précédemment, notons E l'espace des suites indicées par l'ensemble I , et Q le cône convexe défini par les jeux I, II et III d'inégalités. Soit $f : E \rightarrow \mathbb{R}^2$ l'application linéaire qui à une famille $(q_{i,j})$ associe le couple $(\mu_{1,1}, \mu_{1,d})$ où ces réels sont définis comme d'habitude par la formule (1.7). Par ailleurs, par le lemme 1.14, la fonction \dim s'étend en une forme linéaire $\ell : E \rightarrow \mathbb{R}$. Définissons enfin $C = \mathbb{R}^+ \times \mathbb{R}^-$, $D = \mathbb{R}^2$ et notons R le réseau formé des éléments $(q_{i,j}) \in E$ tels que $q_{i,j} \in \frac{1}{b}\mathbb{Z}$ pour tout $(i,j) \in I$ et $q_{i,d} \in \mathbb{Z}$ pour tout $i \in \{1, \dots, d\}$. Les théorèmes 1.9 et 1.17, couplés à la proposition 1.10, fournissent alors l'égalité (on rappelle que l'on suppose $\sigma \neq \text{id}$) :

$$\dim_k \mathcal{X}_{\leq e} = b'_{Q,R,f,\ell,C}(e, 0) \quad (2.7)$$

et donc en particulier $\dim_k \mathcal{X}_{\leq e} \leq b_{Q,R,f,\ell,C}(e, 0)$. Pour estimer ce dernier nombre, nous allons utiliser l'encadrement (2.5), et évaluer les fonctions $b_{Q_{\min},f,\ell,C}$ et $b_{Q_{\max},f,\ell,C}$ à l'aide d'une part de la proposition 2.2 et d'autre part de la description des cônes duaux Q_{\min}^* et Q_{\max}^* donnée dans la proposition 2.6. Cependant, pour pouvoir ce faire, nous devons préalablement exprimer les coordonnées de la fonction f ainsi que la forme linéaire ℓ comme des produits scalaires contre certains vecteurs de E . C'est ce que nous allons faire tout de suite.

2.3.2 Les vecteurs $\vec{\mu}_1, \dots, \vec{\mu}_d$ et $\vec{\delta}$

Pour un indice i compris entre 1 et d , introduisons le vecteur $\vec{\mu}_i \in E$ tel que pour une suite $q = (q_{i,j}) \in E$, on ait $\mu_{i,1} = \langle q | \vec{\mu}_i \rangle_E$ où $\mu_{i,1}$ est, comme précédemment, le réel calculé par la formule (1.7)⁵. Si l'on décide de représenter les éléments de E comme des matrices triangulaires supérieures (le terme d'indice (i,j) étant placé à l'intersection de la i -ième ligne et de la j -ième colonne), on a ainsi :

$$\vec{\mu}_i = \begin{pmatrix} 0 & \dots & 0 & -b & b & 0 & \dots & 0 \\ & \ddots & & & & & & \\ & & 0 & & & & & \\ & & & -b & & & & 0 \\ & & & & b & 0 & \dots & 0 \\ & & & & & 0 & \dots & -1 \\ & & & & & & 0 & \dots & 0 \\ & & & & & & & \ddots & \\ & & & & & & & & 0 \end{pmatrix}$$

où le b sur la diagonale est à l'intersection de la i -ième ligne et de la i -ième colonne. De même, définissons le vecteur $\vec{\delta}$ par $\langle q | \vec{\delta} \rangle_E = \ell(q)$ pour tout $q \in E$. Le lemme 1.14 montre que $\vec{\delta}$ s'exprime comme suit :

$$\vec{\delta} = b \cdot \begin{pmatrix} 1 & \dots & 1 & 0 \\ & \ddots & & -1 \\ & & & \vdots \\ & & & 1 \\ & & & & 2-d \\ & & & & & 1-d \end{pmatrix} + \begin{pmatrix} 0 & \dots & 0 & 1-d \\ & \ddots & & 3-d \\ & & & \vdots \\ & & & 0 \\ & & & & d-3 \\ & & & & & d-1 \end{pmatrix}.$$

Si $J \subset I$ est un sous-ensemble admissible (voir définition 2.5) et si $x = (x_{i,j}) \in E$, on notera $S_J(x)$ la somme des coordonnées $x_{i,j}$ pour (i,j) parcourant J . Les fonctions S_J ainsi définies sont clairement des formes linéaires sur E . Si T est la partie de $\{1, \dots, d\}$ correspondant à l'ensemble admissible J , on s'autorise à noter S_T à la place de S_J . Pour les calculs à suivre, le lemme suivant nous sera fort utile.

Lemme 2.10. *Si T est un sous-ensemble de $\{1, \dots, d\}$, on a :*

$$S_T(\vec{\mu}_i) = b \cdot \mathbb{1}_T(d+1-i) - [(\text{Card } T) \geq i]$$

où $\mathbb{1}_T$ est la fonction indicatrice de T et l'expression $[(\text{Card } T) \geq i]$ vaut 1 si $\text{Card } T \geq i$ et 0 sinon. On a aussi :

$$S_T(\vec{\delta}) = b \cdot \left(\sum_{t \in T} t - \frac{\text{Card } T \cdot (\text{Card } T + 1)}{2} \right) - \text{Card } T \cdot (d - \text{Card } T).$$

Démonstration. C'est un simple calcul à partir des descriptions précédentes. □

⁵Pour le calcul de la dimension de $\mathcal{X}_{\leq e}$, seuls les vecteurs $\vec{\mu}_1$ et $\vec{\mu}_d$ seront utiles. Cependant, les autres vecteurs $\vec{\mu}_i$ serviront dans la suite pour estimer la dimension d'autres variétés, et nous avons pensé qu'il était préférable de les introduire tous en même temps.

2.3.3 Calcul du majorant

Commençons par calculer la fonction $b_{Q_{\min},f,\ell,C}$ en utilisant la proposition 2.2, ce qui nous amène à déterminer l'ensemble $B_{Q_{\min},f,\ell,C} = A_{Q_{\min},f,\ell} \cap C^*$. Il est facile de voir que $C^* = \mathbb{R}^+ \times \mathbb{R}^-$; reste donc à calculer $A_{Q_{\min},f,\ell}$. Comme $f = (\langle \vec{\mu}_1, \cdot \rangle_E, \langle \vec{\mu}_d, \cdot \rangle_E)$ et $\ell = \langle \vec{\delta}, \cdot \rangle_E$, la formule (2.1) s'écrit :

$$A_{Q_{\min},f,\ell} = \{ y = (y_1, y_d) \in \mathbb{R}^2 \mid y_1 \vec{\mu}_1 + y_d \vec{\mu}_d - \vec{\delta} \in Q_{\min}^* \}.$$

On cherche donc les couples (y_1, y_d) tels que $y_1 \geq 0$, $y_d \leq 0$, et $y_1 \vec{\mu}_1 + y_d \vec{\mu}_d - \vec{\delta} \in Q_{\min}^*$. D'après la proposition 2.6, la dernière condition se réécrit :

$$\begin{cases} y_1 S_{I_s}(\vec{\mu}_1) + y_d S_{I_s}(\vec{\mu}_d) \leq S_{I_s}(\vec{\delta}) & \forall s \in \{1, \dots, d\} \\ y_1 S_{I_d}(\vec{\mu}_1) + y_d S_{I_d}(\vec{\mu}_d) = S_{I_d}(\vec{\delta}) \end{cases} \quad (2.8)$$

où on rappelle que I_s désigne l'ensemble admissible formé des couples $(i, j) \in I$ tels que $j - i \geq d - s$. Comme cet ensemble correspond à la partie $T = \{1, \dots, s\}$, le lemme 2.10 nous dit que si $s < d$, on a $S_{I_s}(\vec{\mu}_1) = -1$, $S_{I_s}(\vec{\mu}_d) = b$ et $S_{I_s}(\vec{\delta}) = -s(d-s)$, tandis que pour $s = d$, on a $S_{I_d}(\vec{\mu}_1) = S_{I_d}(\vec{\mu}_d) = b-1$, $S_{I_d}(\vec{\delta}) = 0$. Ainsi, le système (2.8) est équivalent à :

$$y_1 + y_d = 0 \quad \text{et} \quad y_1 \geq \frac{s(d-s)}{b+1}, \quad \forall s \in \{1, \dots, d-1\}.$$

Comme on voit aisément que le maximum de $s(d-s)$ vaut $\lfloor \frac{d^2}{4} \rfloor$, l'ensemble $B_{Q_{\min},f,\ell,C}$ est formé des couples $(y, -y)$ avec $y \geq \lfloor \frac{d^2}{4} \rfloor \cdot \frac{1}{b+1}$. Ainsi, si $y_1 \geq y_d$, on obtient :

$$b_{Q_{\min},f,\ell,C}(y_1, y_d) = \left\lfloor \frac{d^2}{4} \right\rfloor \cdot \frac{y_1 - y_d}{b+1}.$$

On souhaite à présent montrer que l'expression ci-dessus vaut encore pour la fonction $b_{Q_{\max},f,\ell,C}$. Comme on sait que $b_{Q_{\min},f,\ell,C} \leq b_{Q_{\max},f,\ell,C}$, il suffit, pour établir ce que l'on veut, de montrer que $(\lfloor \frac{d^2}{4} \rfloor \cdot \frac{1}{b+1}, -\lfloor \frac{d^2}{4} \rfloor \cdot \frac{1}{b+1}) \in B_{Q_{\max},f,\ell,C}$, c'est-à-dire que pour toute partie $T \in \{1, \dots, d\}$, on a :

$$\left\lfloor \frac{d^2}{4} \right\rfloor \cdot (S_T(\vec{\mu}_1) - S_T(\vec{\mu}_d)) \leq (b+1) \cdot S_T(\vec{\delta}).$$

(Notez que le cas d'égalité, qui doit être obtenu pour $T = \{1, \dots, d\}$, a déjà été vérifié.) On commence par éliminer les cas triviaux $T = \emptyset$ et $T = \{1, \dots, d\}$, et on distingue ensuite quatre cas selon que les entiers 1 et d appartiennent ou n'appartiennent pas à T . Remarquons d'abord que si $T = \{t_1, \dots, t_s\}$ avec $t_1 < \dots < t_s$, la formule du lemme 2.10 se réécrit

$$S_T(\vec{\delta}) = -s(d-s) + b \sum_{i=1}^s t_i - i. \quad (2.9)$$

Si $1 \in T$ et $d \notin T$, alors $S_T(\vec{\mu}_1) - S_T(\vec{\mu}_d) = -b-1$ et l'inégalité à démontrer devient $S_T(\vec{\delta}) \geq -\lfloor \frac{d^2}{4} \rfloor$. Or les $t_i - i$ étant tous positifs ou nuls, la formule (2.9) montre que $S_T(\vec{\delta}) \geq -s(d-s)$ d'où il suit ce que l'on veut. Pour les autres cas, il est important de remarquer que si $1 \notin T$, alors tous les $t_i - i$ sont supérieurs ou égaux à 1, alors que si $d \in T$, on a $t_s - s = d - s$. En particulier, si l'on excepte le cas que l'on vient de traiter, c'est-à-dire si l'on suppose que $1 \notin T$ ou que $d \in T$, on a

$$S_T(\vec{\delta}) \geq b \cdot \min(s, d-s) - s(d-s).$$

Comme on a supposé $b \geq d-1$, on en déduit que $S_T(\vec{\delta}) \geq 0$, ce qui suffit à conclure dans le cas où les deux nombres 1 et d appartiennent (resp. n'appartiennent pas) à T puisqu'alors $S_T(\vec{\mu}_1) - S_T(\vec{\mu}_d) = -1 \leq 0$. Si finalement, $1 \notin T$ et $d \in T$, la minoration de $S_T(\vec{\delta})$ est renforcée comme suit :

$$S_T(\vec{\delta}) \geq b(s-1+d-s) - s(d-s) = b(d-1) - s(d-s) \geq b(d-1) - \left\lfloor \frac{d^2}{4} \right\rfloor.$$

Étant donné que $S_T(\vec{\mu}_1) - S_T(\vec{\mu}_d) = b - 1$ dans ce cas, il suffit d'établir l'inégalité

$$(b + 1) \left(b(d - 1) - \left\lfloor \frac{d^2}{4} \right\rfloor \right) \geq (b - 1) \cdot \left\lfloor \frac{d^2}{4} \right\rfloor,$$

mais cela suit à nouveau de l'inégalité $b \geq d - 1$. On a finalement démontré que

$$b_{Q_{\max}, f, \ell, C}(y_1, y_d) = \left\lfloor \frac{d^2}{4} \right\rfloor \cdot \frac{y_1 - y_d}{b + 1} \quad \text{pour } y_1 \geq y_d.$$

à partir de quoi il résulte la majoration du théorème 2 puisque l'on sait que la dimension de $\mathcal{X}_{\leq e}$ est majorée par $b_{Q, f, \ell, C}(e, 0)$ lui même majoré par $b_{Q_{\max}, f, \ell, C}(e, 0)$.

3 Dimension des variétés $\mathcal{X}_{\leq e}$, \mathcal{X}_μ et $\mathcal{X}_{\leq \mu}$

Pour estimer les dimensions des variétés $\mathcal{X}_{\leq e}$, \mathcal{X}_μ et $\mathcal{X}_{\leq \mu}$, nous suivons la méthode introduite précédemment, sauf que nous remplaçons désormais la fonction f par la fonction

$$g : E \rightarrow \mathbb{R}^d, \quad q \mapsto (\langle \vec{\mu}_1 | q \rangle_E, \langle \vec{\mu}_2 | q \rangle_E, \dots, \langle \vec{\mu}_d | q \rangle_E)$$

et que la lettre C fait désormais référence au nouveau cône convexe $\{(y_1, \dots, y_d) \in \mathbb{R}^d \mid y_1 \geq \dots \geq y_d\}$. Toutes les autres notations ($Q, R, Q_{\min}, Q_{\max}, \ell, \vec{\mu}_i, \vec{\delta}$, etc.) sont conservées ; nous nous contentons donc de renvoyer le lecteur aux §§2.2 et 2.3.2 s'il souhaite se remémorer les définitions. Le cône dual de C jouera un rôle particulier dans la suite ; remarquons d'ores et déjà qu'il est engendré par les vecteurs de la forme $(0, \dots, 0, 1, -1, 0, \dots, 0)$. On en déduit facilement une description en termes d'inégalités :

$$C^* = \left\{ (z_1, \dots, z_d) \in \mathbb{R}^d \mid \begin{array}{l} z_1 + \dots + z_d = 0 \\ z_1 + \dots + z_i \geq 0, \forall i \in \{1, \dots, d\} \end{array} \right\}.$$

Remarquons encore qu'étant donné que les vecteurs $\vec{\mu}_i$ forment trivialement une famille libre dans E , l'application linéaire g est surjective. Ceci nous autorise à appliquer la proposition 2.3 avec les données que nous venons de décrire.

À partir de maintenant, on se restreint à nouveau au cas où $\sigma \neq \text{id}$, le cas opposé se traitant exactement de la même façon sauf qu'il faut ajouter $\frac{d(d-1)}{2}$ à tous les majorants. Par le théorème 1.17, pour $\mu = (\mu_1, \dots, \mu_d)$ vérifiant les bonnes hypothèses, la dimension de \mathcal{X}_μ (resp. $\mathcal{X}_{\leq \mu}$) est majorée (et même bien approchée en vertu de la proposition 2.3) par le nombre $b_{Q, g, \ell}(\mu)$ (resp. $b_{Q, g, \ell, C^*}(\mu)$). On est ainsi ramené à calculer $b_{Q, g, \ell, 0}(\mu)$ et $b_{Q, g, \ell, C^*}(\mu)$, et pour cela, à étudier les ensembles $B_{Q, g, \ell}$ et B_{Q, g, ℓ, C^*} . C'est ce que nous allons faire dans un premier temps.

3.1 Les points extrémaux de $A_{Q_{\max}, g, \ell}$

Notons \mathfrak{S}_d l'ensemble des permutations de l'ensemble $\{1, \dots, d\}$. Pour tout $w \in \mathfrak{S}_d$, définissons le vecteur $\vec{\rho}_w \in \mathbb{R}^d$ par :

$$\vec{\rho}_w = \left((b - 1) \cdot \sum_{n=1}^{\infty} \frac{d + 1 - i - w^n(i)}{b^n} \right)_{1 \leq i \leq d}.$$

Il est clair que la somme infinie que l'on vient d'écrire converge. En fait, la suite des $w^n(i)$ étant périodique, elle converge même vers un nombre rationnel (qui s'exprime comme l'évaluation en b d'une fraction rationnelle coefficients entiers). Remarquons également que lorsque $w = w_0$ est la permutation $i \mapsto d + 1 - i$, le vecteur $\vec{\rho}_{w_0}$ est égal à $\frac{2\vec{\rho}}{b+1}$ où on rappelle que $\vec{\rho} = (\frac{d-1}{2}, \frac{d-3}{2}, \dots, \frac{1-d}{2})$.

