Notes creuses sur l'élimination creuse

Ioannis Z. Emiris

Université d'Athènes, Grèce
emiris@di.uoa.gr, http://www.di.uoa.gr/∼emiris
INRIA Sophia-Antipolis, France

5 mars 2009

Table des matières

1 Motivation

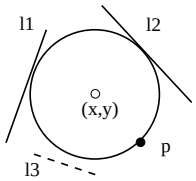
La théorie d'élimination creuse utilise plusieurs notions géométriques dans l'étude de polynômes et de systèmes algébriques. On commence avec la notion de base qui est le volume mixte, et on propose des méthodes pour son calcul. Quand il y a plusieurs coefficients égaux à zéro, comme dans la plupart

des problèmes en robotique, en vision et en géométrie algorithmique, le volume mixte donne des bornes beaucoup plus précises. Cela est la base de la théorie de l'élimination creuse qui a commencé à se développer depuis les années 1970, et qui arrive aujourd'hui à proposer des méthodes effectives pour l'étude des systèmes algébriques.

Ensuite on étudie le résultant torique, ou creux, et propose plusieurs algorithmes pour son calcul effectif via des formules matricielles. En particulier, on étudie des algorithmes pour construire une matrice de Newton qui exprime un multiple non-trivial du résultant creux, ainsi que la matrice de Macaulay, de Bézout et de Dixon. On montre comment réduire la résolution d'un système de dimension zéro au calcul des valeurs et vecteurs propres, en utilisant ces formules matricielles du résultant creux et on offre quelques exemples et applications.

Pour motiver l'étude de la théorie d'élimination creuse, on note quelques applications typiques où elle donne des résultats beaucoup plus précis que les approches classiques, ou des exemples où l'application des résultants quelconques est intéressante.

1. En la cinématique inverse d'un robot 6R (6 degrés de liberté de rotation) aux axes qui s'intersectent, le nb de configurations possible est 16 qui est égal au volume mixte et la borne de Bézout multi-homogène du système algébrique correspondant, tandis que la borne de Bézout classique $= 64$.
2. En géométrie algorithmique, dans le calcul du diagramme de Voronoï de segments, on applique plusieurs fois le test "InCircle". Si les coordonnées projectives sont données en k chiffres, la précision est de $48k + O(1)$ chiffres pour le calcul [BMS94, Lem. 1]. La démonstration de ce fait ainsi que le calcul lui-même est immédiate avec les résultants. Considérons le cas pire :

   Ceci donne un système de 3 polynômes complètement denses en les 2 coordonnées du centre :

   $$\mathrm{dist}(l_1,(x,y)) - \mathrm{dist}(l_2,(x,y)) = \mathrm{dist}(p,(x,y)) - \mathrm{dist}(l_1,(x,y)) = \mathrm{dist}(l_3,(x,y)) - \mathrm{dist}(p,(x,y)) = 0.$$

   Les coefficients sont de $4k$ chiffres, le degré total du résultant creux est $\deg R = 12$ et la matrice de Dixon est optimale, donc le nombre de chiffres nécessaires et suffisantes est $48k + O(1)$.
3. Dans un cas moins coûteux on est donné 4 points projectifs $(a_i : b_i : c_i)$ et $\deg_{a,b,c} R = 4$. Ici, la matrice de Macaulay et de Newton sont exactes donc on peut effectuer le calcul avec $8k$ chiffres.
4. Un problème important en modélisation et en CAO est celui de *l'implicitation* d'une courbe ou d'une surface paramétrée. Prenons l'exemple d'une surface *bilinéaire* aux paramètres s, t :

   $$f_0 = c_{00} + c_{01}s + c_{02}t + c_{03}st,\ f_1 = c_{10} + c_{11}s + c_{12}t + c_{13}st,\ f_2 = c_{20} + c_{21}s + c_{22}t + c_{23}st. \quad (1)$$

   Il s'agit de trouver une équation dont les solutions sont les points de cette surface, en éliminant les s, t. Le *résultant* des f_0, f_1, f_2 par rapport aux s, t nous donne cette équation en général. Mais le résultant *classique* (projectif) de ce système peut être identiquement nul (exercice 8.5). Par contre, le résultant *creux* donne précisément l'équation implicite de la surface.

Nous citons une autre motivation pour étudier le polytope de Newton. Soit $f \in \mathbb{C}[x_1^{\pm 1}, \ldots, x_n^{\pm 1}]$ et sa variété $Z \subset (\mathbb{C}^*)^n$. L'application

$$\log : (\mathbb{C}^*)^n \to \mathbb{R}^n : (x_1, \ldots, x_n) \mapsto (\log|x_1|, \ldots, \log|x_n|).$$

définie *l'amibe* de F comme l'image $\log(Z)$. Elle sera fortement liée au polytope de Newton. C'est une notion introduite dans [GKZ94], où sont établis les théorèmes ci-dessous.

Nous commençons avec deux faits connus : Pour une série de Laurent, son domaine de convergence dans $(\mathbb{C}^*)^n$ est de la forme $\log^{-1}(B)$ pour un convexe $B \subset \mathbb{R}^n$. Si $\phi(x)$ est holomorphe[1] dans un domaine de la forme $\log^{-1}(B)$, pour $B \subset \mathbb{R}^n$ convexe et ouvert, alors il existe une série de Laurent unique qui converge vers $\phi(x)$ dans ce domaine.

Corollaire 1.1 [GKZ94, Cor.1.6] *Les composantes de $\mathbb{R}^n - \log(Z)$ sont convexes et sont en bijection avec les expansions en séries de Laurent de $1/f(x)$.*

Soit Q le polytope de Newton de f, γ un sommet, et $N(\gamma)$ le cône des normales sortantes de Q à γ. Suppposons que

$$f = c_\gamma x^\gamma (1 + g(x)), \quad g \in \mathbb{C}[x_1^{\pm 1}, \dots, x_n^{\pm 1}].$$

Nous écrivons l'expansion en série de Laurent :

$$R_\gamma(x) = \frac{1}{f} = c_\gamma^{-1} x^{-\gamma}(1 - g + g^2 - \cdots).$$

Notons que les exposants de $R_\gamma(x)$ appartiennent au cône translaté $-\gamma + \mathbb{R}_+(Q - \gamma) \subset \mathbb{R}^n$.