Proposition 3.1. *On suppose $b \geq 1 + \frac{d^2}{4}$. Les points extrémaux de $A_{Q_{\max}, g, \ell}$ sont exactement les vecteurs $\vec{\rho}_w$ pour w parcourant le groupe des permutations de $\{1, \dots, d\}$.*

Nous consacrons la fin de cette partie à la démonstration de la proposition. On peut d'ores et déjà présenter le convexe $A_{Q_{\max}, g, \ell}$ comme une intersection de demi-espaces ; il suffit pour cela d'injecter la

description de Q_{\max}^* donnée par la proposition 2.6 dans la formule (2.1). On obtient ainsi qu'un élément $y = (y_1, \dots, y_d) \in \mathbb{R}^d$ appartient à $A_{Q_{\max}, g, \ell}$ si, et seulement si

$$y_1 S_T(\vec{\mu}_1) + y_2 S_T(\vec{\mu}_2) + \dots + y_d S_T(\vec{\mu}_d) \leq S_T(\vec{\delta})$$

pour toute partie $T \subset \{1, \dots, d\}$ et l'égalité est atteinte lorsque $T = \{1, \dots, d\}$. Avec les expressions du lemme 2.10, ceci se réécrit :

$$\begin{cases} y_1 + y_2 + \dots + y_d = 0 \\ f_T(y) \geq 0, \quad \forall T \subsetneq \{1, \dots, d\} \end{cases} \quad (3.1)$$

où on a posé $s = \text{Card}T$ et :

$$f_T(y) = (y_1 + \dots + y_s) - b \cdot \sum_{t \in T} y_{d+1-t} - s(d-s) + b \cdot \left(\sum_{t \in T} t - \frac{s(s+1)}{2} \right). \quad (3.2)$$

Ceci étant dit, un point extrémal de $A_{Q_{\max}, g, \ell}$ n'est autre qu'un point de $A_{Q_{\max}, g, \ell}$ qui se trouve être à l'intersection de $d-1$ hyperplans affines indépendants parmi ceux d'équation $f_T(x) = 0$ avec $T \subsetneq \{1, \dots, d\}$. Calculer ces points revient donc à déterminer une condition nécessaire et suffisante sur les parties T_1, \dots, T_{d-1} de $\{1, \dots, d\}$ pour que :

- i) en posant $T_d = \{1, \dots, d\}$, les hyperplans affines d'équation $f_{T_i}(x) = 0$ ($1 \leq i \leq d$) aient un unique point d'intersection, et
- ii) ce point d'intersection appartienne à $A_{Q_{\max}, g, \ell}$.

On commence par deux lemmes.

Lemme 3.2. *Considérons des entiers m et n tels que $0 \leq m < n \leq d$. Soit également $y = (y_1, \dots, y_d) \in A_{Q_{\max}, g, \ell}$. Alors :*

$$-m(n-m) \leq x_{m+1} + x_{m+2} + \dots + x_n \leq (n-m)(d-n).$$

Démonstration. Commençons par prouver la majoration. Dans le cas où $m = 0$, celle-ci provient directement de l'inégalité $f_T(y) \geq 0$ où $T = \{d+1-n, \dots, d\}$. Dans le cas où $m > 0$, on considère la partie $T = \{d+1-n, \dots, d-m\}$. L'inégalité $f_T(y) \geq 0$ donne alors :

$$(y_1 + \dots + y_{n-m}) - b(y_{m+1} + \dots + y_n) \geq (n-m)(d-n+m) - b(n-m)(d-n).$$

Mais par ailleurs, on sait déjà que $y_1 + \dots + y_{n-m} \leq (n-m)(d-n+m)$. Le résultat s'ensuit. Pour la minoration, le plus rapide est sans doute de remarquer que l'application $(y_1, \dots, y_d) \mapsto (-y_d, \dots, -y_1)$ définit une bijection de $A_{Q_{\max}, g, \ell}$ dans lui-même. Via cette bijection, la majoration que nous venons de démontrer donne la minoration. \square

Lemme 3.3. *On suppose $b > d$. Soient T_1 et T_2 deux parties de $\{1, \dots, d\}$, et soit $y \in A_{Q_{\max}, g, \ell}$. On a :*

$$f_{T_1}(y) + f_{T_2}(y) \geq f_{T_1 \cap T_2}(y) + f_{T_1 \cup T_2}(y)$$

et l'égalité a lieu si, et seulement si $T_1 \subset T_2$ ou $T_2 \subset T_1$.

Démonstration. Notons $s_1, s_2, s_{1 \cap 2}$ et $s_{1 \cup 2}$ les cardinaux respectifs de $T_1, T_2, T_1 \cap T_2$ et $T_1 \cup T_2$. On a évidemment $s_1 + s_2 = s_{1 \cap 2} + s_{1 \cup 2}$ et $s = s_1 - s_{1 \cap 2} = s_{1 \cup 2} - s_2 \geq 0$. Par ailleurs, quitte à intervertir T_1 et T_2 , on peut supposer $s_1 \leq s_2$. Un calcul immédiat conduit alors à

$$\begin{aligned} & f_{T_1}(y) + f_{T_2}(y) - f_{T_1 \cap T_2}(y) - f_{T_1 \cup T_2}(y) \\ &= (y_{s_{1 \cap 2}+1} + \dots + y_{s_1}) - (y_{s_2+1} + \dots + y_{s_{1 \cup 2}}) + \frac{1}{2} \cdot s(b-2) \cdot (s_{1 \cup 2} + s_2 - s_1 - s_{1 \cap 2}). \end{aligned}$$

à partir de quoi, on trouve en utilisant le lemme précédent :

$$f_{T_1}(y) + f_{T_2}(y) - f_{T_1 \cap T_2}(y) - f_{T_1 \cup T_2}(y) \geq s \cdot ((b-1)(s_2 - s_1) + bs - d).$$

Il est clair que cette dernière expression est positive ou nulle et, qu'en outre, elle est strictement positive dès que $s \geq 1$. Le cas d'égalité ne peut donc se produire que lorsque $s = 0$, mais dire que $s = 0$ revient à dire que $T_1 \cap T_2 = T_1$, i.e. $T_1 \subset T_2$. \square

On est maintenant prêt à démontrer la proposition 3.1. On suppose donc $b \geq 1 + \frac{d^2}{4}$. Si l'on excepte le cas $b = d = 2$ que l'on vérifie à part à la main, on a $b > d$ et donc le lemme précédent s'applique. Considérons T_1, \dots, T_{d-1} des parties de $\{1, \dots, d\}$ vérifiant les hypothèses i) et ii) énoncées en amont des lemmes. On pose également $T_d = \{1, \dots, d\}$. Quitte à renuméroter les T_i , on peut supposer que leurs cardinaux sont rangés par ordre croissant. Puisque les hyperplans affines d'équation $f_{T_i}(y) = 0$ ($1 \leq i \leq d$) ont un unique point d'intersection, que l'on notera y dans la suite, il est clair que les T_i sont deux à deux distincts. Comme $y \in A_{Q_{\max, g, \ell}}$ par hypothèse, les nombres $f_{T_i \cup T_j}(y)$ et $f_{T_i \cap T_j}(y)$ sont positifs ou nuls pour tous indices i et j . Ainsi, on est nécessairement dans le cas d'égalité du lemme précédent, ce qui signifie, dans le cas où $i < j$, que $T_i \subset T_j$ d'après l'hypothèse supplémentaire que nous avons faite sur les cardinaux. Ainsi, on obtient

$$T_1 \subset T_2 \subset \dots \subset T_{d-1} \subset T_d = \{1, \dots, d\}$$

et toutes les inclusions sont strictes car nous avons déjà dit que les T_i étaient nécessairement deux à deux distincts. On en déduit qu'il existe une permutation $w^* \in \mathfrak{S}_d$ telle que $T_i = \{w^*(1), w^*(2), \dots, w^*(i)\}$ pour tout i . Il reste à calculer les coordonnées (y_1, \dots, y_d) du point y . Celles-ci sont solutions du système d'équations suivant :

$$\begin{cases} y_1 - by_{d+1-w^*(1)} = d - 1 - b(w^*(1) - 1) \\ (y_1 + y_2) - b(y_{d+1-w^*(1)} + y_{d+1-w^*(2)}) = d^2 - 4 - b(w^*(1) + w^*(2) - 3) \\ \vdots \\ (y_1 + \dots + y_{d-1}) - b(y_{d+1-w^*(1)} + \dots + y_{d+1-w^*(d-1)}) \\ \quad = d^2 - (d-1)^2 - b(w^*(1) + \dots + w^*(d-1) - \frac{d(d-1)}{2}) \\ y_1 + \dots + y_d = 0 \end{cases} \quad (3.3)$$

En retranchant chaque équation de sa précédente, le système se réécrit

$$y_i - by_{d+1-w^*(i)} = d + 1 - 2i - b(w^*(i) - i), \quad \text{pour } 1 \leq i \leq d.$$

En notant w la permutation inverse de $i \mapsto d + 1 - w^*(i)$, et en posant $z_i = y_i - d - 1 + 2i$ pour tout i , ceci se réécrit encore $z_i = w(i) - i + \frac{z_{w(i)}}{b}$ et donne donc :

$$z_i = w(i) - i + \frac{z_{w(i)}}{b} = w(i) - i + \frac{w^2(i) - w(i)}{b} + \frac{z_{w^2(i)}}{b^2} = \dots = \sum_{n=0}^{\infty} \frac{w^{n+1}(i) - w^n(i)}{b^n}.$$

Un calcul facile montre alors que $y = \vec{\rho}_w$. Réciproquement, pour montrer que $\vec{\rho}_w$ est un point extrémal, si l'on prend en considération ce que l'on a déjà dit, il reste à montrer qu'il appartient à $A_{Q_{\max, g, \ell}}$. Posons $y = \vec{\rho}_w$ et notons (y_1, \dots, y_d) ses coordonnées. Pour $T \subsetneq \{1, \dots, d\}$, un nouveau calcul conduit à l'égalité suivante :

$$\frac{f_T(y)}{b-1} = \sum_{n=0}^{\infty} \frac{1}{b^n} \left(\sum_{t \in T} w^{n+1}(d+1-t) - \sum_{i=1}^s w^n(i) \right) \quad (3.4)$$

où, comme d'habitude, s est le cardinal de T . Chaque facteur $\sum_{t \in T} w^{n+1}(d+1-t) - \sum_{i=1}^s w^n(i)$ est, en valeur absolue, inférieur ou égal $s(d-s)$, qui est lui-même inférieur ou égal à $\frac{d^2}{4}$. Ainsi, dans la somme infinie du membre de droite de l'égalité (3.4), la contribution des termes pour $n \geq 1$ est majorée en valeur absolue par $\frac{d^2}{4(b-1)} \leq 1$. Par ailleurs, la contribution pour $n = 0$ vaut $\sum_{t \in T} w(d+1-t) - \sum_{i=1}^s i$ qui est un nombre entier positif ou nul. S'il est strictement positif, il vaut au moins 1 et d'après ce qu'on a démontré précédemment, il ne peut être compensé par le reste de la somme ; ainsi on a bien $f_T(y) \geq 0$ dans ce cas. Si, maintenant, $\sum_{t \in T} w(d+1-t) = \sum_{i=1}^s i$, l'ensemble des $w(d+1-t)$ pour t parcourant T est nécessairement égal à l'ensemble $\{1, \dots, s\}$. Il en résulte que pour tout n , on a aussi $\sum_{t \in T} w^{n+1}(d+1-t) = \sum_{i=1}^s w^n(i)$, et donc que $f_T(y)$ est nul dans ce cas. Ainsi, pour tout sous-ensemble $T \subsetneq \{1, \dots, d\}$, on a $f_T(y) \geq 0$. Comme on a également $y_1 + \dots + y_d = 0$, on trouve bien $\vec{\rho}_w = y \in A_{Q_{\max, g, \ell}}$, et la proposition 3.1 est démontrée.

Lorsque $b > 1 + \frac{d^2}{4}$, on a un léger raffinement.

Lemme 3.4. *On conserve les notations de la démonstration de la proposition et on suppose $b > 1 + \frac{d^2}{4}$. Alors, si T n'est pas l'un des ensembles T_i , on a $f_T(\vec{\rho}_w) > 0$.*

En d'autres termes, le lemme dit que, sous l'hypothèse $d > 1 + \frac{d^2}{4}$, il ne concourt au sommet $\vec{\rho}_w$ que $d - 1$ faces correspondant aux hyperplans d'équation $f_{T_i}(y) = 0$ pour $1 \leq y \leq d - 1$. (Notez bien que l'équation $f_{T_d}(y) = 0$ définit l'hyperplan « somme des coordonnées égale 0 » dans lequel tout est plongé.)

Démonstration. Il suffit de remarquer que dans la somme de la formule (3.4), la contribution des termes obtenus pour $n \geq 1$ est maintenant strictement inférieure à 1, et que le fait que l'ensemble des $w(d + 1 - t)$ ($t \in T$) s'égalise avec $\{1, \dots, s\}$ signifie exactement que $T = T_s$. \square

Un mot sur les points extrémaux de $A_{Q_{\max, g, \ell}} + C^*$

On démontrera dans la suite que $A_{Q, g, \ell} = A_{Q_{\max, g, \ell}} + C^*$ (proposition 3.6) et, donc, plutôt que les points extrémaux de $A_{Q_{\max, g, \ell}}$, ce sont ceux de la somme $A_{Q_{\max, g, \ell}} + C^*$ que nous aimerions décrire. Ceux-ci forment un sous-ensemble des points extrémaux de $A_{Q_{\max, g, \ell}}$ qui, malheureusement, semble difficile à comprendre. On peut, malgré tout, définir un ordre sur \mathfrak{S}_d qui permet de comprendre un peu mieux ce qui se passe.

Voici comment on procède. Tout d'abord, pour tout entier $s \in \{1, \dots, d\}$, on définit le préordre \preccurlyeq_s par :

$$w_1 \preccurlyeq_s w_2 \quad \text{ssi} \quad \left(\sum_{i=1}^s w_1^n(i) \right)_{n \geq 1} \leq_{\text{lex}} \left(\sum_{i=1}^s w_2^n(i) \right)_{n \geq 1}$$

où \leq_{lex} désigne l'ordre lexicographique sur l'ensemble des suites, qui donne le plus de poids aux petits indices. On pose enfin :

$$w_1 \preccurlyeq w_2 \quad \text{ssi} \quad w_1 \preccurlyeq_s w_2 \quad \text{pour tout } s \in \{1, \dots, d\}.$$

On vérifie facilement que \preccurlyeq est bien un ordre sur \mathfrak{S}_d . À titre d'exemple, la figure 2 montre son diagramme de Hasse pour $d = 4$ (sur cette figure, la permutation w est notée $(w(1) w(2) w(3) w(4))$). Il existe déjà un certain nombre d'ordres sur le groupe des permutations \mathfrak{S}_d (ordre de Bruhat, ordre faible, *etc.*) mais celui que nous venons de définir ne semble coïncider avec aucun d'entre eux (en tout cas, pas avec ceux qui sont connus de l'auteur). Pour l'instant, l'ordre \preccurlyeq est donc encore assez mystérieux. Quoi qu'il en soit, on a la proposition suivante qui explique le lien avec la problématique de cet article.

Proposition 3.5. *On suppose $b \geq 1 + \frac{d^2}{4}$. Pour toutes permutations $w_1, w_2 \in \mathfrak{S}_d$, on a $w_1 \preccurlyeq w_2$ si, et seulement si $\vec{\rho}_{w_1} \in \vec{\rho}_{w_2} + C^*$.*

Démonstration. Les coordonnées de $\vec{\rho}_{w_1} - \vec{\rho}_{w_2}$ sont

$$(b - 1) \cdot \sum_{n=1}^{\infty} \frac{w_1^n(i) - w_2^n(i)}{b^n}$$

avec $1 \leq i \leq d$. Dire que ce vecteur est dans C^* revient donc à dire que, pour tout $s \in \{1, \dots, d\}$, on a :

$$\sum_{n=1}^{\infty} \frac{1}{b^n} \sum_{i=1}^s (w_1^n(i) - w_2^n(i)) \geq 0$$

et que l'égalité a lieu si $s = d$. En fait, il est clair que l'égalité est toujours vérifiée pour $s = d$; on peut donc oublier cette condition. À part cela, on remarque que la différence $w_1^n(i) - w_2^n(i)$ est toujours majorée en valeur absolue par $d - 1$. Ainsi, pour tout n , la somme $\sum_{i=1}^s w_1^n(i) - w_2^n(i)$ est majorée en valeur absolue par $\frac{d^2}{4(b-1)} \leq 1$. Le signe de la somme infinie dépend donc seulement du signe du premier terme non nul. La proposition découle de cela. \square

Il résulte de la proposition que si deux permutations w_1 et w_2 sont telles que $w_1 \preccurlyeq w_2$, alors $\vec{\rho}_{w_1}$ ne peut être un point extrémal de $A_{Q_{\max, g, \ell}} + C^*$ (toujours sous l'hypothèse $b \geq 1 + \frac{d^2}{4}$). Ainsi, les seuls points extrémaux envisageables correspondent aux permutations w qui sont des éléments maximaux pour \preccurlyeq . Par contre, il se peut que certains éléments maximaux ne définissent pas des points extrémaux de $A_{Q_{\max, g, \ell}} + C^*$; lorsque $d = 4$ par exemple, c'est le cas des vecteurs correspondant aux permutations $(2 4 3 1)$ et $(4 2 1 3)$ (qui sont bien des éléments maximaux comme on le voit sur la figure 2).

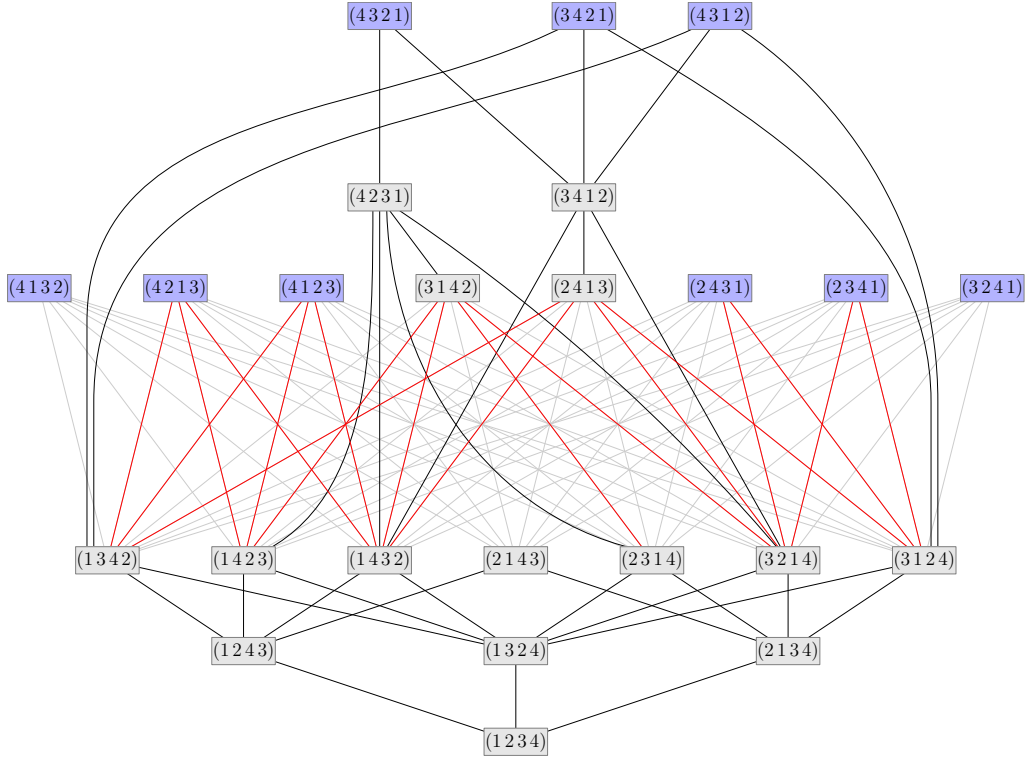


FIG. 2 – Diagramme de Hasse de l'ordre \preccurlyeq sur \mathfrak{S}_4

Les traits gris clairs sur la figure représentent, de la même façon que les traits noirs, des arêtes dans le graphe de Hasse. Attention : afin de faciliter la lecture, nous avons dessiné en rouge les arêtes entre une permutation du troisième étage et une du quatrième qui *ne* sont *pas* dans le diagramme de Hasse !

Les permutations coloriées en bleu sont les éléments maximaux.

3.2 Le calcul de $A_{Q,g,\ell}$

Le but de cette partie est de démontrer la proposition suivante.

Proposition 3.6. *On suppose $b > 1 + \frac{d^2}{4}$. Alors $A_{Q,g,\ell} = A_{Q_{\max},g,\ell} + C^*$.*

L'inclusion $A_{Q_{\max},g,\ell} + C^* \subset A_{Q,g,\ell}$ est facile. En effet, notons déjà que $A_{Q_{\max},g,\ell}$ est inclus dans $A_{Q,g,\ell}$. Soient maintenant $y = (y_1, \dots, y_d) \in A_{Q,g,\ell}$ et $z = (z_1, \dots, z_d) \in C^*$. Il suffit de montrer que $y + z \in A_{Q,g,\ell}$. Par définition de $A_{Q,g,\ell}$, on a $y_1 \vec{\mu}_1 + \dots + y_d \vec{\mu}_d - \vec{\delta} \in Q^*$, ce qui revient à dire que pour tout $q \in Q$,

$$y_1 \langle \vec{\mu}_1 | q \rangle_E + \dots + y_d \langle \vec{\mu}_d | q \rangle_E \geq \langle \vec{\delta} | q \rangle_E. \quad (3.5)$$

Par ailleurs, on sait que la suite des $\langle \vec{\mu}_j | q \rangle_E$ est décroissante en j ; autrement dit elle définit un vecteur de \mathbb{R}^d qui appartient à C . On en déduit que

$$z_1 \langle \vec{\mu}_1 | q \rangle_E + \dots + z_d \langle \vec{\mu}_d | q \rangle_E \geq 0. \quad (3.6)$$

Finalement en additionnant les formules (3.5) et (3.6), on trouve bien $y + z \in A_{Q,g,\ell}$ comme annoncé.

On se concentre désormais sur la démonstration de l'inclusion réciproque. À partir de maintenant, on suppose donc $b > 1 + \frac{d^2}{4}$. Commençons par expliquer la démarche générale. Pour tout point extrémal $\vec{\rho}_w$ de $A_{Q_{\max},g,\ell}$, notons D_w le cône convexe tel qu'au voisinage de $\vec{\rho}_w$, on ait $A_{Q_{\max},g,\ell} = \vec{\rho}_w + D_w$. Si $\vec{\rho}_w$ est un point extrémal de $A_{Q_{\max},g,\ell} + C^*$, les ensembles convexes $A_{Q_{\max},g,\ell} + C^*$ et $\vec{\rho}_w + D_w + C^*$ coïncident encore au voisinage de $\vec{\rho}_w$. On en déduit que

$$A_{Q_{\max},g,\ell} + C^* = \bigcap_{w \in \mathcal{S}_d} (\vec{\rho}_w + D_w + C^*)$$

| | | | | | | |
|-----|-----|---|---|---|---|---|
| | j | 1 | 2 | 3 | 4 | 5 |
| i | 1 | 4 | 3 | 1 | 1 | 1 |
| | 2 | | 4 | 3 | 2 | 2 |
| | 3 | | | 4 | 3 | 3 |
| | 4 | | | | 4 | 4 |
| | 5 | | | | | 5 |

FIG. 3 – La fonction $\text{ord}_{(32451)}$

où l'on a noté \mathcal{S}_d le sous-ensemble de \mathfrak{S}_d correspondant aux points extrémaux de $A_{Q_{\max, g, \ell}} + C^*$. Ainsi, il suffit de montrer que tout élément de $A_{Q, g, \ell}$ appartient à $\vec{\rho}_w + D_w + C^*$ pour tout $w \in \mathcal{S}_d$. Nous allons en fait montrer que c'est le cas pour tout $w \in \mathfrak{S}_d$ et pour cela nous allons interpréter la somme $\vec{\rho}_w + D_w + C^*$ comme des $A_{Q_w, g, \ell}$ pour certaines cônes convexes $Q_w \subset E$. Il suffira alors pour conclure de montrer que tous les Q_w contiennent Q .

3.2.1 Les ensembles Q_w

Fixons w une permutation de l'ensemble $\{1, \dots, d\}$. En nous inspirant du §3.1, notons w^* la permutation $i \mapsto d + 1 - w^{-1}(i)$ et, pour tout s compris entre 1 et d , définissons l'ensemble

$$T_s(w) = \{w^*(1), w^*(2), \dots, w^*(s)\}.$$

Cet ensemble correspond à une partie admissible de I que nous notons $I_s(w)$. Rappelons que, s étant fixé, si on note t_1, \dots, t_s les nombres $w^*(1), \dots, w^*(s)$ triés par ordre décroissant (i.e. $t_1 > t_2 > \dots > t_s$), alors le couple (i, j) est dans $I_s(w)$ si, et seulement si $i \leq s$ et $j > d - t_i$. Lorsque w est la permutation $\omega : i \mapsto d + 1 - i$, on a $w^* = \text{id}$ et donc $T_s(w) = \{1, \dots, s\}$; l'ensemble admissible $T_s(w)$ est alors simplement l'ensemble $I_s = \{(i, j) \in I \mid j - i \geq d - s\}$ que nous avons déjà considéré. On vérifie facilement que les ensembles $I_s(w)$ définissent une partition croissante de I telle que $I_d(w) = I$. Considérons la fonction $\text{ord}_w : I \rightarrow \{1, \dots, d\}$ qui à un couple (i, j) associe le plus petit entier s tel que $(i, j) \in I_s(w)$. De façon évidente, pour tout s , l'ensemble $I_s(w)$ regroupe les éléments $x \in I$ tels que $\text{ord}_w(x) \leq s$.

Pour se représenter les constructions que nous venons de faire, il est commode de considérer les éléments (i, j) comme les cases d'un tableau triangulaire (voir figure 3). La fonction ord_w correspond alors à un remplissage des cases du tableau par les nombres entiers compris entre 1 et d . Celui-ci s'obtient en fait très simplement à partir de la permutation w , comme suit. On place d'abord sur la ligne du haut et dans les $w(1)$ dernières colonnes du tableau le nombre 1. Ensuite, on place le nombre 2 dans les $w(2)$ dernières colonnes du tableau à chaque fois dans la case la plus haute qui n'est pas déjà remplie. Ainsi, si $w(2) < w(1)$, tous les nombres 2 se retrouvent sur la deuxième ligne, tandis que si $w(2) > w(1)$, on écrit $w(1)$ nombres 2 sur les 1 déjà écrits à l'étape précédente, et on met les $w(2) - w(1)$ nombres 2 restants sur la première ligne. On continue ensuite avec les 3 : on les place dans les $w(3)$ dernières colonnes, toujours le plus haut possible. Et ainsi de suite jusqu'à d . La figure 3 montre le remplissage obtenu pour la permutation (32451) (pour $d = 5$ donc).

On définit encore un graphe I_w comme suit : ses sommets sont les éléments de I et l'on convient qu'il y a une arête entre x et y dans ce graphe si $\text{ord}_w(x) \geq \text{ord}_w(y)$. Finalement, on introduit l'ensemble $Q'_w \subset E$: c'est le cône convexe Q_{I_w} associé au graphe I_w par la recette donnée juste en dessous de la définition 2.8.

Lemme 3.7. *On suppose $b > 1 + \frac{d^2}{4}$. Alors, on a $A_{Q'_w, g, \ell} = \vec{\rho}_w + D_w$.*

Démonstration. Les parties admissibles du graphe I_w (dans le sens de la définition 2.8) sont exactement les $I_s(w)$ pour $1 \leq s \leq d$. La proposition 2.9 nous assure donc que le cône dual $(Q'_w)^*$ est défini dans E par les équations :

$$\sum_{(i,j) \in I} x_{i,j} = 0 \quad \text{et} \quad \forall s \in \{1, \dots, s\}, \quad \sum_{(i,j) \in I_s(w)} x_{i,j} \leq 0.$$

où les $x_{i,j}$ sont les coordonnées canoniques sur $E = \mathbb{R}^I$. En injectant cela dans la formule (2.1) et en utilisant le lemme 2.10, on trouve qu'un élément $y = (y_1, \dots, y_d) \in \mathbb{R}^d$ appartient à $A_{Q'_w, g, \ell}$ si, et seulement

si $y_1 + \dots + y_d = 0$ et $f_{I_s(w)}(y) \geq 0$ pour tout s (où la fonction $f_{I_s(w)}$ est défini comme précédemment, voir formule (3.2)).

Par ailleurs, étant donné que b est supposé strictement supérieur à $1 + \frac{d^2}{4}$, le lemme 3.4 s'applique et implique que le cône D_w est défini par les équations et inéquations :

$$y_1 + \dots + y_d = 0 \quad \text{et} \quad g_{I_s(w)}(y) = 0$$

où, si T est une partie de $\{1, \dots, d\}$, on a noté g_T la fonction linéaire associé à f_T : pour tout $y = (y_1, \dots, y_n)$ dans \mathbb{R}^d , on a $g_T(y) = y_1 + \dots + y_s - b \cdot \sum_{t \in T} y_{d+1-t}$ avec $s = \text{Card } T$. Comme $\vec{\rho}_w$ a été justement construit pour vérifier $f_{I_s(w)}(\vec{\rho}_w) = 0$ pour tout s , l'égalité du lemme en découle. \square

Soit D le cône convexe de E défini par $D = \{q = (q_{i,j}) \in E \mid \mu_{1,1} \geq \mu_{1,2} \geq \dots \geq \mu_{1,d}\}$ où les $\mu_{i,j}$ sont définis à partir des $q_{i,j}$ par la formule (1.7). On rappelle que l'on a défini dans le §2.3.2 des vecteurs $\vec{\mu}_j \in \mathbb{R}^d$ tels que $\mu_{1,j} = \langle \vec{\mu}_j | q \rangle_E$ où $q = (q_{i,j}) \in E$. Ainsi D^* , le cône dual de D , n'est autre que le cône convexe engendré par les vecteurs $\vec{\mu}_j - \vec{\mu}_{j+1}$ pour j parcourant l'ensemble d'indices $\{1, \dots, d-1\}$. Par ailleurs, on se souvient que l'application g est définie par $q \mapsto (\langle \vec{\mu}_1 | q \rangle_E, \dots, \langle \vec{\mu}_1 | q \rangle_E)$ et donc qu'elle envoie D^* sur l'ensemble des $y = (y_1, \dots, y_d) \in \mathbb{R}^d$ tels que $y_1 \geq \dots \geq y_d$, c'est-à-dire C . On pose enfin $Q_w = Q'_w \cap D \subset E$. Le cône dual de Q_w est alors égal à $(Q'_w)^* + D^*$. À partir de là et de ce qui a été dit précédemment (et notamment du lemme 3.7), il suit, en déroulant les définitions, que l'ensemble $A_{Q_w, g, \ell}$ est égal à $\vec{\rho}_w + D_w + C^*$ comme nous le souhaitons. Il ne reste donc plus qu'à démontrer que Q_w contient Q .

3.2.2 Intermède : la permutation des perdants

On constate sur l'exemple de la figure 3 que si l'on retire la ligne du haut du damier triangulaire, et que l'on soustrait 1 à tous les nombres restants, on obtient une numérotation qui correspond à une nouvelle permutation w' , qui est ici égale à $(2\ 3\ 4\ 1)$. Dans ce paragraphe, nous montrons que cela est vrai de façon générale et expliquons comment obtenir la permutation w' à partir de w .

Définition 3.8. Soit w une permutation de l'ensemble $\{1, \dots, d\}$.

Un *record* de w est un entier $w(i)$ tel que $w(j) < w(i)$ pour tout $j < i$. Si $w(i)$ est un record de w , on dit qu'il apparaît en *position* i .

La *permutation des perdants* de w est la permutation w' de $\{1, \dots, d-1\}$ définie par récurrence en décrétant que $w'(i)$ est le plus petit élément de l'ensemble différence

$$\{w(1), w(2), \dots, w(i+1)\} \setminus \{w'(1), \dots, w'(i-1)\}. \quad (3.7)$$

La notion de record est maintenant classique : elle a déjà été introduite il y a de nombreuses années dans [13] et a depuis fait l'objet de multiples études, notamment en ce qui concerne leur distribution asymptotique. Par contre, l'auteur n'a pas réussi à trouver une trace antérieure de la permutation des perdants.

On montre immédiatement par récurrence que l'ensemble (3.7) est toujours de cardinal 2 (*i.e.* que l'ensemble que l'on ôte est toujours inclus dans le premier), et plus précisément qu'il contient exactement l'élément $w(i+1)$, et le dernier record de w apparaissant avant i . Ainsi si $w(i+1)$ n'est pas un record de w , on a $w'(i) = w(i+1)$, tandis que dans le cas contraire, $w'(i)$ est le record précédent de w . Dans le cas de la permutation $w = (3\ 2\ 4\ 5\ 1)$ que nous avons déjà considéré, on voit que les records de w sont les entiers 3, 4 et 5 et que la permutation des perdants de w est $w' = (2\ 3\ 4\ 1)$.

On peut donner une reformulation moins mathématique des définitions précédentes qui donne tout son sens à la terminologie. Il faut pour cela imaginer que les entiers de 1 à d sont des candidats qui prennent part à une compétition, dans l'ordre indiqué par la permutation w : si l'on reprend notre exemple, cela signifie que 3 joue d'abord, 2 juste après, *etc.* En outre un candidat est d'autant plus fort au jeu que l'entier qui lui est attaché est grand. Les records correspondent alors aux records au sens usuel : l'entier 3 joue en premier, et donc décroche le record (il n'a pas grand mérite, mais peu importe) ; ensuite vient le tour de l'entier 2 dont la performance est moins bonne, il n'a donc pas le record ; ensuite, joue 4 qui fait un nouveau record ; puis 5 qui bat encore le record ; et enfin 1 qui n'améliore certainement pas le record. Les records successifs sont donc bien 3, 4 et 5.

La permutation des perdants, quand à elle, s'interprète comme suit. Il faut imaginer qu'au fur et à mesure que la compétition se déroule, on met à jour une liste des perdants. Au premier tour, l'entier 3 joue et il n'y

a pour l'instant aucun perdant ; on écrit donc rien sur notre liste. Ensuite, c'est au tour de l'entier 2 de jouer ; celui-ci fait un moins bon résultat et se retrouve ainsi être le premier perdant. C'est maintenant 4 qui s'élançe, et il subtilise le record à 3 ; l'entier 3 devient comme ceci un perdant et on l'inscrit sur la liste en dessous de 2. C'est ensuite 5 qui joue et qui, par sa performance exceptionnelle, envoie 4 (qui détenait jusqu'à présent le record) rejoindre la liste des perdants. C'est enfin autour de 1 qui, par sa médiocrité, s'en va tout de suite compléter la liste des perdants. La liste des perdants — ou la permutation des perdants pour reprendre la terminologie mathématique — est donc dans l'ordre 2, 3, 4 puis 1.

Dans la suite, et notamment lors des démonstrations, nous continuerons d'employer la terminologie imagée issue de la métaphore de la compétition que nous venons d'expliquer.

Lemme 3.9. Soient $w \in \mathfrak{S}_d$ et w' sa permutation des perdants. Soit $\text{ord}_{w'} : I' \rightarrow \{1, \dots, d-1\}$ (avec $I' = \{(i, j) \in \mathbb{N}^2 \mid 1 \leq i \leq j \leq d-1\}$) la fonction associée à w' . Alors $\text{ord}_{w'}(i, j) = \text{ord}_w(i+1, j+1) - 1$.