Proposition 1.2 [GKZ94, Prop.1.7] *Il existe un vecteur $b \in N(\gamma)$ t.q. la série de Laurent R_γ converge absolument pour tout $x \in (\mathbb{C}^*)^n$ t.q. $\log(x) \in b + N(\gamma)$. Pour ces x, $f(x) \neq 0$.*

Preuve Pour la convergeance absolue, il suffit d'avoir $|g(x)| < 1$, pour tout $x \in (\mathbb{C}^*)^n$. Notons que $(b, a - \gamma) \leq 0$ pour tout $b \in N(\gamma)$ et tout $a \in Q \cap \mathbb{Z}^n$, $a \neq \gamma$. Nous choisissons

$$b \in N(\gamma) : \quad (b, a - \gamma) \ll 0, \quad \forall a \in Q \cap \mathbb{Z}^n,\ a \neq \gamma.$$

Puisque le support de $g(x)$ est $Q - \gamma$ alors, pour un monôme $x^{a-\gamma}$, nous avons $\log(|x^{a-\gamma}|) = (a - \gamma) \cdot \log(|x|) \ll 0$, si $\log(x) \in b \in N(\gamma)$. Alors $|g(x)| < 1$. □

Corollaire 1.3 [GKZ94, cor.1.8] *Les sommets de Q sont en bijection avec les composantes connexes de $\mathbb{R}^n - \log(Z)$ qui contiennent un cône (affine) convexe avec intérieur non-vide.*

Proposition 1.4 [GKZ94, prop.1.9] *Supposons que $S^{n-1}(m) \subset \mathbb{R}^n$ est la sphère de rayon m et que $\dim Q = n$. Alors la limite*

$$\lim_{m \to \infty} \frac{1}{m} \cdot \left(S^{n-1}(m) \cap \log(Z) \right)$$

existe et est égale au squellette, de dimension $n - 2$, d'une décomposition de S^{n-1} qui est duale à la décomposition de Q par ses faces.

2 Volume mixte

Dans ce qui suit, tous les polytopes ou polyèdres seront convexes et finis. Un polyèdre est dit *entier* si ses sommets ont de coordonnées entières.

Définition 2.1 *Étant donné un polyèdre $P \subset \mathbb{R}^k$, la* normale extérieure ou sortante *$N \in \mathbb{R}^k$ de sa* face *$F \subset P$ est telle que $f, f' \in F, p \in P \setminus F \Rightarrow (f, N) = (f', N) > (p, N)$ où on note $(\cdot, \cdot)$ le produit scalaire dans $\mathbb{R}^k$. La* normale intérieure ou rentrante *de la même face est $-N$. Si les sommets de P appartiennent à $\mathbb{Z}^k$, nous pouvons choisir $N \in \mathbb{Z}^k$.*

[1] c.à.d. differentiable un nombre infini de fois.

Les faces de dimension 0, 1, ou maximale sont, respectivement, les sommets, arêtes et facettes de P. L'espace des normales d'une face F est de dimension = codim(F). Chaque polyèdre $P \in \mathbb{R}^n$ peut être exprimé comme une intersection finie des demi-espaces définis par ses facettes F : $P = \cap_F \{p \in \mathbb{R}^n : (p, v) \geq (F, v)\}$, où v est la normale rentrante de F.

Dans la suite, $\mathrm{Vol}(P)$ ou $\mathrm{Vol}_n(P)$ est le volume euclidien du polyèdre P dans $\mathbb{R}^n$ t.q. le volume d'un cube aux arêtes de longueur 1 est égal à l'unité. Dans un sous-espace de dimension k, le volume dépend de la base des k vecteurs choisie.

Lemme 2.2 *On appelle volume* normalisé *la fonction de volume* $\mathrm{Vol}'_k(\cdot)$ *dans un sous-espace de dimension k qui s'évalue à 1 sur le parallélotope (dit fondamental) défini par les k vecteurs de la base. Soit un polyèdre $P \in \mathbb{R}^n$ aux sommets entiers, alors $n\mathrm{Vol}_n(P) = \sum_F \mathrm{Vol}'_{n-1}(F)(F, v)$, où $v \in \mathbb{Z}^n$ est la normale sortante de la facette F et pgcd$(v_1, \ldots, v_n) = 1$.*

Dans le cas d'un polytope convexe, prenons un point p à l'intérieur, ce qui décompose P en des simplexes, une par facette. Le volume de la facette qui contient F est $(1/n)\mathrm{Vol}_{n-1}(F)d_F$ où d_F est la distance entre P et F.

Exercice 2.3 Montrez, comme corollaire, que si $P \subset \mathbb{R}^n$ est aux sommets entiers, alors $n!\,\mathrm{Vol}_n(P) \in \mathbb{Z}$. □

La somme de Minkowski est $Q_1 + Q_2 = \{q_1 + q_2 : q_i \in Q_i, i = 1, 2\}$.

Exercice 2.4 Si les Q_i sont convexes (resp. aux sommets entiers) alors la somme $\sum_i Q_i$ est convexe (aux sommets entiers). La face de la somme qui minimise le produit scalaire avec une normale v est égale à $F_1 + F_2$, où les faces $F_i \subset Q_i$ minimisent le produit scalaire avec v dans le Q_i correspondant. Si $A_i \subset \mathbb{Z}^n$, alors $\mathrm{Conv}(\sum_i A_i) = \sum_i \mathrm{Conv}(A_i)$. □

Exercice 2.5 Soient $Q_i \in \mathbb{R}^n$ et $\lambda_1, \ldots, \lambda_k \in \mathbb{R}_{\geq 0}$. $\mathrm{Vol}_n(\lambda_1 Q_1 + \cdots + \lambda_k Q_k)$ est un polynôme dans $\mathbb{Q}[\lambda_1, \ldots, \lambda_k]$, homogène de degré n. □

Par exemple, $\mathrm{Vol}(\lambda Q_1) = \lambda^n \mathrm{Vol}(Q_1)$.

Définition 2.6 *Étant donnés $k \geq n$ polytopes $Q_1, \ldots, Q_k \subset \mathbb{R}^n$ dont les sommets appartiennent à $\mathbb{Z}^n$, le* volume mixte *$VM(Q_1, \ldots, Q_n)$ est le coefficient du monôme $\lambda_1 \cdots \lambda_n$ dans* $\mathrm{Vol}(\lambda_1 Q_1 + \cdots + \lambda_k Q_k)$.

Cette définition est bonne même pour $k < n$ de manière triviale, puisque tous les volumes mixtes seraient nuls. Il est clair que le volume mixte est invariant par rapport aux permutations des Q_i. Notre définition du volume mixte diffère de la définition classique d'un facteur $n!$, où n est la dimension de l'espace euclidien ; c.à.d. nous avons regroupé les $n!$ termes multi-linéaires en les $\lambda_1, \ldots, \lambda_n$. Il est clair que $VM(Q_1, \ldots, Q_n) \geq 0$ et que si $\mathrm{Vol}(Q_i) = 0$, alors $VM(Q_1, \ldots, Q_n) = 0$. L'inverse est démontré dans [Ful93, sect.5.4].

Exercice 2.7 $VM(Q_1, \ldots, Q_n) = 0 \Leftrightarrow \exists I \subset \{1, \ldots, n\} : \dim(\sum_{i \in I} Q_i) < |I|$. De plus, s'il y a $I \subset \{0, \ldots, n\} : |I| \geq n$ et $\dim(\sum_i Q_i) = n$, alors $\exists \{i_1, \ldots, i_n\} \subset \{0, \ldots, n\}$ t.q. $VM(Q_{i_1}, \ldots, Q_{i_n}) > 0$. □

On peut aussi démontrez que le volume mixte ne peut pas s'accroître si on remplace un polytope par un autre inclus dans le premier : $Q'_1 \subset Q_1 \Rightarrow VM(Q'_1, Q_2, \ldots) \leq VM(Q_1, Q_2, \ldots)$.