Démonstration. On raisonne sur la représentation de la fonction ord_w sous forme de tableau triangulaire (voir figure 3). Il s'agit alors de montrer qu'un entier $i \geq 2$ apparaît exactement $w(i) - w'(i-1)$ fois sur la première ligne. Si $w(i)$ n'est pas un record, alors manifestement i n'apparaît pas sur la première ligne et on a déjà dit qu'alors $w(i) = w'(i-1)$. Dans ce cas, on a donc bien ce que l'on voulait. Si, au contraire, $w(i)$ est un record, notons $w(j)$ le record de w qui apparaît juste avant i , i.e. $w(j) = \max\{w(1), \dots, w(i-1)\}$. Alors $w'(i-1) = w(j)$ et l'entier i apparaît $w(i) - w(j)$ sur la première ligne du tableau. On a donc, à nouveau, bien vérifié ce que l'on avait annoncé. \square

3.2.3 La fin de la démonstration

On en revient à la démonstration de la proposition 3.6. Comme nous le disons, il suffit de montrer que $Q_w \subset Q$ pour toute permutation $w \in \mathfrak{S}_d$. On fixe à partir de maintenant $w \in \mathfrak{S}_d$ et un élément $q = (q_{i,j}) \in Q_w$. On note également $\mu_{i,j}$ les nombres réels définis par la formule (1.7). Par hypothèse $\mu_{1,j} \geq \mu_{2,j} \geq \dots \geq \mu_{d,j}$ et, en examinant la définition de Q'_w , on prouve qu'il existe des réels $q_1 \leq q_2 \leq \dots \leq q_d$ tels que $q_{i,j} = q_{\text{ord}_w(i,j)}$. Nous voulons montrer que $q \in Q$, ce qui signifie les inégalités $\mu_{i,j} \leq \mu_{i+1,j}$ et $\mu_{i,j} \geq \mu_{i+1,j+1}$ sont satisfaites pour tout (i, j) pour lequel cela a un sens. La première étape consiste à exprimer les $\mu_{i,j}$ en fonction des q_i . Pour cela, considérons w_1, \dots, w_d les permutations définies par récurrence en convenant que $w_1 = w$ et que w_{i+1} est la permutation des perdants de w_i . Notons que w_i est une permutation de l'ensemble $\{1, \dots, d+1-i\}$. Définissons encore les permutations $w_i^\vee \in \mathfrak{S}_{d+1-i}$ par $w_i^\vee(j) = w_i^{-1}(d+2-i-j)$ où w_i^{-1} désigne bien sûr la permutation inverse de w_i .

Lemme 3.10. Avec les notations précédentes, on a pour tout couple $(i, j) \in I$:

$$\mu_{i,j} = bq_{w_i^\vee(j-i+1)+i-1} - q_j.$$

Démonstration. D'après le lemme 3.9 et les expressions donnant les valeurs de $\mu_{i,j}$, il suffit de démontrer le lemme lorsque $i = 1$, la formule s'écrivant alors simplement $\mu_{1,j} = bq_{w_1^\vee(j)} - q_j$. Par définition, on a :

$$\begin{aligned} \mu_{1,j} &= -q_{j,d} + b \cdot \sum_{i=1}^j q_{i,j} - b \cdot \sum_{i=0}^{j-1} q_{i,j-1} \\ &= -q_{\text{ord}_w(j,d)} + b \cdot \sum_{i=1}^j q_{\text{ord}_w(i,j)} - b \cdot \sum_{i=0}^{j-1} q_{\text{ord}_w(i,j-1)}. \end{aligned}$$

Or, si l'on se souvient de l'interprétation que nous avons donnée de la fonction ord_w en termes de remplissage de tableau, il est clair que $\text{ord}_w(j, d) = j$ et que l'ensemble $\{\text{ord}_w(1, j), \dots, \text{ord}_w(j, j)\}$ consiste en les entiers s tels que $w(s) \geq d+1-j$. Ainsi, trouve-t-on :

$$\{\text{ord}_w(1, j), \dots, \text{ord}_w(j, j)\} = \{\text{ord}_w(1, j-1), \dots, \text{ord}_w(j-1, j-1)\} \cup \{w_1^\vee(j)\}$$

et la formule du lemme en découle. \square

Montrons à présent que $\mu_{1,j} \leq \mu_{2,j}$ pour tout indice $j \in \{2, \dots, d\}$. Par définition de w_2^\vee , on a $w_2 \circ w_2^\vee(j-1) = d+1-j$; autrement dit, l'entier $d+1-j$ apparaît en position $w_2^\vee(j-1)$ dans la permutation

des perdants de w . Il a donc forcément joué avant le tour $w_2^\vee(j-1) + 1$, ce qui se traduit mathématiquement par l'inégalité $w_1^\vee(j) \leq w_2^\vee(j-1) + 1$. Ainsi, grâce au lemme 3.10, on obtient :

$$\mu_{1,j} = bq_{w_1^\vee(j)} - q_j \leq bq_{w_2^\vee(j-1)+1} - q_j = \mu_{2,j}$$

ce qui est bien ce que l'on désire. La démonstration de l'inégalité $\mu_{1,j} \geq \mu_{2,j+1}$ suit une idée analogue. Remarquons d'abord que, d'après le lemme 3.10, la différence entre les deux nombres à comparer s'exprime comme suit :

$$\mu_{1,j} - \mu_{2,j+1} = b(q_{w_1^\vee(j)} - q_{w_2^\vee(j)+1}) + q_{j+1} - q_j.$$

Comme $q_{j+1} \geq q_j$, l'égalité que l'on souhaite démontrer est trivialement satisfaite si $q_{w_1^\vee(j)} \geq q_{w_2^\vee(j)+1}$ et donc dès que $w_1^\vee(j) > w_2^\vee(j)$. On suppose donc à partir de maintenant que $w_1^\vee(j) \leq w_2^\vee(j)$. Posons $i_1 = w_1^\vee(j)$ et $i_2 = w_2^\vee(j)$; on a alors $w_1(i_1) = d + 1 - j$ et $w_2(i_2) = d - j$. Selon la permutation w , l'entier $d - j$ a donc forcément joué avant le temps $i_2 + 1$. Par ailleurs, il n'a pas pu jouer avant le temps i_1 car sinon, il aurait été battu par $d + 1 - j$ au temps i_1 et donc aurait au pire rejoint la liste des perdants en position $i_1 - 1$. De même, il n'a pas pu jouer en i_1 car c'était alors le tour de $d + 1 - j$, ni entre les temps $i_1 + 1$ et i_2 car il aurait été alors perdant tout de suite (étant donné que $d + 1 - i$ aurait déjà fait une meilleure performance avant). On en déduit que $d - j$ a joué au temps $i_2 + 1$, c'est-à-dire que $w(i_2 + 1) = d - j$, soit encore $w_1^\vee(j + 1) = i_2 + 1 = w_2^\vee(j) + 1$. En appliquant le lemme 3.10, on obtient

$$\mu_{1,j+1} = bq_{w_1^\vee(j+1)} - q_{j+1} = bq_{w_2^\vee(j)+1} - q_{j+1} = \mu_{2,j+1}$$

et la conclusion résulte alors de l'hypothèse $\mu_{1,j} \geq \mu_{1,j+1}$.

À présent, des deux égalités que l'on vient de prouver, il suit $\mu_{2,j} \geq \mu_{1,j} \geq \mu_{2,j+1}$ pour tout $j \in \{2, \dots, d-1\}$. On peut donc réitérer l'argumentation précédente en décalant les indices (ou, si l'on préfère, appliquer ce que l'on vient de démontrer à la permutation w') afin d'obtenir les inégalités $\mu_{2,j} \leq \mu_{3,j}$ pour $3 \leq j \leq d$, et $\mu_{2,j} \geq \mu_{3,j+1}$ pour $2 \leq j \leq d-1$. En continuant ainsi, on démontre bien au final ce que l'on voulait.

3.3 Démonstration des théorèmes 2, 4 et 5

3.3.1 Le cas des variétés \mathcal{X}_μ

Commençons par démontrer le théorème 4. Considérons un d -uplet $\mu = (\mu_1, \dots, \mu_d)$ où les μ_i sont des nombres entiers vérifiant $\mu_1 \geq \dots \geq \mu_d$. En passant au déterminant, on démontre tout de suite que si $b-1$ ne divise pas $\mu_1 + \dots + \mu_d$, la variété \mathcal{X}_μ est vide. On suppose désormais que $\mu_1 + \dots + \mu_d$ est un multiple de $b-1$. On a

$$\dim_k \mathcal{X}_\mu = \max \dim_k \mathcal{X}_\varphi$$

où le maximum est pris sur tous les $\varphi \in \Phi_Z$ tels que $\mu_{1,i}(\varphi) = \mu_i$ pour tout i . Les congruences énoncées sont donc une conséquence immédiate du corollaire 1.16 et du théorème 1.17. Pour le reste, rappelons que l'on se restreint au cas où σ n'est pas l'identité. On a donc $\dim_k \mathcal{X}_\mu = b'_{Q,R,g,\ell,0}(\mu)$, et, en vertu de la proposition 2.3, on est amené à justifier les deux assertions suivantes :

- l'image de $R \cap Q_{\mathbb{R}}$ par la fonction g contient l'ensemble des d -uplets (y_1, \dots, y_d) tels que $b-1$ divise $y_1 + \dots + y_d$;
- le nombre $b'_{Q,R,g,\ell,0}(\mu) = a_{Q,g,\ell}(\mu)$ est égal au minimum qui apparaît dans l'énoncé du théorème 4.

Commençons par la première. Rappelons que $Q_{\mathbb{R}}$ est défini comme le \mathbb{R} -espace vectoriel engendré par Q . Dans notre cas, il est facile de construire un élément $q = (q_{i,j})$ telle que toutes les inégalités des jeux I, II et III définissant Q soient strictes; on pourra pour cela s'inspirer de l'exemple de la figure 1. Un tel point est dans l'intérieur de Q , ce qui assure que Q est d'intérieur non vide et donc que $Q_{\mathbb{R}} = E$. Si l'on note $\vec{v}_1, \dots, \vec{v}_d$ la base canonique de \mathbb{R}^d , un calcul facile montre que, étant donné un entier s compris entre 1 et d , l'image par g de l'élément $(q_{i,j}) \in R$ défini par $q_{i,j} = \delta_{(i,j),(s,d)}$ (δ étant le symbole de Kronecker) est $\vec{w}_s = b\vec{v}_d - \vec{v}_s$. En outre, un vecteur y de coordonnées (y_1, \dots, y_d) se décompose sur la familles de \vec{w}_s comme suit :

$$y = \frac{b}{b-1} \cdot (y_1 + \dots + y_d) \cdot \vec{w}_d - (y_1 \vec{w}_1 + \dots + y_d \vec{w}_d).$$

Ainsi on trouve bien que y appartient à $g(R) = g(R \cap Q_{\mathbb{R}})$ dès que $b-1$ divise la somme de ses coordonnées $y_1 + \dots + y_d$.

On en vient maintenant à la seconde assertion. Comme l'on ne considère que des éléments μ dans C , on a $a_{Q,g,\ell}(\mu) = b_{Q,g,\ell,0,C}(\mu)$ et de même $a_{Q_{\max},g,\ell}(\mu) = b_{Q_{\max},g,\ell,0,C}(\mu)$. D'après la proposition 2.2 et la description des points extrémaux de $A_{Q_{\max},g,\ell}$ donnée par la proposition 3.1, il suffit de montrer que $B_{Q,g,\ell,0,C} = B_{Q_{\max},g,\ell,0,C}$, i.e. $A_{Q,g,\ell} + C^* = A_{Q_{\max},g,\ell} + C^*$, ce qui suit de la proposition 3.6.

Remarque 3.11. Bien entendu, $a_{Q,g,\ell}(\mu)$ s'écrit aussi comme le minimum des produits scalaires $\langle \alpha | \mu \rangle_d$ où α décrit l'ensemble des points extrémaux de $A_{Q,g,\ell}$. Cela signifie que le théorème 4 reste vrai si l'on se contente de prendre le minimum sur le sous-ensemble (strict) \mathcal{S}_d de \mathfrak{S}_d , qui est défini au début du §3.2. En d'autres termes, les permutations qui n'appartiennent pas à \mathcal{S}_d ne contribuent jamais (i.e. pour aucun $\mu \in C$) au minimum.

Il reste enfin encore à démontrer que lorsque μ est b -régulier, alors le minimum des produits scalaires $\langle \vec{\rho}_w | \mu \rangle_d$ (pour w décrivant \mathfrak{S}_d) est atteint lorsque $w = w_0 : i \mapsto d + 1 - i$, et qu'il vaut alors $\frac{1}{b+1} \cdot \langle 2\vec{\rho} | \mu \rangle_d$ (on rappelle que $\vec{\rho}$ est défini par $\vec{\rho} = (\frac{d-1}{2}, \frac{d-3}{2}, \dots, \frac{1-d}{2}) \in \mathbb{R}^d$). Notons pour cela Reg le sous-ensemble de \mathbb{R}^d formé des éléments $\mu = (\mu_1, \dots, \mu_d)$ qui sont b -réguliers ; il s'agit d'un cône convexe dont on note Reg^* le cône dual. Avec la proposition 2.2, on voit aisément qu'il suffit de démontrer le lemme suivant.

Lemme 3.12. *Soit w_0 la permutation $i \mapsto d + 1 - i$. On a l'égalité :*

$$A_{Q_{w_0},g,\ell} = \frac{2\vec{\rho}}{b+1} + \text{Reg}^*.$$

Remarque 3.13. On notera, à juste titre, que Q_{w_0} n'est autre que l'ensemble Q_{\min} que nous avons déjà rencontré et utilisé.

Démonstration. Pour $i \in \{1, \dots, d-1\}$, notons $\vec{v}_i \in \mathbb{R}^d$ le vecteur $\vec{v}_i = (0, \dots, 0, 1, -1, 0, \dots, 0)$ où le 1 est en i -ème position. Ces vecteurs forment une base de l'hyperplan « somme des coordonnées égale 0 », noté H . D'après la définition des points b -réguliers, le cône dual Reg^* est le cône convexe engendré par les vecteurs $\vec{w}_i = b\vec{v}_{d-i} - \vec{v}_i$ pour $1 \leq i \leq d-1$. Par ailleurs, le système (3.3) nous dit qu'un élément $y = (y_1, \dots, y_d) \in \mathbb{R}^d$ appartient à $A_{Q_{w_0},g,\ell}$ si, et seulement si

$$\begin{cases} y_1 + y_2 + \dots + y_d = 0 \\ (y_1 + \dots + y_s) - b(y_{d+1-s} + \dots + y_d) \geq s(d-s), \quad \forall s \in \{1, \dots, d-1\}. \end{cases}$$

Comme le vecteur $\frac{2\vec{\rho}}{b+1}$ n'est autre que l'intersection de ces d hyperplans (vérification immédiate), le convexe $-\frac{2\vec{\rho}}{b+1} + A_{Q_{w_0},g,\ell}$ est le cône défini dans H par les inégalités $(y_1 + \dots + y_s) - b(y_{d+1-s} + \dots + y_d) \geq 0$ pour $s \in \{1, \dots, d-1\}$. Pour conclure, il suffit de montrer que ce cône est engendré par les vecteurs \vec{w}_i . Or, il est engendré par les intersections $(d-2)$ à $(d-2)$ des $(d-1)$ hyperplans (de H) frontière des demi-espaces précédents. Un calcul direct montre enfin que ces intersections sont exactement les vecteurs \vec{w}_i , ce qui conclut. \square

3.3.2 Le cas des variétés $\mathcal{X}_{\leq \mu}$

Nous en venons maintenant aux variétés $\mathcal{X}_{\leq \mu}$, c'est-à-dire à la démonstration du théorème 5. Pour ce faire, nous suivons à nouveau la même méthode : nous donnons une description de l'ensemble convexe B_{Q,g,ℓ,C^*} , à partir de laquelle nous déduisons une formule pour la fonction b_{Q,g,ℓ,C^*} d'où résultera le théorème.

Le calcul de $A_{Q,g,\ell} \cap C$ Le lemme 3.12 donne une description explicite de l'ensemble $A_{Q_{w_0},g,\ell} = A_{Q_{\min},g,\ell}$. Dans ce paragraphe, nous nous proposons de démontrer qu'il s'en déduit une autre description simple de l'intersection $A_{Q,g,\ell} \cap C$, au moins si b est suffisamment grand. Plus précisément, nous allons démontrer que, si $b \geq 1 + \frac{d^2}{4}$, on a :

$$A_{Q,g,\ell} \cap C = A_{Q_{\min},g,\ell} \cap C = \left(\frac{2\vec{\rho}}{b+1} + \text{Reg}^* \right) \cap C \quad (3.8)$$

D'après la proposition 3.6 (en fait, seule l'inclusion facile sert), il suffit d'établir l'égalité $(A_{Q_{\max},g,\ell} + C^*) \cap C = A_{Q_{\min},g,\ell} \cap C$. Nous commençons par un lemme concernant les points extrémaux de $A_{Q_{\max},g,\ell}$.

Lemme 3.14. On suppose $b \geq 1 + \frac{d^2}{4}$. Alors le seul point extrémal de $A_{Q_{\max},g,\ell}$ qui appartient à C est $\frac{2\vec{\rho}}{b+1}$.

Démonstration. Comme on a supposé $b \geq 1 + \frac{d^2}{4}$, la proposition 3.1 s'applique et les points extrémaux de $A_{Q_{\max},g,\ell}$ sont de la forme $\vec{\rho}_w$. On est ainsi ramené à montrer que le vecteur $\vec{\rho}_w$ n'appartient pas à C dès que w n'est pas la permutation $i \mapsto d+1-i$. Or, par définition de C et d'après la formule donnant les coordonnées de $\vec{\rho}_w$, le fait que $\vec{\rho}_w$ soit élément de C implique que pour tout $i \in \{1, \dots, d-1\}$, l'égalité suivante est satisfaite :

$$\sum_{n=1}^{\infty} \frac{w^n(i+1) - w^n(i) + 1}{b^n} \geq 0.$$

Du fait que $b \geq 1 + \frac{d^2}{4}$, ceci implique que le premier terme de la somme (i.e. pour $n=1$) est lui-même positif ou nul. Ainsi, obtient-on $w(i+1) \geq w(i) - 1$ pour tout indice $i \in \{1, \dots, d-1\}$. Il est alors clair que w ne peut être que la permutation $i \mapsto d+1-i$. \square

Lemme 3.15. Soit $y = (y_1, \dots, y_d)$ un élément de $A_{Q_{\min},g,\ell}$ tel que $y_i \leq y_{i+1} + 1$ pour tout $i \in \{1, \dots, d-1\}$. Alors $y \in A_{Q_{\max},g,\ell}$.

Démonstration. D'après la description de $A_{Q_{\max},g,\ell}$ donnée par le système (3.1), il s'agit de montrer que $f_T(y) \geq 0$ pour toute partie T de $\{1, \dots, d\}$. Soit T une telle partie. Si on note $t_1 < \dots < t_s$ ses éléments (avec, donc, $s = \text{Card } T$), l'inégalité $f_T(y) \geq 0$ devient

$$y_1 + \dots + y_s - b \cdot \sum_{i=1}^s y_{d+1-t_i} \geq s(d-s) - b \cdot \sum_{i=1}^s (t_i - i). \quad (3.9)$$

Par ailleurs, comme y est pris dans $A_{Q_{\min},g,\ell}$, on a

$$y_1 + \dots + y_s - b \cdot \sum_{i=1}^s y_{d+1-t_i} \geq s(d-s) + b \cdot \sum_{i=1}^s (y_{d+1-i} - y_{d+1-t_i}).$$

Or, on a $t_i \geq i$ pour tout i d'où, d'après notre hypothèse, on tire $y_{d+1-i} - y_{d+1-t_i} \leq t_i - i$. L'inégalité (3.9) s'ensuit. \square

On peut à présent démontrer l'égalité (3.8) lorsque $b \geq 1 + \frac{d^2}{4}$. Il suffit, comme nous l'avons expliqué, de montrer que le polytope $P_1 = A_{Q_{\min},g,\ell} \cap C$ est inclus dans le polytope $P_2 = (A_{Q_{\max},g,\ell} + C^*) \cap C$ et, pour cela, il est suffisant de prouver que tous les sommets de P_1 (en incluant ceux à l'infini) sont dans P_2 . On vérifie tout de suite que $\text{Reg} \subset C^*$; ainsi $C \subset \text{Reg}^*$ et la description donnée par le lemme 3.12 implique $A_{Q_{\max},g,\ell} + C = A_{Q_{\max},g,\ell}$ et finalement $P_1 + C = P_1$. Comme en plus $P_1 \subset C$, on en déduit que les sommets à l'infini de P_1 sont ceux de C . Mais du fait que $C \subset C^*$ (vérification facile), il suit que $P_2 + C = P_2$. Ainsi les sommets à l'infini de C sont bien dans P_2 .

Il reste donc à traiter le cas des sommets de P_1 à distance fini, c'est-à-dire des points extrémaux de P_1 . Notons F_1, \dots, F_{d-1} les facettes de $A_{Q_{\min},g,\ell}$; ce sont des cônes simpliciaux de dimension $d-2$ issus de $\frac{2\vec{\rho}}{b+1}$. Le lemme 3.15 assure que les convexes $A_{Q_{\max},g,\ell} + C^*$ et $A_{Q_{\min},g,\ell}$ sont égaux sur un voisinage de $\frac{2\vec{\rho}}{b+1}$. On en déduit que $A_{Q_{\max},g,\ell} + C^*$ a exactement $d-1$ facettes issues de $\frac{2\vec{\rho}}{b+1}$ et que l'on peut numéroter celles-ci F'_1, \dots, F'_{d-1} de sorte que $F'_i \subset F_i$ pour tout i . Pour chaque i , les sommets de F'_i à distance finie sont des points extrémaux de $A_{Q_{\max},g,\ell} + C^*$ et donc *a fortiori* des points extrémaux de $A_{Q_{\max},g,\ell}$. En particulier, d'après la proposition 3.1, ceux-ci ne sont pas dans C . Les sommets à l'infini, quant à eux, correspondent aux directions de Reg^* , c'est-à-dire aux vecteurs \vec{w}_i introduits dans la démonstration du lemme 3.12. Comme aucun des \vec{w}_i , ni de leurs opposés, n'est dans C , on en déduit finalement que $F_i \cap C = F'_i \cap C$.

Il est maintenant facile de conclure : tout point extrémal de $P_1 = A_{Q_{\min},g,\ell} \cap C$ appartient à l'une des faces F_i et bien sûr également à C . Il appartient donc à la face F'_i correspondante, et par suite à $A_{Q_{\max},g,\ell} + C^*$ puis à P_2 .

Obtention de la majoration On sait que la dimension de la variété $\mathcal{X}_{\leq \mu}$ est majorée par la quantité $b_{Q,g,\ell,C^*}(\mu)$ qui d'après la proposition 2.2 vaut $\inf_{\alpha \in B_{Q,g,\ell,C^*}} \langle \alpha | \mu \rangle_E$ où, on rappelle que $B_{Q,g,\ell,C^*} = A_{Q,g,\ell} \cap C$. Pour démontrer la première majoration :

$$\dim_k \mathcal{X}_{\leq \mu} \leq \frac{\langle 2\vec{\rho} | \mu \rangle_d}{b+1}$$

il suffit donc de prouver que le vecteur $\frac{2\vec{\rho}}{b+1}$ est dans B_{Q,g,ℓ,C^*} . Il est déjà évident qu'il appartient à C . De plus, le lemme 3.12 montre qu'il appartient à $A_{Q_{\min},g,\ell}$, d'où il suit, grâce au lemme 3.15, qu'il est aussi dans $A_{Q_{\max},g,\ell}$ et donc *a fortiori* dans $A_{Q,g,\ell}$. Passons à présent à la deuxième majoration du théorème : on suppose $b \geq 1 + \frac{d^2}{4}$ et on veut montrer

$$\dim_k \mathcal{X}_{\leq \mu} \leq \sup_{\substack{\mu' \leq \mu \\ \mu' \in \text{Reg}}} \frac{\langle 2\vec{\rho} | \mu' \rangle_d}{b+1}. \quad (3.10)$$

Si l'on définit la forme linéaire $L : \mathbb{R}^d \rightarrow \mathbb{R}$, $\mu \mapsto \frac{1}{b+1} \cdot \langle 2\vec{\rho} | \mu \rangle_d$, on remarque que le majorant dans (3.10) n'est autre que $b_{\text{Reg},\text{id},L,C^*}(\mu)$. Pour terminer la preuve, il suffit donc de montrer que $b_{\text{Reg},\text{id},L,C^*} = b_{Q,g,\ell,C^*}$. Or, en déroulant les définitions, on trouve $A_{\text{Reg},\text{id},L} = \frac{2\vec{\rho}}{b+1} + \text{Reg}^*$ et donc $A_{\text{Reg},\text{id},L} = A_{Q_{\min},g,\ell}$ d'après le lemme 3.12. L'égalité (3.8) implique alors $A_{\text{Reg},\text{id},L} \cap C = A_{Q,g,\ell} \cap C$ à partir de quoi la proposition 2.2 permet de conclure.

Obtention de la minoration Il ne reste plus qu'à démontrer la minoration. Étant donné que si $\mu' \leq \mu$, on a tautologiquement $\mathcal{X}_{\leq \mu'} \subset \mathcal{X}_{\leq \mu}$ et donc $\dim_k \mathcal{X}_{\leq \mu'} \leq \dim_k \mathcal{X}_{\leq \mu}$, il suffit de montrer que si $\mu = (\mu_1, \dots, \mu_d)$ est fortement intégralement b -régulier, alors :

$$\dim_k \mathcal{X}_{\leq \mu} \geq \frac{\langle 2\vec{\rho} | \mu \rangle_d}{b+1} - (d-1)^2 - \frac{(d-2)^2}{4}.$$

Pour cela, il suffit de trouver un élément $q \in Q \cap R$ tel que $g(q) \in \mu - C^*$ et $\ell(q) \geq \frac{\langle 2\vec{\rho} | \mu \rangle_d}{b+1} - (d-1)^2 - \frac{(d-2)^2}{4}$. Posons, pour tout i , $q'_i = \frac{\mu_i + b\mu_{d+1-i}}{b^2-1}$. La condition de divisibilité qui apparaît dans la définition d'un d -uplet fortement intégralement b -régulier assure que si $q'_1 + \dots + q'_d$ est un entier alors que les conditions d'inégalité se traduisent par $q'_1 \leq q'_2 \leq \dots \leq q'_{d-1} \leq q'_d - d$. Pour $i < d$, notons q_i la partie entière supérieure de q'_i (i.e. le plus petit entier plus grand ou égal à q'_i) et définissons q_d de sorte que $q_1 + \dots + q_d = q'_1 + \dots + q'_d$. Tous les q_i sont alors des entiers, et on vérifie directement que la suite qu'ils forment est croissante. Ainsi le vecteur q de coordonnées $q_{i,j} = q_{d-j+i}$ (pour $(i,j) \in I$) appartient à Q . En outre, un calcul immédiat montre que pour tout s , on a :

$$\begin{aligned} \langle \vec{\mu}_1 + \dots + \vec{\mu}_s | q \rangle_E &= b(q_d + \dots + q_{d+1-s}) - (q_1 + \dots + q_s) \\ &= -b(q_1 + \dots + q_{d-s}) - (q_1 + \dots + q_s) \\ &\leq -b(q'_1 + \dots + q'_{d-s}) - (q'_1 + \dots + q'_s) \\ &= b(q'_d + \dots + q'_{d+1-s}) - (q'_1 + \dots + q'_s) = \mu_1 + \dots + \mu_s \end{aligned}$$

et l'égalité est atteinte lorsque $s = d$. Autrement dit, on a bien $g(q) \in \mu - C^*$. Il reste à minorer $\ell(q)$:

$$\ell(q) = \langle \vec{\delta} | q \rangle_d = \sum_{i=1}^d (2i - d - 1)q_i = \frac{\langle 2\vec{\rho} | \mu \rangle_d}{b+1} + \sum_{i=1}^d (2i - d - 1)(q_i - q'_i).$$

Or $q_d - q'_d$ est compris entre $1 - d$ et 0 , tandis que les $q_i - q'_i$ pour $i < d$ sont compris entre 0 et 1 . On en déduit que :

$$\ell(q) \geq \frac{\langle 2\vec{\rho} | \mu \rangle_d}{b+1} - (d-1)^2 - \sum_{i=2}^d \max(2i - d - 1, 0) \geq \frac{\langle 2\vec{\rho} | \mu \rangle_d}{b+1} - (d-1)^2 - \frac{(d-2)^2}{4}.$$

3.3.3 Le cas des variétés $\mathcal{X}_{\leq e}$

Rappelons que nous avons déjà démontré la majoration du théorème 2 lorsque $b \geq d - 1$ dans le §2.3. En utilisant le théorème 5 que nous venons de démontrer, nous complétons ici cette démonstration. Comme d'habitude, on suppose que σ n'est pas l'identité, le cas contraire s'obtenant pareillement en ajoutant $\frac{d(d-1)}{2}$ à tous les majorants.

Preuve de la majoration Soit e un nombre entier. La variété $\mathcal{X}_{\leq e}$ s'écrit manifestement comme l'union disjointe des variétés $\mathcal{X}_{\leq \mu}$ pour $\mu = (\mu_1 \geq \dots \geq \mu_d)$ vérifiant $\mu_1 \leq e$ et $\mu_d \geq 0$. Il suffit donc de démontrer que, si μ est tel qu'on vient de le décrire, la dimension de $\mathcal{X}_{\leq \mu}$ est majorée par $\left\lfloor \frac{d^2}{4} \right\rfloor \cdot \frac{e}{b+1}$. Or, par le théorème 5, on sait que cette dimension est majorée par $\frac{1}{b+1} \cdot \langle 2\vec{\rho} | \mu \rangle_d$ et on a

$$\frac{\langle 2\vec{\rho} | \mu \rangle_d}{b+1} = \sum_{i=1}^d \frac{d+1-i}{b+1} \cdot \mu_i \leq e \cdot \sum_{i=1}^{\lfloor d/2 \rfloor} \frac{d+1-i}{b+1} = \left\lfloor \frac{d^2}{4} \right\rfloor \cdot \frac{e}{b+1}.$$

La conclusion en résulte.

Preuve de la minoration Pour obtenir la minoration, nous devons estimer la quantité $b'_{Q,R,f,\ell,C}(e,0)^6$. Or, il est évident par définition que si $q \in Q \cap R$ vérifie $f(q) \in (e,0) + C$, cette quantité est minorée par $\ell(q)$. Il suffit donc, pour terminer la démonstration du théorème 2, de construire un élément $q = (q_{i,j}) \in Q \cap R$ tel que :

$$f(q) \in (e,0) + C \quad \text{et} \quad \ell(q) = \left\lfloor \frac{d^2}{4} \right\rfloor \cdot \left\lfloor \frac{e-b+2}{b+1} \right\rfloor.$$

C'est ce que nous allons faire de façon explicite. Posons $n = \left\lfloor \frac{e-b+2}{b+1} \right\rfloor$ et définissons m comme le reste de la division euclidienne de $(-n)$ par $b-1$. On considère l'élément q défini comme suit :

$$\begin{aligned} q_{i,j} &= \frac{m+bn}{b-1} & \text{si } 0 \leq j-i < \frac{d}{2} \\ q_{i,j} &= \frac{m+n}{b-1} & \text{si } j-i \geq \frac{d}{2}. \end{aligned}$$

Il est clair que $\frac{m+bn}{b-1} \geq \frac{m+n}{b-1}$. À partir de là et du fait que la valeur de $q_{i,j}$ ne dépend que de la différence $j-i$, il résulte que q appartient à Q_{\min} , et donc *a fortiori* à Q . Comme, par ailleurs, il suit de la définition de m que tous les $q_{i,j}$ sont entiers, on a bien $q \in Q \cap R$. D'autre part, un calcul direct donne $\langle \vec{\mu}_1 | q \rangle_E = m+n(b+1) \leq b-2+e-b+2 = e$ et $\langle \vec{\mu}_d | q \rangle_E = m \geq 0$, d'où il suit $f(q) \in (e,0) + C$. Finalement, à nouveau un calcul facile conduit à la valeur souhaitée pour $\ell(q) = \langle \vec{\delta} | q \rangle_E$.

3.4 Points extrémaux de $A_{Q,g,\ell} \cap C$: quelques exemples

Revenons un instant sur la démonstration que nous avons faite de la majoration du théorème 5 : dans un premier temps, nous avons utilisé le théorème 1.17 afin de majorer la dimension de $\mathcal{X}_{\leq \mu}$ par la quantité $b_{Q,g,\ell,C^*}(\mu)$, et ensuite nous avons prouvé l'égalité $b_{Q,g,\ell,C^*}(\mu) = b_{\text{Reg},\text{id},L,C^*}(\mu)$ en montrant que chacun de ces deux nombres s'égalisait avec :

$$M(\mu) = \inf_{\alpha \in K} \langle \alpha | \mu \rangle_d \quad \text{où} \quad K = \left(\frac{2\vec{\rho}}{b+1} + \text{Reg}^* \right) \cap C.$$

Ainsi, l'expression $M(\mu)$ est une nouvelle façon d'exprimer le majorant obtenu. En outre, K est un polytope qui n'a qu'un nombre fini de points extrémaux, et si on appelle Λ leur ensemble, on a :

$$M(\mu) = \inf_{\lambda \in \Lambda} \langle \lambda | \mu \rangle_d$$

pour tout $\mu \in \text{Reg} + C^* = C^*$, c'est-à-dire dès que $\mu_1 \geq \dots \geq \mu_d$ si, comme d'habitude, on appelle μ_i ($1 \leq i \leq d$) les coordonnées de μ .

Déterminer les points extrémaux de K apparaît donc comme une question naturelle et importante. Malheureusement, bien que K soit défini de façon plutôt simple (c'est l'intersection de $2d-2$ demi-espaces affines dans un espace de dimension $d-1$), la combinatoire de ses points extrémaux paraît compliquée. Par exemple, le nombre de ces points semble exploser très rapidement lorsque d augmente. Ces deux dernières impressions se sont forgées à la suite de calculs numériques effectués grâce au logiciel `polymake` [3]. La deuxième ligne du tableau 1 donne, par exemple, le nombre de points extrémaux de K pour diverses valeurs de d avec $b = 10\,000$ (la valeur de b importe peu pour la complexité de l'ensemble des points extrémaux de K comme nous allons l'expliquer ensuite). La croissance est apparemment exponentielle ; on notera qu'elle ne peut, en tout cas, pas être pire car, un point extrémal étant situé à l'intersection de d hyperplans parmi les $2d$ définissant K , leur nombre est trivialement majoré par $\binom{2d-2}{d-1} \leq 4^{d-1}$.

⁶Remarquez que la proposition 2.3 et la discussion qui suit sa démonstration nous dit qu'elle diffère de $b_{Q,f,\ell,C}(e,0)$ d'une quantité bornée. Cependant, pour arriver à la minoration énoncée dans le théorème 2, nous avons besoin d'être plus précis que cela.

| Dimension d | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
|---------------------------------------|---|---|---|----|----|----|-----|-----|-----|
| Nombre de points extrémaux de K | 1 | 3 | 6 | 15 | 33 | 70 | 136 | 347 | 667 |
| Nombre de points extrémaux de $K+C^*$ | 1 | 3 | 5 | 9 | 17 | 31 | 47 | 103 | 163 |

TAB. 1 – Nombre de points extrémaux de K et $K + C^*$ pour $b = 10\,000$

Cependant, les points extrémaux que l'on a trouvé précédemment ne sont pas vraiment tous pertinents pour notre problème, dans un sens que nous allons expliquer maintenant. La remarque essentielle est que l'on ne s'intéresse aux variétés $\mathcal{X}_{\leq \mu}$ que lorsque les coordonnées de μ sont triés par ordre décroissant⁷, c'est-à-dire lorsque $\mu \in C$. Ainsi, au lieu de considérer la fonction b_{Q,f,ℓ,C^*} , on peut plutôt travailler avec $b_{Q,f,\ell,C^*,C}$ qui, rappelons-le, est définie par :

$$\begin{aligned} b_{Q,g,\ell,C^*,C}(y) &= b_{Q,g,\ell,C^*}(y) && \text{si } y \in C \\ &= -\infty && \text{sinon.} \end{aligned}$$

Par la proposition 2.2, on a

$$M'(\mu) = \inf_{\alpha \in K'} \langle \alpha | \mu \rangle_d \quad \text{où } K' = K + C^*$$

Ainsi, plutôt que décrire les points extrémaux de K , on a plutôt envie de comprendre ceux de $K + C^*$ qui forment un sous-ensemble (en général strict) des points extrémaux de K . Si l'on reprend les exemples précédents ($b = 10\,000$, d petit), on constate sur le tableau 1, que l'on élimine en effet ainsi un bon paquet de points extrémaux, au moins pour les petites valeurs de d .