Exercice 2.8 Si $\dim Q_i = 1, Q_i \subset \mathbb{R}^n$, $i = 1, \ldots, n$, alors $VM(Q_1, \ldots, Q_n) = \mathrm{Vol}_n(\sum_{i=1}^n Q_i) = |\det A|$, où A est une matrice $n \times n$ dont les lignes ou les colonnes expriment les vecteurs Q_i. Notons que $\sum_{i=1}^n Q_i$ est un parallélotope. □

Théorème 2.9 [Ewa96] *$VM(Q_1,\dots,Q_n) > 0 \Leftrightarrow$ il existe des segments E_i : $\dim E_i = 1, E_i \subset Q_i$, $i = 1,\dots,n$ tels que $VM(E_1,\dots,E_n) > 0$, ce qui par l'exercice précédent revient à dire que les vecteurs E_i sont linéairement indépendants.*

Lemme 2.10 [Ful93]

$$VM(Q_1,\dots,Q_n) = \sum_{I\subset\{1,\dots,n\}} (-1)^{n-|I|}\mathrm{Vol}\left(\sum_{i\in I} Q_i\right).$$

Lemme 2.11 *Le volume mixte de n polytopes entiers en dimension n prend des valeurs dans $\mathbb{Z}_{\geq 0}$, il est symétrique, invariant sous translations, invariant sous rotations qui préservent le volume ($SL_n(\mathbb{Z})$), multi-linéaire :*

$$VM(Q_1,\dots,\mu Q_k+\rho Q'_k,\dots,Q_n) = \mu VM(Q_1,\dots,Q_k,\dots,Q_n)+\rho VM(Q_1,\dots,Q'_k,\dots,Q_n), \qquad \mu,\rho\in\mathbb{R}_{\geq 0},$$

et satisfait : $VM(Q_1,\dots,Q_1) = n!\,\mathrm{Vol}(Q_1)$.

Exercice 2.12 Démontrez le lemme en considérant les coefficients de $\lambda_1\cdots\lambda_k\cdots\lambda_n$ et $\lambda_1\cdots\lambda'_k\cdots\lambda_n$ dans $\mathrm{Vol}(\lambda_1 Q_1+\cdots+\lambda_k Q_k+\lambda'_k Q'_k+\cdots+\lambda_n Q_n)$. Soit $S\subset\mathbb{R}^n$ la simplexe standard, aux sommets $\{(0,\dots,0),(1,0,\dots,0),\dots,(0,\dots,0,1)\}\subset\mathbb{Z}^n$. Utilisez le lemme pour montrer que $VM(d_1S,\dots,d_nS) = \prod_i d_i$. □

Définition 2.13 *Un* complexe polyédrique *est un ensemble de polyèdres, qui s'appellent* cellules *(ou faces), t.q. l'intersection de deux cellules est une face de chacune de deux cellules et aussi une cellule du complexe. Une* subdivision *d'un polyèdre est un complexe polyédrique dont l'union des cellules est P.*

La subdivision où chaque cellule est un simplexe est une triangulation. *L'enveloppe inférieure* d'un polyèdre $P\subset\mathbb{R}^k$ est l'union des facettes dont la dernière (k-ème) coordonnée de la normale sortante (resp. rentrante) est négative (positive).

Un *relèvement* est spécifié par les fonctions $l_i : \mathbb{Z}^n \to \mathbb{Q}$, $i = 1,\dots,n$, On obtient un relèvement *linéaire* si $l_1,\dots,l_n\in\mathbb{Z}[x_1,\dots,x_n]$ sont des *formes linéaires*, ou des vecteurs en $\mathbb{Z}^n$ (alors l'évaluation des l_i se réduit à un produit scalaire). Pour un ensemble de points A_i et son enveloppe convexe Q_i, $\widehat{A}_i = \{(a, l_i(a)) : a\in A_i\}\subset\mathbb{Q}^{n+1}$ et $\widehat{Q}_i = \mathrm{Conv}(\widehat{A}_i)$. Pour un relèvement linéaire, $\widehat{Q}_i\subset\mathbb{R}^{n+1}$ est de dimension $\dim(Q_i)$, $i = 1,\dots,n$. Les relèvements (surtout linéaires) vont jouer un rôle central en la démonstration de certains théorèmes ci-dessous, ainsi que dans la construction des matrices du résultant creux.

Exercice 2.14 Suite à l'exercice 2.8, soient $A_1 = \{(0,0),(1,0),(2,0)\}, A_2 = \{(0,0),(0,1),(0,2)\}$. Calculez leur volume mixte d'après lemme 2.18 en utilisant un relèvement linéaire et un relèvement non-linéaire. Choisissez ce dernier de telle façon afin d'obtenir une seule cellule mixte. Généralisez dans le cas $A_i\subset\mathbb{Z}^n$ avec $|A_i| > 2$ et $\dim(Q_i) = 1$, $i = 1,\dots,n$. Calculez $VM(Q_1,\dots,Q_n)$ par un relèvement linéaire et un non-linéaire qui donne une seule cellule. □

L'enveloppe inférieure de la somme $\widehat{Q} = \widehat{Q}_1+\cdots+\widehat{Q}_n$ est une surface polyédrique de dimension n qui se projette, de manière bijective, sur Q. Les faces de l'enveloppe se projettent sur les cellules de la subdivision et la dimension de la cellule ne depasse pas celle de la face.

Définition 2.15 *La projection canonique $\pi : \mathbb{R}^{n+1}\to\mathbb{R}^n$ de l'enveloppe inférieure de $\widehat{Q}$ définie une subdivision, dite* induite, *de la somme de Minkowski $Q_1+\cdots+Q_n$. La subdivision induite s'appelle* exacte *("tight") ssi chaque face de l'enveloppe inférieure se projette sur une cellule de le même dimension.*

Une subdivision est cohérente (ou régulière) *si, pour une fonction linéaire sur $\mathbb{R}^{n+1}$, son minimum sur $\pi^{-1}(x)$, pour tout $x\in Q$, est atteint sur la facette $\widehat{F}$ de $\widehat{Q}$, où $x\in\pi(\widehat{F})$. De manière équivalente, il existe une fonction concave, linéaire par morceaux sur la subdivision, telle que les domaines de linéarité coincident avec les cellules [GKZ94, sec.7.1.C].*

Ici cette fonction est la $(n+1)$-ème coordonnée, donc la subdivision induite est cohérente. On pourrait projeter l'enveloppe supérieure pour définir une (autre) subdivision induite, alors la fonction minimisée serait l'inverse de la $(n+1)$-ème coordonnée. La cohérence garantie la continuité et l'unicité requises par la définition 2.17. Si le relèvement est suffisamment générique, la subdivion est exacte donc les facettes de l'enveloppe se projettent sur les cellules maximales de la subdivision.