Nous avons dit précédemment que la dépendance en b est moins délicate à comprendre. En fait, nous avons le théorème suivant.

Théorème 3.16. *Posons, comme précédemment,*

$$K(b) = \left(\frac{2\vec{\rho}}{b+1} + \text{Reg}^* \right) \cap C \quad \text{et} \quad K'(b) = K(b) + C^*$$

et notons $\Lambda(b)$ et $\Lambda'(b)$ l'ensemble des points extrémaux de $K(b)$ et $K'(b)$ respectivement. Alors, pour b suffisamment grand, le cardinal de $\Lambda(b)$ (resp. $\Lambda'(b)$) est constant et les coordonnées de points de cet ensemble s'expriment comme des fractions rationnelles en b .

Démonstration. Le théorème résulte du fait que les méthodes de calcul de points extrémaux de polytopes s'appliquent dans n'importe quel corps ordonné. Ici donc, nous pouvons voir $K(b)$ et $K'(b)$ comme des polytopes définis sur le corps réel $\mathbb{R}(b)$ muni de l'ordre qui fait de b un élément infiniment grand. Ces polytopes ont alors bien sûr un nombre de sommets qui ne dépend pas de b (le cas contraire n'aurait aucun sens) et les coordonnées de ces sommets sont des éléments de $\mathbb{R}(b)$, c'est-à-dire des fractions rationnelles en b . Il reste à justifier que ces expressions redonnent bien les points extrémaux de $K(b)$ et $K'(b)$ lorsque l'on spécialise b en une valeur suffisamment grande. Mais c'est évident car le calcul des sommets faits dans $\mathbb{R}(b)$ est valable dès que b satisfait un certain nombre fini d'inégalités, et donc en particulier dès que b est suffisamment grand. \square

Le tableau 2 montre les fractions rationnelles que l'on obtient pour les petites valeurs de d .

4 Perspectives et conjectures

4.1 Peut-on espérer une formule exacte pour la dimension ?

Si σ n'est pas l'identité, le théorème 1.17 donne une formule exacte pour la dimension des variétés \mathcal{X}_φ . On peut donc raisonnablement penser que, dans ce cas, il est possible d'en déduire une formule exacte pour

⁷En fait, si μ est quelconque, on montre qu'il existe $\mu' = (\mu'_1 \geq \dots \geq \mu'_d)$, facilement explicitable à partir de μ , tel que $\mathcal{X}_{\leq \mu} = \mathcal{X}_{\leq \mu'}$.

| Dimension d | Domaine de validité | Points extrémaux de $K + C^*$ |
|---------------|---------------------|--|
| 2 | $b \geq 2$ | $\frac{2\vec{\rho}}{b+1} = \frac{(1, -1)}{b+1}$ |
| 3 | $b \geq 2$ | $\frac{2\vec{\rho}}{b+1} = \frac{(2, 0, -2)}{b+1}$ $\frac{(-2, -2, 4)}{b+2}$ $\frac{(4, -2, -2)}{b+2}$ |
| 4 | $b \geq 3$ | $\frac{2\vec{\rho}}{b+1} = \frac{(3, 1, -1, -3)}{b+1}$ $\frac{(3, 3, 3, -9)}{b+3}$ $\frac{(9, -3, -3, -3)}{b+3}$ $\frac{(1, -1, -1, 1)}{b-1} + \frac{(4, 0, 0, -4)}{b+1}$ $\frac{(-1, 1, 1, -1)}{b-1} + \frac{(4, 0, 0, -4)}{b+1}$ |
| 5 | $b \geq 6$ | $\frac{2\vec{\rho}}{b+1} = \frac{(4, 2, 0, -2, -4)}{b+1}$ $\frac{(4, 4, 4, 4, -16)}{b+4}$ $\frac{(16, -4, -4, -4, -4)}{b+4}$ $\frac{(3, -2, -2, -2, 3)}{b-1} + \frac{(7, 0, 0, 0, -7)}{b+1}$ $\frac{(-3, 2, 2, 2, -3)}{b-1} + \frac{(7, 0, 0, 0, -7)}{b+1}$ $\frac{(-2, 2, 0, 0, 0)}{b} + \frac{(6, 0, 0, 0, -6)}{b+1}$ $\frac{(0, 0, 0, -2, 2)}{b} + \frac{(6, 0, 0, 0, -6)}{b+1}$ $\frac{(4, 0, 0, 0, -4)}{b+1} + \frac{(0, 2, 2, -4, 0)}{b+2}$ $\frac{(4, 0, 0, 0, -4)}{b+1} + \frac{(0, 4, -2, -2, 0)}{b+2}$ |

TAB. 2 – Coordonnées des points extrémaux de $K + C^*$

la dimension de $\mathcal{X}_{\leq e}$, \mathcal{X}_μ et $\mathcal{X}_{\leq \mu}$. Et de fait, d'ailleurs, on dispose d'une telle formule car on peut toujours écrire (comme nous l'avons déjà fait plusieurs fois) :

$$\dim_k \mathcal{X}_{\leq e} = b'_{Q,R,f,\ell,\mathbb{R}^+ \times \mathbb{R}^-}(0, e) = \sup_{\substack{q \in Q \cap R \\ f(q) \in (e,0) - (\mathbb{R}^+ \times \mathbb{R}^-)}} \ell(q) \quad (4.1)$$

ainsi que des expressions analogues pour les autres variétés. Dans la formule (4.1), nous avons repris les notations couramment utilisées dans les sections précédentes ; nous renvoyons le lecteur aux débuts des §§2.2 et 2.3.2 s'il souhaite revoir les définitions. Ainsi, au moins lorsque σ n'est pas l'identité, calculer la dimension de $\mathcal{X}_{\leq e}$ revient à calculer le nombre $b'_{Q,R,f,\ell,\mathbb{R}^+ \times \mathbb{R}^-}(0, e)$. Comme ce dernier s'exprime comme le maximum d'une forme linéaire sur un ensemble fini on peut, en un certain sens, considérer que le problème est résolu ; en tout cas, il est aisé à partir de là d'écrire un algorithme qui répond à la question pour des entiers d , b et un d -uplet μ donnés. Toutefois, cela n'est pas entièrement satisfaisant. La raison principale est que l'on aimerait comprendre le comportement précis de la dimension de $\mathcal{X}_{\leq e}$ lorsque les paramètres d , b et e varient. Pour ce type de questions, l'approche algorithmique naïve, que l'on vient de présenter, s'avère insuffisante. À l'opposé de cette approche algorithmique, il y a un théorème général de logique qui prédit la dépendance de $b'_{Q,R,f,\ell,\mathbb{R}^+ \times \mathbb{R}^-}(0, e)$ en fonction de e . Voici ce qu'il implique dans notre cas.

Théorème 4.1. *On suppose que $\sigma \neq \text{id}$. Alors, il existe un entier N et une fonction $f : \mathbb{Z}/N\mathbb{Z} \rightarrow \mathbb{Q}$ tel que, pour e suffisamment grand, on ait :*

$$\dim_k \mathcal{X}_{\leq e} = \left\lfloor \frac{d^2}{4} \right\rfloor \cdot \frac{e}{b+1} + f(e \bmod N).$$

Démonstration. D'après la formule (4.1), la différence $\delta(e) = \dim_k \mathcal{X}_{\leq e} - \left\lfloor \frac{d^2}{4} \right\rfloor \cdot \frac{e}{b+1}$ est définie par une formule de l'arithmétique de Presburger ayant la variable libre e . Par le théorème d'élimination des quantificateurs dans l'arithmétique de Presburger, cette formule est équivalente à une formule sans quantificateurs. Par ailleurs, le théorème 2 montre que la fonction $\delta : e \mapsto \delta(e)$ est bornée sur \mathbb{N} . On déduit facilement à partir de là que, pour e suffisamment grand, elle ne dépend que de la réduction de e modulo un certain entier N . C'est exactement ce que dit le théorème. \square

Le théorème 4.1 est intéressant en soi mais, tel quel, il est absolument inutile car il ne dit rien ni sur l'entier N , ni sur la fonction f , ni sur le moment à partir duquel la formule pour la dimension est correcte. Précisons en outre, au cas où l'énoncé n'était pas clair que ces données dépendent *a priori* de d et de b . Un point positif malgré tout est qu'il existe des algorithmes pour les calculer. Par contre, malheureusement, au delà de la dimension 3 (pour laquelle on peut encore faire les calculs à la main comme nous allons le voir ensuite), il n'est pas envisageable d'utiliser de tels outils, ceux-ci étant trop peu efficaces.

Le théorème 4.1 admet un analogue pour les variétés \mathcal{X}_μ et $\mathcal{X}_{\leq \mu}$ que nous n'écrivons pas (mais nous donnerons des exemples qui devraient clarifier la situation dans la suite). Plutôt que cela, remarquons que le théorème 4.1 implique la rationalité de la série génératrice

$$\sum_{e=0}^{\infty} (\dim_k \mathcal{X}_{\leq e}) \cdot X^e.$$

De la même façon, les analogues que nous venons d'évoquer impliquent la rationalité des séries :

$$\sum_{\mu \in \mathbb{N}^d} (\dim_k \mathcal{X}_\mu) \cdot X_1^{\mu_1} X_2^{\mu_2} \cdots X_d^{\mu_d} \quad \text{et} \quad \sum_{\mu \in \mathbb{N}^d} (\dim_k \mathcal{X}_{\leq \mu}) \cdot X_1^{\mu_1} X_2^{\mu_2} \cdots X_d^{\mu_d}$$

où les entiers μ_i désignent les coordonnées de μ .

4.1.1 Calcul en petites dimensions

En guise d'illustration du résultat du théorème 4.1 (ou plutôt de l'un de ses analogues qui viennent d'être évoqués), nous nous proposons de calculer les dimensions exactes des variétés \mathcal{X}_μ lorsque $d = 2$ et également lorsque $d = 3$ dans certains cas. Pour cela, plutôt que d'utiliser les $q_{i,j}$ pour paramétrer les

d -uplet $\varphi = (\varphi_1, \dots, \varphi_d)$ comme nous l'avons fait jusqu'à présent, nous allons ici travailler avec les $\mu_{i,j}$, ce qui sera plus commode. Les inégalités qui définissent l'ensemble Q s'écrivent

$$\begin{aligned} \mu_{i-1,j-1} \leq \mu_{i,j} \leq \mu_{i-1,j} \quad \text{et} \quad b\mu_{i,i} + b \sum_{s=i+1}^j (\mu_{i,s} - \mu_{i+1,s}) + \sum_{s=j+1}^d (\mu_{i,s} - \mu_{i+1,s}) \\ \leq b\mu_{i-1,i-1} + b \sum_{s=i}^{j-1} (\mu_{i-1,s} - \mu_{i,s}) + \sum_{s=j}^d (\mu_{i-1,s} - \mu_{i,s}) \end{aligned}$$

pour tout couple d'entiers (i, j) avec $2 \leq i \leq j \leq d$. alors que les conditions d'intégrité, qui définissent le réseau R , sont données par la proposition 1.10 :

$$\begin{aligned} \forall (i, j) \in I, \quad \mu_{i,j} \in \mathbb{Z} \\ \forall i \in \{1, \dots, d\}, \quad \mu_{1,i} + \mu_{2,i+1} + \dots + \mu_{i,d} \equiv 0 \pmod{b-1}. \end{aligned}$$

On rappelle que si φ est l'élément de Φ correspondant à une donnée $(\mu_{i,j})$ satisfaisant les conditions précédentes, alors pour tout réseau $L \subset M$, les exposants des diviseurs élémentaires du $k[[u]]$ -module engendré par $\phi(L)$ par rapport à L sont les $\mu_i = \mu_{1,i}$ (voir propositions 1.2 et 1.6) et que :

$$\dim(\varphi) = \sum_{j=1}^d (d+1-j) \cdot \mu_{1,j} - \sum_{(i,j) \in I} \mu_{i,j} = \sum_{j=1}^d (d+1-j) \cdot \mu_j - \sum_{(i,j) \in I} \mu_{i,j}$$

(voir lemme 1.14). Dans la suite, on supposera toujours que $\sigma \neq \text{id}$ de sorte que la quantité précédente s'égalise avec la dimension de la variété \mathcal{X}_φ . On note $\lceil x \rceil$, la partie entière supérieure du nombre réel x , c'est-à-dire le plus petit entier supérieur ou égal à x . On pose aussi $\text{def}(x) = \lceil x \rceil - x$; c'est à l'évidence un nombre compris entre 0 et 1 qui ne dépend que de la congruence de x modulo \mathbb{Z} .

En dimension 2 D'après ce que l'on vient de rappeler, étant donnés des nombres entiers $\mu_1 \geq \mu_2$ tels que $b-1$ divise $\mu_1 + \mu_2$, calculer la dimension de la variété $\mathcal{X}_{(\mu_1, \mu_2)}$ revient à maximiser le nombre $\mu_1 - \mu_{1,2}$ sous les contraintes

$$\begin{cases} \mu_1 \leq \mu_{1,2} \leq \mu_2 \\ (b+1)\mu_{1,2} \geq b\mu_1 + \mu_2 \\ b-1 \text{ divise } \mu_{1,2} \end{cases}$$

En écrivant $\mu_{1,2} = (b-1)x$, on voit tout de suite que le maximum cherché est atteint pour $x = \lceil \frac{b\mu_1 + \mu_2}{b^2 - 1} \rceil$. Ainsi, obtient-on :

$$\dim_k \mathcal{X}_{(\mu_1, \mu_2)} = \mu_1 - (b-1) \cdot \left\lceil \frac{b\mu_1 + \mu_2}{b^2 - 1} \right\rceil = \frac{\mu_1 - \mu_2}{b+1} - (b-1) \cdot \text{def} \left(\frac{b\mu_1 + \mu_2}{b^2 - 1} \right) \quad (4.2)$$

On constate immédiatement sur la dernière écriture que la dimension de $\mathcal{X}_{(\mu_1, \mu_2)}$ s'exprime comme la somme de $\frac{\mu_1 - \mu_2}{b+1}$ (qui correspond au terme attendu) et d'un terme correctif qui ne dépend que des congruences de μ_1 et μ_2 modulo $b^2 - 1$. De surcroît, ce terme correctif varie dans l'intervalle $]1-b, 0]$; la dimension de $\mathcal{X}_{(\mu_1, \mu_2)}$ se caractérise donc encore comme le plus grand entier $\leq \frac{\mu_1 - \mu_2}{b+1}$ qui est congru à μ_1 modulo $b-1$ (en accord avec la congruence du théorème 4).

La dimension de la variété $\mathcal{X}_{\leq e}$, quant à elle, s'obtient en prenant le maximum de $\dim_k \mathcal{X}_{(\mu_1, \mu_2)}$ sur tous les couples d'entiers (μ_1, μ_2) vérifiant $0 \leq \mu_2 \leq \mu_1 \leq e$ et $\mu_1 + \mu_2 \equiv 0 \pmod{b-1}$. Le calcul devient alors pénible et conduit à distinguer de nombreux cas; nous ne le faisons pas. Il est quand même possible à peu de frais de préciser le théorème 4.1 comme suit.

Proposition 4.2. *On suppose $d = 2$ et $\sigma \neq \text{id}$. Alors pour tout entier $e \geq 0$, on a :*

$$\dim_k \mathcal{X}_{\leq e+(b^2-1)} = \dim_k \mathcal{X}_{\leq e} + (b-1).$$

Avant de donner la preuve remarquons que la proposition signifie exactement que, dans le théorème 4.1, on peut choisir $N = b^2 - 1$ et que l'égalité énoncée vaut alors pour tout e .