Exemple 2.16 La projection des arêtes $\{(0,1),(1,2)\}$ et $\{(2,1),(1,0)\}$ du carré $\{(0,1),(1,2),(2,1),(1,0)\}$ donne une subdivision du segment $\{(0,0),(2,0)\}$ mais pas induite ni cohérente. Par contre, la projection de l'enveloppe inférieure est induite et cohérente. □

Définition 2.17 *Étant donnés polytopes $Q_1,\ldots,Q_k \subset \mathbb{R}^n$ pour n'importe quel $k \in \mathbb{N}$, une subdivision* mixte *de la somme (de Minkowski) $Q = Q_1 + \cdots + Q_k$ est une subdivision cohérente et exacte de Q où chaque cellule σ de dimension maximale n s'exprime comme une somme (de Minkowski) de faces $F_i \subset Q_i$ telles que :*

$$\sigma = F_1 + \cdots + F_k \Rightarrow \dim\sigma = \dim F_1 + \cdots + \dim F_k = n.$$

Cette dernière expression sera unique et aussi "continue" : $\sum_i F'_i \subset \sigma \Rightarrow F'_i \subset F_i$.

Lemme 2.18 *Soit Δ une subdivision mixte de la somme (de Minkowski) $Q = Q_1 + \cdots + Q_k$, pour $k \geq n$, d'après la définition 2.17. Pour tout sous-ensemble de n polyèdres Q_i,*

$$VM(Q_1,\ldots,Q_n) = \sum_\sigma \mathrm{Vol}(\sigma), \qquad \dim\sigma = n, \sigma = \sum_{i=1}^{k} E_i \in \Delta, \dim E_i \leq 1, E_i \subset Q_i, i = 1,\ldots,k.$$

Preuve Considérons la subdivision mixte de $\lambda_1 Q_1 + \cdots + \lambda_k Q_k$, $\lambda_i \geq 0$, analogue à Δ, et soit σ_λ une de ses cellules maximales égale à la somme de n arêtes. Alors $\mathrm{Vol}(\sigma_\lambda) = \lambda_1 \cdots \lambda_n \mathrm{Vol}(\sigma)$; ces cellules contribuent au coefficient multi-linéaire du polynôme homogène (de degré n) $\mathrm{Vol}(\lambda_1 Q_1 + \cdots + \lambda_k Q_k)$ et donc au volume mixte. Par contre, les cellules qui ne sont pas la somme de n arêtes ne contribuent pas à ce coefficient multi-linéaire. □

Algorithme 2.19 *Une façon de construire une subdivision mixte est comme une subdivision induite définie par un relèvement linéaire* suffisamment générique. *La condition de généricité demande que, pour toute cellule maximale $\sigma = \sum_i F_i$, où $F_i = \pi(\widehat{F_i})$, $\dim \sum_i \widehat{F_i} = n$. Cette condition se traduit au fait que certains déterminants en les coordonnées de points relevés doivent être non-nuls [HS97].*

Pour deux ensembles différents $\{p_1,\ldots,p_n\} \neq \{q_1,\ldots,q_n\}$ de sommets *$p_i, q_i \in Q_i$ qui engendrent des sommes égales $\sum_i p_i = \sum_i q_i$ en Q, la condition de généricité implique que, si une des sommes relevées se trouve sur l'enveloppe inférieure, l'autre ne s'y trouve pas, c.à.d. $\sum_{i=1}^n \widehat{p}_i \neq \sum_{i=1}^n \widehat{q}_i \in \widehat{Q}$.*

Exemple 2.20 $f_1 = c_{10} + c_{11}xy + c_{12}x^2y + c_{13}x$, $f_2 = c_{20} + c_{21}y + c_{22}xy + c_{23}x$ ont des polytopes de Newton et une subdivision mixte montrés en figure 1. Un relèvement qui donne cette subdivision serait : $l_1 = -x - 2y, l_2 = 4x + y$. □

Exemple 2.21 Augmentons le système de l'exemple précédant :

$$f_0 = c_{00} + c_{01}xy + c_{02}x^2y + c_{03}x,\ f_1 = c_{10}y + c_{11}x^2y^2 + c_{12}x^2y + c_{13}x,\ f_2 = c_{20} + c_{21}y + c_{22}xy + c_{23}x.$$

Pour un relèvement linéaire $l_1(x,y) = Lx + L^2y, l_2(x,y) = -L^2x - y, l_3(x,y) = x - Ly$, avec $L \gg 0$ suffisamment large, les polytopes de Newton relevés et l'enveloppe inférieure de leur somme, tous en $\mathbb{R}^3$, sont montrés en figure 2. À cause de la linéarité du relèvement, les $\widehat{Q}_i$ sont plats. La triangulation de l'enveloppe inférieure est dû au programme de calcul des enveloppes et n'est pas significatif ici. □

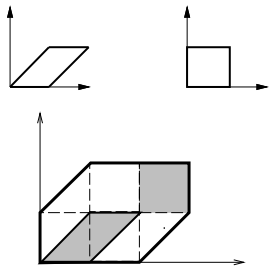


FIG. 1 – Les Q_1, Q_2 et leur somme avec une subdivision mixte où les cellules noires sont copies de Q_1, Q_2 et les cellules mixtes sont blanches ; $VM(Q_1, Q_2) = 3$.

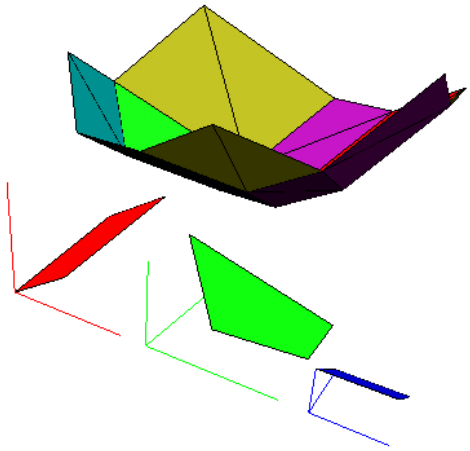


FIG. 2 – Vue perspective des polytopes de Newton relevés et de l'enveloppe inférieure de leur somme.

Exercice 2.22 Bornez la probabilité que la subdivision induite par un relèvement linéaire ne soit pas mixte quand les coefficients des l_i sont distribués uniformément sur $[0, L]$. □

Exercice 2.23 Soient Q_1, Q_2 les enveloppes convexes de

$$A_1 = \{(2,2),(2,0),(0,2),(1,1),(0,0)\},\ \ A_2 = \{(1,1),(1,0),(0,1),(0,0)\}.$$

(1) Dessiner Q_1, Q_2. (2) Calculer la borne de Bézout aussi que le volume mixte du système (A_1, A_2) en appliquant la formule d'exclusion-inclusion. (3) Construire la somme de Minkowski $Q = Q_1 + Q_2$ et une subdivision mixte de Q. Identifier les cellules mixtes et calculer $VM(A_1, A_2)$ comme une somme des volumes des cellules mixtes.

Faites les mêmes étapes pour les Q_i donnés par leurs sommets : ceux de Q_1 sont $\{(0,0),(0,1)\}$ et de Q_2 sont $\{(0,0),(1,1),(2,1),(1,0)\}$. Vous pouvez réduire le calcul au calcul des $VM(Q_1, e_1) = 1$, $VM(Q_1, e_2) = 1$, où $e_1 = ((0,0),(1,1))$ et $e_2 = ((0,0),(1,0))$. □

Étant donnée la somme de Minkowski des polytopes relevés, une partie de son enveloppe inférieure (c.à.d. les cellules maximales qui sont des sommes d'arêtes) contient toute l'information pour le volume mixte. Le lemme suivant accélère le calcul considérablement.

Lemme 2.24 (Élaguer) *Supposons qu'on applique un certain relèvement aux polytopes donnés. Pour tout $J \subset \{1, \ldots, n\}$, et tout $T \subset J$, si $\sum_{j\in J} \widehat{e}_j$ se trouve sur l'enveloppe inférieure de $\sum_{j\in J} \widehat{Q}_j$ alors $\sum_{t\in T} \widehat{e}_t$ se trouve sur l'enveloppe inférieure de $\sum_{t\in T} \widehat{Q}_t$.*

Preuve L'hypothèse est équivalente au fait que $\sum_j l_j(e_j/2) = \min\{\sum_j l_j(p_j) : p_j \in Q_j, \sum_j p_j = \sum_j e_j/2\}$, $e_j/2$ étant le point au milieu de l'arête e_j. Cela implique $\sum_t l_t(e_t/2) = \min\{\sum_t l_t(p_t) : T \subset J, \sum_t p_t = \sum_t e_t/2\}$, qui est équivalent à la conclusion. □

On définie une condition nécessaire pour qu'un ensemble d'arêtes appartienne à un ensemble définissant une cellule mixte. Pour un relèvement fixe, $(e_1, \ldots, e_k)$ est un *candidat-mixte* ssi la somme $\sum_{i=1}^k \widehat{e}_i$ se trouve sur l'enveloppe inférieure de $\sum_{i=1}^k \widehat{Q}_i$.

Exercice 2.25 Décrire un test sur $(e_1, \ldots, e_k)$ qui décide si la suite est un candidat-mixte, en exécutant un seul programme linéaire. □

Algorithme 2.26 (Calcul du *VM*) *Entrée : $Q_1, \ldots, Q_n \subset \mathbb{R}^n$ aux sommets entiers.*
Sortie : $VM(Q_1, \ldots, Q_n) \in \mathbb{Z}_{\geq 0}$.
Description :
1. Calculer les ensembles des arêtes $E_1, \ldots, E_n$.
2. Choisir un relèvement linéaire $l_1, \ldots, l_n \in \mathbb{Z}[x_1, \ldots, x_n]$ au hasard.
3. Appliquer l'algorithme VM-contraint ci-dessous sur $(E_1, \ldots, E_n)$.

Algorithme 2.27 (*VM*-contraint) *Entrée : $(e_1, \ldots, e_k, E'_{k+1}, \ldots, E'_n)$, $0 \leq k \leq n$, $e_i \in E_i$, $E'_j \subset E_j, j > k$.*
Sortie : $\sum \mathrm{Vol}(\sigma)$ sur toute cellule mixte (par rapport au relèvement choisi) $\sigma = e_1 + \cdots + e_k + e'_{k+1} + \cdots + e'_n$, $\exists e'_j \in E'_j$, $j > k$.
Description :
1. Si $k = n$ et $(e_1, \ldots, e_n)$ est un candidat-mixte, alors la séquence est mixte et l'algorithme termine et envoie $VM(e_1, \ldots, e_n)$.
2. Si $k = n$ mais $(e_1, \ldots, e_n)$ n'est pas un candidat-mixte l'algorithme termine et envoie 0.
3. Si $k < n$ on initialise vmc à 0. Pour chaque $e'_{k+1} \in E'_{k+1}$ tel que $(e_1, \ldots, e_k, e'_{k+1})$ est candidat-mixte, vmc := vmc + VM-contraint $(e_1, \ldots, e_k, e'_{k+1}, E'_{k+2}, \ldots, E'_n)$. L'algorithme termine en envoyant vmc.

Le logiciel Relever-Élaguer ("Lift-Prune") [EC95], accessible sur la page Web de l'auteur, calcule les cellules mixtes. Pour le "benchmark" des racines cycliques de l'unité (voir sect. 8.3) l'implémentation de l'algorithme 2.27 a calculé les premières bornes pour $n = 9, 10, 11$.

Exercice 2.28 Soit P^v la face de polytope P définie par un vecteur $v \in \mathbb{Z}^n$.

$$VM(Q_1, \ldots, Q_n) = \sum_v (v, Q_1) VM'(Q_2^v, \ldots, Q_n^v)$$

pour toute normale v rentrante de Q_1 qui définit des faces Q_i^v de dimension ≥ 1 pour $i = 2, \ldots, n$. Le produit scalaire (minimale) de v sur Q_1 est (v, Q_1). $VM'(\cdot)$ est le volume mixte *normalisé*, égal à $VM(Q_2^v, \ldots, Q_n^v)/\mathrm{Vol}_{n-1}(P)$ si P est le parallélotope fondamental de l'hyperplan perpendiculaire à v. □

Une question importante dans le calcul de complexité en élimination creuse est la relation entre volume mixte et le volume de la somme de Minkowski, puisque le premier exprime la complexité intrinsèque et du deuxième dépend la complexité des algorithmes. La discussion suivante résume les résultats de [Emi96], basés sur l'inégalité célèbre d'Aleksandrov-Fenchel (1935-6) :

Proposition 2.29 (Aleksandrov-Fenchel)

$$VM^2(Q_1, Q_2, Q_3, \ldots, Q_n) \geq VM(Q_1, Q_1, Q_3, \ldots, Q_n) VM(Q_2, Q_2, Q_3, \ldots, Q_n).$$

Lemme 2.30

$$VM^n(Q_1,\ldots,Q_n) \geq (n!)^n \prod_{i=1}^{n} \mathrm{Vol}(Q_i).$$

Preuve Nous commençons avec une (grande) puissance de $VM(Q_1,\ldots,Q_n)$ et nous appliquons l'inégalité d'Aleksandrov-Fenchel (proposition 2.29) plusieurs fois afin d'obtenir une expression à droite qui inclut seulement les $VM(Q_i,\ldots,Q_i)$ pour $i=1,\ldots,n$. Puisque l'inégalité d'Aleksandrov-Fenchel utilise deux volumes mixtes de chaque côté, son application produit des nouvelles inégalités avec le même nombre de volumes mixtes de chaque côté.