Démonstration. Considérons un couple (μ_1, μ_2) pour lequel les variétés $\mathcal{X}_{\leq e}$ et $\mathcal{X}_{(\mu_1, \mu_2)}$ ont même dimension. Alors par la formule (4.2), on a $\dim_k \mathcal{X}_{(\mu_1, \mu_2 + b^2 - 1)} = \dim_k \mathcal{X}_{(\mu_1, \mu_2)} + (b - 1)$. Il en résulte l'inégalité $\dim_k \mathcal{X}_{\leq e + (b^2 - 1)} \geq \dim_k \mathcal{X}_{\leq e} + (b - 1)$. Posons à présent $e' = e + (b^2 - 1)$ et choisissons (μ'_1, μ'_2) tel que $\dim_k \mathcal{X}_{\leq e'} = \mathcal{X}_{(\mu'_1, \mu'_2)}$. Comme $e' \geq b^2 - 1$, on a :

$$b - 1 = \dim_k \mathcal{X}_{\leq b^2 - 1} \leq \dim_k \mathcal{X}_{\leq e'} \leq \frac{\mu'_1 - \mu'_2}{b + 1}$$

d'où $\mu'_1 - (b^2 - 1) \geq \mu'_2$. La dimension de la variété $\mathcal{X}_{(\mu'_1 - (b^2 - 1), \mu'_2)}$ peut donc encore se calculer par la formule (4.2) et elle vaut $\dim_k \mathcal{X}_{(\mu'_1, \mu'_2)} - (b - 1)$. À partir de là, on déduit $\dim_k \mathcal{X}_{\leq e} \geq \dim_k \mathcal{X}_{\leq e'} - (b - 1)$, et la proposition est démontrée. \square

En dimension 3 Considérons (μ_1, μ_2, μ_3) un triplet d'entiers tels que $\mu_1 \geq \mu_2 \geq \mu_3$ et $\mu_1 + \mu_2 + \mu_3 \equiv 0 \pmod{b - 1}$. De façon similaire à ce qui se passait en dimension 2, calculer la dimension de $\mathcal{X}_{(\mu_1, \mu_2, \mu_3)}$ revient à maximiser la quantité $\dim(\mu) = 2\mu_1 + \mu_2 - \mu_{2,2} - \mu_{2,3} - \mu_{3,3}$ sous les contraintes

$$\begin{cases} \mu_3 \leq \mu_{2,3} \leq \mu_2 \leq \mu_{2,2} \leq \mu_1 & ; \quad \mu_{2,3} \leq \mu_{3,3} \leq \mu_{2,2} \\ (b + 1)\mu_{3,3} \geq b\mu_{2,2} + \mu_{2,3} \\ (b + 1)\mu_{2,2} + 2\mu_{2,3} - z \geq b\mu_1 + \mu_2 + \mu_3 \\ 2b\mu_{2,2} + (b + 1)\mu_{2,3} - bz \geq b\mu_1 + b\mu_2 + \mu_3 \\ \mu_{2,2} + \mu_{2,3} \equiv \mu_{3,3} \equiv 0 \pmod{b - 1} \end{cases}$$

Remarquons en premier lieu qu'à $\mu_{2,2}$ et $\mu_{2,3}$ fixés, le meilleur $\mu_{3,3}$ (*i.e.* le plus petit) est toujours $(b - 1) \cdot \lceil \frac{b\mu_{2,2} + \mu_{2,3}}{b^2 - 1} \rceil$. Ceci nous permet de reformuler le problème en éliminant la variable $\mu_{3,3}$: notre nouvel objectif est de maximiser la somme

$$2\mu_1 + \mu_2 - \mu_{2,2} - \mu_{2,3} - (b - 1) \cdot \left\lceil \frac{b\mu_{2,2} + \mu_{2,3}}{b^2 - 1} \right\rceil$$

sous les nouvelles contraintes

$$\begin{cases} \mu_3 \leq \mu_{2,3} \leq \mu_2 \leq \mu_{2,2} \leq \mu_1 \\ (b + 1)\mu_{3,3} \geq b\mu_{2,2} + \mu_{2,3} \\ (b + 1)\mu_{2,2} + 2\mu_{2,3} - (b - 1) \cdot \left\lceil \frac{b\mu_{2,2} + \mu_{2,3}}{b^2 - 1} \right\rceil \geq b\mu_1 + \mu_2 + \mu_3 \\ 2b\mu_{2,2} + (b + 1)\mu_{2,3} - b(b - 1) \cdot \left\lceil \frac{b\mu_{2,2} + \mu_{2,3}}{b^2 - 1} \right\rceil \geq b\mu_1 + b\mu_2 + \mu_3 \\ \mu_{2,2} + \mu_{2,3} \equiv 0 \pmod{b - 1} \end{cases}$$

L'écriture se simplifie encore si l'on effectue le changement de variables $x = \frac{b\mu_{2,2} + \mu_{2,3}}{b - 1}$ et $y = \frac{\mu_{2,2} + \mu_{2,3}}{b - 1} - \lceil \frac{x}{b + 1} \rceil$. En effet, on a alors

$$\dim(\mu) = 2\mu_1 + \mu_2 - 2(b - 1) \cdot \left\lceil \frac{x}{b + 1} \right\rceil - (b - 1)y$$

tandis que les contraintes deviennent :

$$\begin{cases} x, y \in \mathbb{Z} \\ \mu_3 \leq -x + b \cdot \left\lceil \frac{x}{b + 1} \right\rceil + by \leq \mu_2 \leq x - \left\lceil \frac{x}{b + 1} \right\rceil - y \leq \mu_1 \\ x + y \geq \frac{b\mu_1 + \mu_2 + \mu_3}{b - 1} \quad ; \quad x + by \geq \frac{b\mu_1 + b\mu_2 + \mu_3}{b - 1} \end{cases}$$

Oublions momentanément les inégalités compliquées de la seconde ligne et concentrons-nous sur celles de la troisième. Sur la figure 4 est représentée la région définie par celles-ci (en gris) et sont notées les valeurs de la fonction à maximiser (à une constante additive près). En étudiant cette figure — et notamment en comparant les pentes des droites définissant le domaine à celle de la droite oblique en pointillés qui

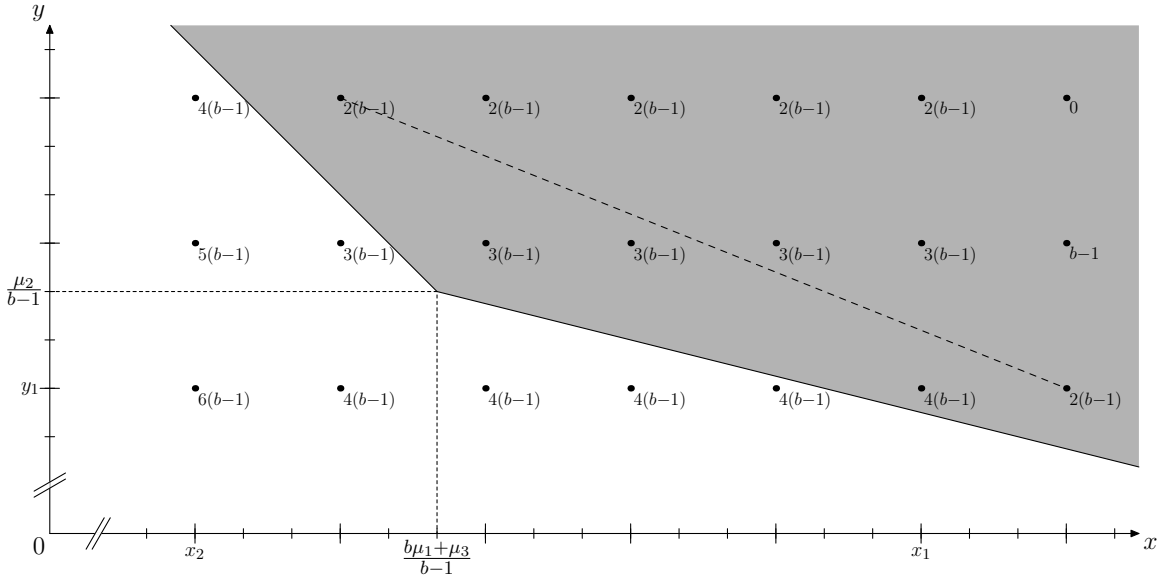


FIG. 4 – Illustration de notre problème d'optimisation pour $b = 4$

relie deux points de même valeur — on démontre que le maximum est nécessairement atteint au point de coordonnées (x_1, y_1) avec

$$x_1 = (b+1) \cdot \left\lceil \frac{b\mu_1 + \mu_3}{b^2 - 1} \right\rceil \quad \text{et} \quad y_1 = \left\lceil \frac{\mu_2}{b-1} - \frac{b+1}{b} \cdot \text{def} \left(\frac{b\mu_1 + \mu_3}{b^2 - 1} \right) \right\rceil$$

ou au point de coordonnées (x_2, y_2) avec

$$x_2 = x_1 - (b+1) \quad \text{et} \quad y_2 = b+1 + \left\lceil \frac{\mu_2}{b-1} - (b+1) \cdot \text{def} \left(\frac{b\mu_1 + \mu_3}{b^2 - 1} \right) \right\rceil.$$

Plus précisément, le maximum est atteint en (x_1, y_1) si $\text{def} \left(\frac{b\mu_1 + \mu_3}{b^2 - 1} \right) \leq \frac{b}{b+1}$ et en (x_2, y_2) dans le cas contraire. Dans la suite, nous noterons (x_0, y_0) ce point. Au sujet de la valeur du maximum, un calcul montre qu'il vaut :

$$2\mu_1 + \mu_2 - 2(b-1) \cdot \left\lceil \frac{b\mu_1 + \mu_3}{b^2 - 1} \right\rceil - (b-1) \cdot \left\lceil \frac{\mu_2}{b-1} - (b+1)m \right\rceil \quad (4.3)$$

avec

$$m = \min \left\{ \frac{1}{b} \cdot \text{def} \left(\frac{b\mu_1 + \mu_3}{b^2 - 1} \right), \text{def} \left(\frac{b\mu_1 + \mu_3}{b^2 - 1} \right) - \frac{b-1}{b+1} \right\}.$$

Rappelons-nous quand même que nous avons mis de côté certaines contraintes. Nous devons donc encore au moins nous demander à quelles conditions les x_0 et y_0 que nous venons de trouver les satisfont. Remarquons pour cela que $b+1$ divise x_0 de sorte que $\lceil \frac{x_0}{b+1} \rceil = \frac{x_0}{b+1}$ et que l'on a les encadrements suivants :

$$\frac{b\mu_1 + \mu_3}{b-1} - 1 \leq x_0 \leq \frac{b\mu_1 + \mu_3}{b-1} + b \quad \text{et} \quad \frac{\mu_2}{b-1} - 1 \leq y_0 \leq \frac{\mu_2}{b-1} + 1.$$

Ainsi il vient :

$$\frac{-b\mu_1 + b(b+1)\mu_2 - \mu_3}{b^2 - 1} - \frac{b^2 + 2b}{b+1} \leq -x_0 + b \left\lceil \frac{x_0}{b+1} \right\rceil + by_0 \leq \frac{-b\mu_1 + b(b+1)\mu_2 - \mu_3}{b^2 - 1} + \frac{b^2 + b + 1}{b+1}$$

$$\frac{b^2\mu_1 - (b+1)\mu_2 + b\mu_3}{b^2 - 1} - \frac{2b+1}{b+1} \leq x_0 - \left\lceil \frac{x_0}{b+1} \right\rceil - y_0 \leq \frac{b^2\mu_1 - (b+1)\mu_2 + b\mu_3}{b^2 - 1} + \frac{b^2 + b + 1}{b+1}$$

à partir de quoi il suit que le couple (x_0, y_0) est solution de notre problème dès que le triplet (μ_1, μ_2, μ_3) vérifie $\mu_1 - \mu_2 \leq b(\mu_2 - \mu_3) - (b^2 + b + 1)(b - 1)$ et $\mu_2 - \mu_3 \leq b(\mu_1 - \mu_2) - (b^2 + b + 1)(b - 1)$, ce qui revient encore à dire que le triplet $(\mu_1 - b^2 - b - 1, \mu_2, \mu_3 + b^2 + b + 1)$ est b -régulier. Nous avons ainsi démontré la proposition suivante.

Proposition 4.3. *On suppose $\sigma \neq \text{id}$. Soit (μ_1, μ_2, μ_3) un triplet tel que $(\mu_1 - b^2 - b - 1, \mu_2, \mu_3 + b^2 + b + 1)$ soit intégralement b -régulier (voir définition 3 de l'introduction). Alors la dimension de la variété $\mathcal{X}_{(\mu_1, \mu_2, \mu_3)}$ est donnée par la formule (4.3).*

À partir de la formule (4.3), on voit que, dans le cas où $(\mu_1 - b^2 - b - 1, \mu_2, \mu_3 + b^2 + b + 1)$ est intégralement b -régulier, la dimension de $\mathcal{X}_{(\mu_1, \mu_2, \mu_3)}$ est la somme du terme attendu $\frac{2(\mu_1 - \mu_3)}{b+1}$ et d'une quantité bornée qui ne dépend que des congruences de $b\mu_1 + \mu_3$ modulo $b^2 - 1$ et μ_2 modulo $b - 1$. À partir de cela, on peut déduire que, lorsque $d = 3$, il est possible de prendre $N = b^2 - 1$ dans le théorème 4.1. Comme c'était déjà le cas pour $d = 2$, on peut se demander s'il s'agit là d'un fait général.

4.2 Généralisations envisageables

4.2.1 À un Frobenius arbitraire

Dans tout cet article, nous avons supposé que le Frobenius agissait coordonnées par coordonnées sur M . Ceci est en fait assez restrictif, et une situation plus générale que nous aimerions étudier (notamment car elle correspond à certains problèmes importants de déformation) est celle où le Frobenius est une application semi-linéaire ϕ_M quelconque. Dans ce cas, les variétés $\mathcal{X}_{\leq e}(\phi_M)$, $\mathcal{X}_\mu(\phi_M)$ et $\mathcal{X}_{\leq \mu}(\phi_M)$ sont définies de façon analogue. Par exemple, l'ensemble des k -points de $\mathcal{X}_{\leq e}(\phi_M)$ est l'ensemble des réseaux L de M satisfaisant

$$u^e L \subset \phi_M^*(k[[u]] \otimes_{\phi, k[[u]]} L) \subset L$$

où $\phi_M^* : k[[u]] \otimes_{\phi, k[[u]]} M \rightarrow M$ est l'application linéarisée de ϕ_M . Si A désigne la matrice de ϕ_M dans une $k((u))$ -base de M (par exemple la base canonique), on s'autorisera à écrire $\mathcal{X}_{\leq e}(A)$ à la place de $\mathcal{X}_{\leq e}(\phi_M)$, et de même pour les deux autres variantes.

Nous pensons que les théorèmes 2, 4 et 5 s'étendent sans grande modification à ce cas plus général. Ci-dessous nous donnons une conjecture précise mais avant de pouvoir énoncer celle-ci nous avons besoin de faire une remarque au sujet du déterminant de ϕ_M . Comme ϕ_M est une application semi-linéaire, le déterminant de sa matrice peut varier lorsqu'on le calcule dans deux bases différentes ; toutefois la congruence modulo $b - 1$ de sa valuation reste, elle, fixe. Il fait donc bien sens d'écrire que $\text{val}(\det \phi_M)$ est congru à un certain entier modulo $b - 1$.

Conjecture 4.4. *Il existe des constantes b_0, c_1, \dots, c_7 et un vecteur $\mu_0 \in \mathbb{R}^d$ tel que si $b \geq b_0$, alors*

– pour tout entier e , on ait :

$$\dim_k \mathcal{X}_{\leq e}(\phi_M) \leq c_1 + \left\lfloor \frac{d^2}{4} \right\rfloor \cdot \frac{e}{b+1}$$

– pour tout entier e suffisamment grand, on ait :

$$\dim_k \mathcal{X}_{\leq e}(\phi_M) \geq -c_2 + \left\lfloor \frac{d^2}{4} \right\rfloor \cdot \frac{e}{b+1}$$

– pour tout $\mu = (\mu_1, \dots, \mu_d) \in \mathbb{R}^d$ tel que $\mu_1 \geq \dots \geq \mu_d$ et $\mu_1 + \dots + \mu_d \equiv \text{val}(\det \phi_M) \pmod{b-1}$, on ait :

$$\dim_k \mathcal{X}_\mu(\phi_M) \leq c_3 + (b-1) \cdot \sum_{i=1}^d \sum_{n=1}^{\infty} \mu_i \cdot \frac{d+1-i-w^n(i)}{b^n}$$

– pour tout μ comme précédemment tel qu'en outre $\mu_i \geq \mu_{i+1} + c_4$ pour tout i , on ait si $d \geq 3$:

$$\dim_k \mathcal{X}_\mu(\phi_M) \geq -c_5 + (b-1) \cdot \sum_{i=1}^d \sum_{n=1}^{\infty} \mu_i \cdot \frac{d+1-i-w^n(i)}{b^n}$$

– pour tout $\mu = (\mu_1, \dots, \mu_d) \in \mathbb{R}^d$ tel que $\mu_1 \geq \dots \geq \mu_d$, on ait :

$$-c_6 + \sup_{\substack{\mu' \leq \mu \\ \mu' - \mu_0 \text{ b-rég.}}} \frac{\langle 2\bar{\rho} | \mu' \rangle_d}{b+1} \leq \dim_k \mathcal{X}_{\leq \mu}(\phi_M) \leq c_7 + \sup_{\substack{\mu' \leq \mu \\ \mu' \text{ b-rég.}}} \frac{\langle 2\bar{\rho} | \mu' \rangle_d}{b+1}.$$

On notera que dans le cas où la somme $\mu_1 + \dots + \mu_d$ n'est pas congrue à $\text{val}(\det \phi_M)$, la variété \mathcal{X}_μ est vide. La condition $d \geq 3$ peut paraître étrange, mais certains calculs explicites en dimension 2 (voir par exemple [5]) montrent que, dans ce cas, pour certains ϕ_M (précisément, ceux qui conduisent à des objets simples) des congruences supplémentaires sur les μ_i doivent être imposées afin que la variété $\mathcal{X}_\mu(\phi_M)$ résultante ne soit pas vide. Néanmoins, l'auteur pense — et certains calculs numériques tendent à le confirmer — qu'il s'agit là d'un phénomène lié à la petite dimension qui disparaît à partir de $d = 3$.

Il paraît envisageable d'attaquer la conjecture 4.4 par des méthodes similaires à celles de cet article. Signalons également une autre piste possible. Étant donné un Frobenius quelconque ϕ_M sur M , il existe toujours une extension totalement ramifiée $k((v))$ de $K = k((u))$ et une base de $k((v)) \otimes_{k((u))} M$ dans laquelle la matrice de ϕ_M est l'identité. En outre d'après la description des objets simples obtenue dans [2] (pour le cas $k = \mathbb{F}_p$) et [7] (pour le cas général), l'extension $k((v))/k((u))$ peut être choisie modérément ramifiée si le ϕ -module M est semi-simple. Comprendre comment les variétés $\mathcal{X}_{\leq e}(\phi_M)$, etc. (et notamment leurs dimensions) se comportent lorsque l'on change K en une extension totalement ramifiée (éventuellement seulement modérément ramifiée) pourrait donc peut-être permettre de démontrer la conjecture 4.4 à partir des théorèmes 2, 4 et 5 de cet article.