Deuxièmement, chaque fois que l'inégalité est appliquée, l'expression à droite inclut de volumes mixtes moins "mixtes", c.à.d. dont le nombre de Q_i distincts décroît. Eventuellement, donc, on arrivera au produit $\prod_i VM(Q_i,\ldots,Q_i)$. □

En 2009, nous avons découvert un énnoncé plus général de l'inégalité d'Aleksandrov-Fenchel :

$$VM^k(Q_1,\ldots,Q_n) \geq \prod_{i=1}^{k} VM(Q_i,\ldots,Q_i,Q_{k+1},\ldots,Q_n).$$

Corollaire 2.31 *Soit* $\mathrm{Vol}(Q_\mu)$ *le volume minimal, alors le* facteur scalaire du système *est le réel minimum* $s \geq 1$ *t.q.* $Q_i \subset sQ_\mu$, $\forall i$. *Soit* e *la base des logarithmes naturels et supposons que* $\mathrm{Vol}(Q_\mu) > 0$.

$$\frac{\mathrm{Vol}\left(Q_1+\cdots+Q_n\right)}{VM(Q_1,\ldots,Q_n)} = O\left(\frac{e^n s^n}{\sqrt{n}}\right).$$

Définissons Q_μ *et* s *de manière analogue pour un système de* $n+1$ *polynômes en* n *variables. Si* $\mathrm{Vol}(Q_\mu) > 0$ *et* $VM_{-i} = VM(Q_0,\ldots,Q_{i-1},Q_{i+1},\ldots,Q_n)$,

$$\mathrm{Vol}\left(Q_0+\cdots+Q_n\right) = O\left(\frac{e^n s^n}{n} \sum_{i=0}^{n} VM_{-i}\right).$$

Une autre propriété des volumes mixtes est la suivante :

Exercice 2.32 Soient polytopes $P_1,\ldots,P_k \subset \mathbb{R}^{m+k}$ et $Q_1,\ldots,Q_m \subset \mathbb{R}^m$ dont les coordonnées sont réelles (et pas forcement entières), alors :

$$VM_{m+k}(P_1,\ldots,P_k,Q_1,\ldots,Q_m) = VM_m(Q_1,\ldots,Q_m)VM_k(P'_1,\ldots,P'_k),$$

où P'_i est la projection de P_i dans $\mathbb{R}^k$ et VM_i est le volume mixte en $\mathbb{R}^i$. □

2.1 Majoration du nombre de racines communes

Pour le reste des notes, K est un corps de caractéristique zéro et $\overline{K}$ est sa clôture algébrique. Rappelons deux théorèmes classiques.

Théorème 2.33 (Borne de Bézout homogène) *Soient* $f_1,\ldots,f_n \in K[x_0,x_1,\ldots,x_n]$ *homogènes et soit* d_i *le degré total de* f_i. *Le nombre de racines isolées dans* $\mathbb{P}^n$ *est borné par* $\prod_{i=1}^n d_i$. *Pour de coefficients génériques (intersection complète) cette borne est exacte.*

Définition 2.34 *Un polynôme est* multi-homogène *en les paquets de variables* $X_1,\ldots,X_r$ *ssi il est séparément homogène en chaque paquet.*

Chaque polynôme multi-homogène de degré d_i en les X_i est aussi homogène de degré $\sum_i d_i$.

Théorème 2.35 (Borne de Bézout multi-homogène) *Soient $f_1, \ldots, f_n$ multi-homogènes en $X_1, \ldots, X_r$, où le paquet X_i contient $l_i + 1$ variables en total et $n = \sum_i l_i$. Soit d_{ij} le degré de f_i en X_j. Le nombre de racines isolées dans $\mathbb{P}^{l_1} \times \cdots \times \mathbb{P}^{l_r}$ est borné par*

$$\textit{le coefficient de } \prod_{j=1}^{r} y_j^{l_j} \textit{ dans le polynôme } \prod_{i=1}^{n} \sum_{j=1}^{r} d_{ij} y_j.$$

Pour de coefficients génériques cette borne est exacte.

Exemple 2.36 Le polynôme $f = c_{110}x_1x_2y_0 + c_{201}x_1^2y_1 + c_{111}x_1x_2y_1 + c_{001}x_0^2y_1$ est multi-homogène en les paquets $X_1 = (x_0, x_1, x_2)$, $X_2 = (y_0, y_1)$, $r = 2$, où $l_1 = 2, l_2 = 1$ et $d_1 = 2, d_2 = 1$. □

La *théorie de l'élimination creuse* associe à chaque polynôme son polytope de Newton qui offre une notion plus générale ainsi que plus précise que celle du degré total.

Définition 2.37 *Le* support *A_i d'un polynôme $f_i \in K[x_1^{\pm 1}, \ldots, x_n^{\pm 1}]$ est l'ensemble des exposants en $\mathbb{Z}^n$ correspondant aux coefficients non-nuls, c.à.d. $f_i = \sum_{a \in A_i} c_a x^a$, $c_a \neq 0$. Le* polytope de Newton *Q_i de f_i en $\mathbb{R}^n$ est l'enveloppe convexe de A_i.*

Notons que $\mathrm{supp}(fg) \subset \mathrm{supp}(f) + \mathrm{supp}(g)$, $\mathrm{supp}(f + g) \subset \mathrm{supp}(f) \cup \mathrm{supp}(g)$. Le polytope de Newton de fg est la somme des polytopes de Newton de f et g.

Exercice 2.38 Soit $f \in K[x]$ un polynôme avec un segment de Newton Q. Si ses coefficients sont génériques, le nombre de ses racines isolées, comptant les multiplicités, dans $(\overline{K}^*)^n$ est égal à la longueur de Q, c.à.d. $VM(Q)$. □

On peut observer que le volume mixte de n polytopes de Newton change comme le nombre générique de racines communes du système polynomial correspondant. Nous allons formaliser cette observation, en commençant avec le cas $A_1 = \cdots = A_n$, établi par Kushnirenko [Kus75]. Si $|A_1| = n + 1$, la preuve revient à celle du théorème 2.41 en utilisant une forme de Smith ou une forme de Hermite.

Exercice 2.39 Continuons avec le cas $A_1 = \cdots = A_n \subset \mathbb{Z}^n$. Si $\dim Q_1 < n$, alors il n'y a pas de solution isolée dans $(\overline{K}^*)^n$, commune aux polynômes $f_1, \ldots, f_n \in K[x, x^{-1}]$ aux coefficients génériques. □

Lemme 2.40 *Finissons avec le cas $A_1 = \cdots = A_n$. Si $\dim(Q_1) = n$ et les coefficients sont génériques, alors le nombre de solutions communes isolées dans $(\overline{K}^*)^n$ est égal à $VM(Q_1, \ldots, Q_1)$.*

Preuve Ici nous indiquons ce qui serait différent par rapport à la preuve du théorème 2.41 ci-dessous. Nous utilisons un relèvement non-linéaire et suffisamment générique de Q_1. La projection de l'enveloppe inférieure triangularise Q_1. En passant par les séries de Puiseux, comme dans la preuve du théorème 2.41, nous arrivons à considérer des sous-systèmes correspondants à chaque facette de $\widehat{Q}_1$.