4.2.2 À d'autres propriétés géométriques

Nous nous sommes pour l'instant intéressés exclusivement à la dimension des variétés $\mathcal{X}_{\leq e}$, \mathcal{X}_μ et $\mathcal{X}_{\leq \mu}$ mais d'autres propriétés géométriques revêtent également un intérêt certain. Il en est ainsi notamment du nombre de composantes connexes de ces variétés. À part pour le cas $d = 2$ qui peut être traité à la main par des méthodes *ad hoc* (voir [5]) et qui conduit déjà à des énoncés non triviaux, pratiquement rien n'est connu. De façon générale, étudier la géométrie fine des variétés précédentes paraît être une question très difficile. On peut néanmoins se demander dans quelle mesure les méthodes développées dans cet article sont susceptibles de nous aider dans cette tâche. Si tout ce qui concerne l'optimisation linéaire semble lié exclusivement au calcul de la dimension, il reste possible que la stratification par les variétés \mathcal{X}_φ que nous avons définie au §1 ait encore un rôle à jouer pour d'autres questions, comme par exemple le calcul de la fonction zêta si le corps de base k est fini ou de la caractéristique d'Euler-Poincaré.

En s'inspirant de la théorie de l'intégration motivique, on peut être encore plus précis. Notons $K_0(\text{Var}_k)$ le groupe abélien présenté de la façon suivante :

- les générateurs sont les symboles $[X]$ où X est un schéma de type fini sur k ;
- les relations sont

$$\begin{aligned} [X] &= [X_{\text{red}}] && \text{où } X_{\text{red}} \text{ est le réduit de } X \\ [X] &= [Y] && \text{si } X \text{ et } Y \text{ sont isomorphes} \\ [X] &= [U] + [F] && \text{si } U \text{ est un ouvert de } X \text{ et } F \text{ est le fermé complémentaire.} \end{aligned}$$

La formule $[X] \cdot [Y] = [X \times_k Y]$ définit un produit sur $K_0(\text{Var}_k)$ qui est fait un anneau commutatif. L'élément neutre pour l'addition (resp. la multiplication) est le symbole de la variété vide (resp. du point). De même que l'on a considéré dans le §4.1 les séries génératrices des dimensions de $\mathcal{X}_{\leq e}$, \mathcal{X}_μ et $\mathcal{X}_{\leq \mu}$, on peut définir ici la série génératrice suivante :

$$S(X_1, \dots, X_d) = \sum_{\mu \in \mathbb{N}^d} [\mathcal{X}_\mu(\phi_M)] \cdot X_1^{\mu_1} X_2^{\mu_2} \dots X_d^{\mu_d}$$

où ϕ_M est un certain opérateur ϕ -semi-linéaire agissant sur M et les μ_i sont les coordonnées de μ . Bien sûr, on peut également considérer les séries génératrices associées aux variétés $\mathcal{X}_{\leq \mu}(\phi_M)$ et $\mathcal{X}_{\leq e}(\phi_M)$ mais celles-ci se déduisent de la précédente à l'aide de manipulations algébriques élémentaires, et c'est pourquoi nous nous contenterons de celle-ci.

Si l'on note $\mathbb{L} = [\mathbb{A}_k^1]$ le symbole de la droite affine, des résultats ou conjectures classiques en intégration motivique stipulent que les séries du type de S sont en fait des fractions rationnelles lorsque leurs coefficients sont vus dans le localisé $K_0(\text{Var}_k)[\mathbb{L}^{-1}]$ (ou parfois encore, un certain complété de cet anneau). Nous pensons qu'il est raisonnable d'énoncer une conjecture similaire dans notre situation.

Conjecture 4.5. *Il existe deux polynômes $P, Q \in K_0(\text{Var}_k)[X_1, \dots, X_d]$ tels que $Q(0, \dots, 0)$ soit inversible dans $K_0(\text{Var}_k)[\mathbb{L}^{-1}]$ et l'égalité*

$$S(X_1, \dots, X_d) = \frac{P(X_1, \dots, X_d)}{Q(X_1, \dots, X_d)}$$

ait lieu dans l'anneau $K_0(\text{Var}_k)[\mathbb{L}^{-1}][[X_1, \dots, X_d]]$.

L'intérêt d'un tel énoncé est qu'il peut être spécialisé à un certain nombre d'invariants géométriques ou arithmétiques plus classiques. Plus précisément dès que l'on dispose d'un morphisme f de $K_0(\text{Var}_k)$ dans un anneau A qui envoie \mathbb{L} sur un élément inversible, sa véracité implique la rationalité de la série :

$$\sum_{\mu \in \mathbb{N}^d} f([\mathcal{X}_\mu(\phi_M)]) \cdot X_1^{\mu_1} X_2^{\mu_2} \dots X_d^{\mu_d}.$$

Or, il existe un certain nombre de tels morphismes f intéressants. Si k est un corps fini, il y a par exemple celui qui a un symbole $[X]$ associe le cardinal de $X(k)$, ou plus généralement la fonction zêta de X . Pour un corps k quelconque, on dispose également d'exemples construits par voie cohomologique comme les nombres de Betti ou le polynôme de Poincaré virtuel. À partir de là, on peut retrouver la dimension de X ou encore son nombre de composantes irréductibles de dimension maximale. La conjecture 4.5 admet donc pour conséquence la rationalité de la série génératrice des dimensions (que nous avons démontrés directement dans cet article), mais implique également la rationalité d'autres séries génératrices numériques.

Finalement, pour étudier d'autres propriétés géométriques qui ne proviennent pas de $K_0(\text{Var}_k)$, il pourrait être intéressant de comprendre comment les variétés \mathcal{X}_φ s'agencent entre elles à l'intérieur de $\mathcal{X}_{\leq e}$, \mathcal{X}_μ ou $\mathcal{X}_{\leq \mu}$. Notamment, une question qui nous paraît importante est de déterminer l'adhérence de \mathcal{X}_φ à l'intérieur de ces variétés. Par exemple, s'écrit-elle comme une union de certains $\mathcal{X}_{\varphi'}$ où φ' vérifie une condition qui s'exprime facilement en fonction de φ ?

4.2.3 À un groupe réductif connexe arbitraire

À l'instar des variétés de Deligne-Lusztig, il est possible d'étendre la définition des variétés \mathcal{X}_μ et $\mathcal{X}_{\leq \mu}$ à un groupe réductif connexe déployé quelconque (le cas que nous venons d'étudier étant celui de GL_d). Plus précisément, considérons un groupe réductif connexe G défini sur le corps k (que, pour simplifier, nous continuons à supposer algébriquement clos) et $T \subset G$ un tore maximal. Notons $X_*(T)$ le groupe des caractères de T , et fixons une chambre de Weyl dans $X_*(T) \otimes \mathbb{R}$ dont nous notons C l'adhérence. Si $\lambda \in X_*(T)$, notons encore u^λ l'image de $u \in \mathbb{G}_m(K)$ dans $T(K) \subset G(K)$, où $K = k((u))$. Posons également $\mathcal{O}_K = k[[u]]$. Par la décomposition de Cartan, on sait que $G(K)$ s'écrit comme l'union disjointe des doubles classes $G(\mathcal{O}_K)u^\mu G(\mathcal{O}_K)$ où μ parcourt l'ensemble des copoids dominants. Pour un tel copoids μ et $A \in G(K)$, on peut alors définir des variétés $\mathcal{X}_\mu^G(A)$ dont les k -points sont :

$$\mathcal{X}_\mu^G(A)(k) = \{ g \in G(K)/G(\mathcal{O}_K) \mid g^{-1}A\phi(g) \in G(\mathcal{O}_K)u^\mu G(\mathcal{O}_K) \}.$$

On définit également $\mathcal{X}_{\leq \mu}^G(A)$ comme la réunion des $\mathcal{X}_{\mu'}^G(A)$ où μ' décrit l'ensemble des copoids dominants tels que $\mu - \mu'$ s'écrit comme une combinaison linéaire à coefficients positifs des racines simples correspondant à notre choix de C . Si G est le groupe linéaire GL_d , on retrouve les variétés $\mathcal{X}_\mu(A)$ et $\mathcal{X}_{\leq \mu}(A)$. De façon générale, les variétés $\mathcal{X}_\mu^G(A)$ et $\mathcal{X}_{\leq \mu}^G(A)$ sont toujours de dimension finie, et on peut s'interroger sur la valeur de cette dimension.

Dans cette optique, une première question est de savoir si le théorème 4 a des chances de se généraliser à cette nouvelle situation, et le cas échéant sous quelle forme. Un premier coup d'œil à l'expression

$$(b-1) \cdot \min_{w \in \mathfrak{S}_d} \langle \vec{\rho}_w \mid \mu \rangle_d \quad \text{où} \quad \vec{\rho}_w = \left(\sum_{n=1}^{\infty} \frac{d+1-i-w^n(i)}{b^n} \right)_{1 \leq i \leq d} \in \mathbb{R}^d \quad (4.4)$$

qui apparaît dans son énoncé (et qui constitue une première approximation de la dimension de \mathcal{X}_μ) laisse bon espoir. En effet, on voit d'emblée apparaître un minimum pris sur le groupe des permutations de $\{1, \dots, d\}$, c'est-à-dire exactement sur le groupe de Weyl de GL_d . En outre si l'on fait agir ce groupe de manière

naturelle sur \mathbb{R}^d — c'est-à-dire par $w \cdot (y_1, \dots, y_d) = (y_{w^{-1}(1)}, \dots, y_{w^{-1}(d)})$ — le vecteur $\vec{\rho}_w$ s'exprime en fonction de $\vec{\rho} = (\frac{d+1}{2} - i)_{1 \leq i \leq d}$ comme suit :

$$\vec{\rho}_w = (b-1) \cdot \sum_{n=1}^{\infty} \frac{\vec{\rho} + w^{-n}\vec{\rho}}{b^n} = \vec{\rho} + (b-1) \cdot (bw-1)^{-1}(\vec{\rho})$$

au moins lorsque b est assez grand pour que l'endomorphisme $bw-1$ de \mathbb{R}^d soit inversible. Si l'on se rappelle finalement que $\vec{\rho}$ est égal à la demi-somme des racines positives du système de racines A_d , on voit que la formule (4.4) s'exprime uniquement en termes du système de racines du groupe GL_d . Ces considérations conduisent à la conjecture suivante.

Conjecture 4.6. *Soit G un groupe réductif connexe sur k . Soit T un tore maximal de G . Notons W le groupe de Weyl associé et fixons une fois pour toutes le choix d'une chambre de Weyl. Soit $\vec{\rho}$ la demi-somme des racines positives de G . Considérons enfin $A \in G(K)$. Alors, il existe des constantes b_0 et c_0 telles que pour tout $b \geq b_0$, on ait :*

$$\dim_k \mathcal{X}_{\mu}^G(A) \leq c_0 + \inf_{w \in W} \langle \vec{\rho}_w | \mu \rangle \quad \text{où} \quad \vec{\rho}_w = \vec{\rho} + (b-1) \cdot (bw-1)^{-1}(\vec{\rho})$$

pour tout copoids dominant μ .

Il paraît aussi raisonnable de croire qu'une minoration de la dimension de $\mathcal{X}_{\mu}^G(A)$ par une expression du même type soit valable, au moins lorsque μ vérifie une certaine condition d'intégrité et reste suffisamment lors de la frontière de C . Malgré tout, gardant à l'esprit le comportement singulier des variétés $\mathcal{X}_{\mu}(\phi_M)$ lorsque ϕ_M représente un ϕ -module simple en dimension 2, nous préférons rester prudent et évasif à ce sujet.

Quoi qu'il en soit, soulignons que le mot le plus long de W , noté w_0 , échange les racines positives avec les racines négatives. En particulier, on en déduit que $w_0(\vec{\rho}) = -\vec{\rho}$, d'où il résulte que $(bw_0-1)(\vec{\rho}) = -(b+1)\vec{\rho}$, et par suite que $\vec{\rho}_{w_0} = \frac{2\vec{\rho}}{b+1}$; on retrouve donc encore une fois ce vecteur particulier. La conjecture donne également une indication sur la façon d'étendre la définition de copoids b -réguliers : un copoids dominant μ est dit b -régulier lorsque le minimum des produits scalaires $\langle \vec{\rho}_w | \mu \rangle$ ($w \in W$) est atteint pour $w = w_0$, ce qui s'écrit en déroulant les définitions :

$$\langle \vec{\rho} + (b+1) \cdot (bw-1)^{-1}(\vec{\rho}) | \mu \rangle \geq 0 \tag{4.5}$$

pour tout $w \in W$. Cette définition s'étend à tous les $\mu \in X_{\star}(T) \otimes \mathbb{R}$. On peut démontrer que, si b est assez grand, un copoids μ est b -régulier si, et seulement si, il vérifie les inégalités (4.5) pour tout $w \in W$ de longueur $\ell(w_0) - 1$. Par ailleurs, pour b suffisamment grand, la suite des copoids b -réguliers est croissante en b (i.e. si μ est b -régulier, alors il est b' -régulier pour tout $b' \geq b$) et tout copoids b -régulier est dominant, dans le sens où il appartient à C . Réciproquement, si μ est un élément de l'intérieur de C (c'est-à-dire un élément de la chambre de Weyl que nous avons choisie), il est b -régulier pour b suffisamment grand (le « suffisamment » dépendant bien sûr de μ).

Nous avons également une conjecture pour les variétés $\mathcal{X}_{\leq \mu}^G(A)$:

Conjecture 4.7. *Soit G un groupe réductif connexe sur k . Soit T un tore maximal de G . Notons W le groupe de Weyl associé et fixons une fois pour toutes le choix d'une chambre de Weyl. Soit $\vec{\rho}$ la demi-somme des racines positives de G . Considérons enfin $A \in G(K)$. Alors, il existe des constantes c_1 et c_2 et un élément $\mu_0 \in X_{\star}(T) \otimes \mathbb{R}$ tels que :*

$$-c_2 + \sup_{\substack{\mu' \leq \mu \\ \mu' - \mu_0 \text{ b-rég.}}} \frac{\langle 2\vec{\rho} | \mu' \rangle_d}{b+1} \leq \dim_k \mathcal{X}_{\leq \mu}^G(A) \leq c_1 + \sup_{\substack{\mu' \leq \mu \\ \mu' \text{ b-rég.}}} \frac{\langle 2\vec{\rho} | \mu' \rangle_d}{b+1}$$

où μ' désigne, ici, un copoids réel.

Un cas particulièrement intéressant, qui apparaît déjà dans l'article de Kisin [6], est celui où l'on suppose le corps k parfait (par exemple $k = \mathbb{F}_p$), où l'on se donne une extension finie ℓ de k et où l'on considère le groupe G défini comme la restriction des scalaires à la Weil de ℓ à k de GL_d . Les variétés obtenues ont alors encore une interprétation arithmétique puisqu'elles apparaissent comme certains espaces de modules de schémas en groupes définis sur des corps locaux. Lorsque $d = 2$, le calcul de leur dimension a déjà été accompli par Imai dans [10] et, dans ce cas, les résultats qu'il obtient sont en accord avec les conjectures précédentes.

Références

- [1] C. Breuil, *Schémas en groupes et corps des normes*, disponible à <http://www.ihes.fr/~breuil/publications.html>, 1998
- [2] X. Caruso, *Sur la classification de quelques ϕ -modules simples*, Mosc. Math. J. **9** (2009)
- [3] E. Gawrilow, M. Joswig, *polymake : a Framework for Analyzing Convex Polytopes in Polytopes — Combinatorics and Computation*, Birkhäuser (2000), pp. 43–74
- [4] U. Görtz, T. Haines, R. Kottwitz, D. Reuman, *Dimensions of some affine Deligne-Lusztig varieties*, Ann. Scient. Éc. Norm. Sup. **39** (2006), pp. 467–511
- [5] E. Hellmann, *On the structure of some moduli spaces of finite flat group schemes*, Mosc. Math. J. **9** (2009), pp. 531–561
- [6] M. Kisin, *Moduli of finite flat group schemes and modularity*, Annals of Math. **170** (2009), pp. 1085–1180.
- [7] J. Le Borgne, *Un algorithme pour la réduction des ϕ -modules sur $k((u))$* , en préparation
- [8] N. Imai, *On the connected components of moduli spaces of finite flat models*, à paraître à Amer. J. Math.
- [9] N. Imai, *Finite flat models of constant group schemes of rank two*, preprint (2008)
- [10] N. Imai, *Ramification and moduli spaces of finite flat models*, preprint (2008)
- [11] D. Monniaux. *A quantifier elimination algorithm for linear real arithmetic*, in LPAR (Logic for Programming Artificial Intelligence and Reasoning), Lecture Notes in Computer Science **5330**, pp. 243–257.
- [12] C. H. Papadimitriou, K. Steiglitz *The Max-Flow, Min-Cut Theorem in Combinatorial Optimization : Algorithms and Complexity*, Dover (1998), pp. 120–128.
- [13] A. Rényi, *Théorie des éléments saillants d'une suite d'observations*, Ann. Fac. Sci. Univ. Clermont-Ferrand **8** (1962), pp. 7–13
- [14] G. Pappas, M. Rapoport, *Φ -modules and coefficient spaces*, Mosc. Math. J. **9** (2009), pp. 625–663
- [15] E. Viehmann, *The dimension of some affine Deligne-Lusztig varieties*, Ann. Scient. Éc. Norm. Sup. **39** (2006), pp. 513–526