Par la généricité du relèvement, la facette est définie par $\leq n + 1$ sommets. Si elle est définie par $\leq n$ sommets, cela nous amène à un système équivalent de n équations en $\leq n - 1$ variables z_i, qui ne peut pas avoir de solution isolée. Donc $n + 1$ sommets définissent la facette et on revient au cas d'un système avec $n + 1$ points de support ($|A_1| = n + 1$). □

Khovanskii a raffiné la version initiale du théorème pour prendre en compte le cas de composantes de l'ensemble de zéros avec une dimension positive [Kho78]. Pour reconnaître ces trois contributions principales, le théorème est aussi connu comme BKK :

Théorème 2.41 [Ber75] *Pour le système $f_1, \ldots, f_n \in K[x, x^{-1}]$, le nombre de solutions communes isolées dans $(\overline{K}^*)^n$, comptant les multiplicités, est borné par le volume mixte des polytopes de Newton $VM(Q_1, \ldots, Q_n)$. Si les coefficients sont suffisamment génériques, cette borne est exacte.*

Preuve Nous considérons le cas de coefficients génériques, ce qui donne la borne supérieure pour le cas arbitraire et démontre aussi la deuxième conclusion. Supposant que les supports sont translatés pour appartenir à $\mathbb{N}^n$. Le relèvement, défini par les $l_i : A_i \to \mathbb{Z}$, correspond à la définition de polynômes

$$f_i'(x,t) = \sum_{a\in A_i} c_{ia} x^a t^{l_i(a)} \in K[x_1^{\pm 1}, \ldots, x_n^{\pm 1}](t), \quad 0 < t \leq 1,$$

dont le polytope de Newton est $\widehat{Q}_i \in \mathbb{R}^{n+1}$. Quand $1 \gg t > 0$ on a le système initial de l'homotopie, qui serait plus façila à résoudre en fonction de t. Quand $t = 1$ on récupère le système donné, dont le nombre de racines est borné par celui du système initial. Avec des coefficients génériques (le Jacobien est non nul) nous pouvons écrire les racines comme des séries de Puiseux, c.à.d. aux exposants rationnels. Notons que, puisque $\overline{K}$ est algébriquement clos, le corps des séries de Puiseux $\overline{K}((t))$ est algébriquement clos :

$$x(t) = (\alpha_1 t^{\lambda_1}, \ldots, \alpha_n t^{\lambda_n}) + \text{ termes d'ordre supérieur}, \quad \alpha_i \in \overline{K}^*, 1 \gg t > 0,$$

et $\lambda \in \mathbb{Q}^n$ minimal parmi tous les termes. Nous substituant $x(t)$ dans f_i', alors :

$$f_i' = \sum_{a\in A_i} c_{ia} \alpha^a t^{(\lambda,a)+l_i(a)} + \text{ termes d'ordre supérieur},$$

où l'exposant s'écrit $((\lambda, 1), \widehat{a})$, $\widehat{a} = (a, l_i(a)) \in \mathbb{R}^{n+1}$. Considérons le vecteur $(\lambda, 1) \in \mathbb{R}^{n+1}$ comme une normale rentrante, il spécifie une face $\sum_i \widehat{F}_i \subset \widehat{Q}$, et les faces $\widehat{F}_i \subset \widehat{Q}_i$, $i = 1, \ldots, n$.

Maintenant nous démontrons que chaque F_i est une arête. Pour qu'il soit possible de résoudre les équations f_i, il faut calculer chaque α afin de calculer les branches $x(t)$ de manière itérative. La détermination de α demande la résolution des équations $I_i = \sum_{a\in F_i} c_{ia}\alpha^a$. Si $\dim F_i = 0$, alors ce polynôme contient un seul monôme, n'a aucun zéro dans $(\overline{K}^*)^n$ pour des coefficients génériques et $\sum_i F_i$ contribue rien au volume mixte. Alors $\dim F_i \geq 1$ pour $i = 1, \ldots, n$. Mais $\sum_i \dim F_i = \dim \sum_i F_i \leq n$ puisqu'elle est la dimension d'une cellule dans la subdivision mixte induite par les l_i. Cela implique que $\dim F_i = 1$, $i = 1, \ldots, n$.

Il suffit de montrer que le nombre de racines communes du système $I_1 = \cdots = I_n = 0$ est égal à $VM(F_1, \ldots, F_n) = \mathrm{Vol}(\sum_i F_i)$, qui est donné, d'après l'exercice 2.8, par le déterminant de la matrice dont les colonnes (ou lignes) expriment les vecteurs F_i. L'exercice 2.44 traite le cas de $|F_i| > 2$ (relèvement non-linéaire). Nous supposons donc que chaque I_i est un binôme, alors il s'écrit $I_i : c_i x^{a_i} = 1$, pour un coefficient générique c_i. Soit $A = [a_1, \ldots, a_n]$ la matrice $n \times n$ dont les colonnes correspondent aux a_i. Sa forme normale de Hermite (transposée) est

$$AV = \begin{bmatrix} H_{11} & & 0 \\ \vdots & \ddots & \\ H_{n1} & \ldots & H_{nn} \end{bmatrix}, \qquad H_{(i-1)(i-1)} | H_{ii},\ V \in \mathbb{Z}^{n\times n} : \det V \in \{-1, 1\}, \text{c.à.d. } V \in \mathrm{SL}_n(\mathbb{Z}).$$

Le système suivant est équivalent (voir exercice 2.42), défini par V, et triangulaire :

$$\prod_{k=1}^{n} (c_k x^{a_k})^{V_{kj}} = c_j' \prod_{i=1}^{n} x_i^{H_{ij}} = 1, \qquad j = 1, \ldots, n. \tag{2}$$

Sa résolution commence avec la n-ème équation qui ne contient que x_n, donnant H_{nn} racines. La spécialisation de la $(n-1)$-ème équation à chacune racine donne $H_{(i-1)(i-1)}$ racines pour x_{n-1}. Ainsi nous calculons toutes les solutions communes sont dans $(\overline{K}^*)^n$ et leur cardinal est de $|H_{11} \cdots H_{nn}| = |\det(AV)| = |\det A|$. Si $\exists H_{ii} = 0 \Rightarrow$ la i-ème équation n'a aucune solution dans $(\overline{K}^*)^n$ donc le système n'a pas de solutions communes. □

La dernière étape s'effectue aussi par le biais de la forme normale de Smith de A :

$$UAV = \begin{bmatrix} s_1 & & 0 \\ & \ddots & \\ 0 & & s_n \end{bmatrix}, \qquad s_{i-1}|s_i,\ U,V \in \mathbb{Z}^{n\times n} : \det U, \det V \in \{-1,1\}, \text{c.à.d. } U,V \in \mathrm{SL}_n(\mathbb{Z}).$$

U définie un changement de variables $x_i = z_1^{U_{1i}} \cdots z_n^{U_{ni}}$, alors $I_i : c_i z^{Ua_i} = 1$. Un système équivalent est défini à partir de l'application inversible V :

$$\prod_{i=1}^{n} \left(c_i z^{Ua_i}\right)^{V_{ij}} = c'_j z_j^{s_j} = 1, \qquad j = 1,\ldots,n.$$

dont toutes les équations contiennent exactement une variable. Si $\exists s_i = 0 \Rightarrow$ le système n'a pas de solution, sinon il y a $|s_1 \cdots s_n| = |\det(UAV)| = |\det A|$ solutions dans $(\overline{K}^*)^n$.

Exercice 2.42 Soit le système $I_i : c_i x^{a_i} = 1$, $i = 1,\ldots,n$ et $A = [a_1,\ldots,a_n]$ la matrice $n \times n$ dont les colonnes sont les $a_i \in \mathbb{Z}^n$. Soit $AV = H$ sa forme de Hermite, où $\det V \in \{-1,1\}$. Montrez que le système suivant est équivalent :

$$G_j = \prod_{k=1}^{n} \left(c_k x^{a_k}\right)^{V_{kj}} = c'_j \prod_{i=1}^{n} x_i^{H_{ij}} = 1, \qquad j = 1,\ldots,n.$$

□

Exemple 2.43 Substituant $x = \alpha t^{\lambda}$ dans les polynômes relevés de l'exemple 2.20, nous avons

$$c_{10}+c_{11}\alpha^{(1,1)}t^{-3+\lambda_1+\lambda_2}+c_{12}\alpha^{(2,1)}t^{-4+2\lambda_1+\lambda_2}+c_{12}\alpha^{(1,0)}t^{-1+\lambda_1}, c_{20}+c_{21}\alpha^{(0,1)}t^{1+\lambda_2}+c_{22}\alpha^{(1,1)}t^{5+\lambda_1+\lambda_2}+c_{22}\alpha^{(1,0)}t^{4+\lambda_1}.$$

Prenons la cellule mixte la plus à droite dans la subdivision mixte de la figure 1, la normale rentrante est $(-4,7,1) \Rightarrow \lambda = (-4,7)$. Pour $t \to 0$, les polynômes deviennent

$$c_{10} + c_{11}\alpha^{(1,1)} + c_{12}\alpha^{(2,1)}t^{-5} + c_{12}\alpha^{(1,0)}t^{-5}, c_{20} + c_{21}\alpha^{(0,1)}t^{8} + c_{22}\alpha^{(1,1)}t^{8} + c_{22}\alpha^{(1,0)}.$$

Nous pouvons poser $I_1 : c_1x_1x_2 = 1, I_2 : c_2x_1 = 1$. Les formes de Hermite et de Smith s'obtiennent comme :

$$\begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} 1 & 1 \\ 0 & -1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \text{ et } \begin{bmatrix} 1 & 0 \\ -1 & 1 \end{bmatrix}\begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} 1 & 1 \\ 0 & -1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}.$$

La première définit le système triangulaire $c'_1x^{(1,1)1+(1,0)0} = c'_1x_1x + 2 = 1$ et $c'_2x^{(1,1)1+(1,0)-1} = c'_2x_2 = 1$. La forme de Smith spécifie $x_1 = z_1z_2^{-1}, x_2 = z_2, x_1x_2 = z^{(1,0)}, x_1 = z^{(1,-1)}$ ce qui donne le système $c'_1z_1 = c'_2z_2 = 1$ avec une seule solution dans $(\overline{K}^*)^2$.

Pour la cellule mixte la plus à gauche, la normale rentrante est $(4,-1,1) \Rightarrow \lambda = (4,-1)$. Pour $t \to 0$, les polynômes deviennent

$$c_{10} + c_{11}\alpha^{(1,1)} + c_{12}\alpha^{(2,1)}t^{3} + c_{12}\alpha^{(1,0)}t^{3}, c_{20} + c_{21}\alpha^{(0,1)} + c_{22}\alpha^{(1,1)}t^{8} + c_{22}\alpha^{(1,0)}t^{8}.$$

Cela donne un autre système binomial avec une autre solution dans $(\overline{K}^*)^2$. □

Exercice 2.44 Si $\dim Q_i = 1, Q_i \subset \mathbb{R}^n$, $i = 1,\ldots,n$, et $|A_i| > 2$ pour quelque $i \in \{1,\ldots,n\}$, complétez la preuve du théorème 2.41 en se ramenant au cas où $|A_i| = 2$ pour tout i. Vous pouvez utilisez un relèvement non-linéaire, comme dans la preuve du lemme 2.40, et l'exercice 2.14. □

Exercice 2.45 Si, pour un degré fixe, tous les monômes possibles, par rapport au degré total de chaque polynôme, ont un coefficient non-nul, les polynômes sont complètement denses et on retrouve la borne classique du théorème de Bézout (exercice 2.12). Si le système est dense multi-homogène, le volume mixte donne la borne de Bézout multi-homogène (theorème 2.35). □

La preuve de la majoration du nombre de racines définie un système de départ par cellule maximale mixte pour qu'une homotopie de continuation (creuse) puisse approcher numériquement toutes les racines communes [HS97].

Exercice 2.46 Il y a d'homotopies "simultanées" (à la Weierstrass) qui peuvent suivre toutes les racines à la fois, donc il n'est pas désirable d'avoir plusieurs sous-systèmes, chacun correspondant à un sous-ensemble des racines, comme ici. Est-il possible dans le cadre creux de définir un seul système de départ ? □

Exemple 2.47 Valeurs et vecteurs propres : $Av = \lambda v$, A est une matrice $n \times n$, $v \in \mathbb{C}^n : \|v\| = 1$, $\lambda \in \mathbb{C}$. Nb pairs $(\lambda, v) = VM = 2n \ll$ borne de Bézout $= 2^{n+1}$. Idem pour les valeurs et vecteurs propres généralisés $Av = \lambda Bv$ avec B une matrice $n \times n$.

La géométrie directe de la plate-forme parallèle de Gough/Stewart : Nb maximal d'orientations réelles $= 40 < VM = 54 <$ borne de Bézout $= 256$.

Nombre de plongements Euclidiens de graphes rigides [EV09]. Pour $n = 5, 6, 7$ sommets dans $\mathbb{R}^2$, le VM donne des bornes exactes $= 8, 32, 64$ tandis que celles de Bézout sont 4^n. Pareil pour $n = 5, 6$ sommets (qui admettent un plongement convexe) dans $\mathbb{R}^3$; le nombres exacts sont donnés par les $VM = 8, 16$ tandis que les bornes de Bézout sont 8^n. □

Canny et Rojas ont montré qu'il suffit d'avoir des coefficients génériques aux monômes extrèmes pour que le VM donne exactement le nombre de racines toriques. Nous citons sans preuve le Second Théorème de Bernstein qui revient sur cette question d'optimalité :

Théorème 2.48 *Soit $A = \mathrm{supp}(f) \in \mathbb{Z}^n, I_v(f) = \sum_{a \in A \cap F} c_a x^a$ où F est la face du polytope de Newton de f définie par la normale v. Si, pour tout $v \in \mathbb{R}^n$, les $I_v(f_1), \ldots, I_v(f_n)$ n'ont aucune solution commune dans $(\overline{K}^*)^n$, alors le nombre de racines isolées des $f_1, \ldots f_n$ est égal au $VM(Q_1, \ldots Q_n)$ [Ber75]. Il suffit de considérer les normales aux facettes de la somme de Minkowski $\sum_{i=1}^n Q_i$ [HS95].*

De point de vue algorithmique, il suffit de tester les facettes mixtes parceque les autres auront toutes au moins un sommet dans leur écriture comme somme de Minkowski, alors $I_v(f_i)$ est un monôme, et il n'a pas de solution dans $(\overline{K}^*)^n$.

Exercice 2.49 Les page Web de l'auteur contiennent le logiciel en `C` qui calcule le volume mixte, et un fichier pour l'appeler depuis Maple. Vérifier que le volume mixte se réduit à la borne de Bézout pour des polynômes dont les polytopes de Newton sont des simplexes, et vérifier la multilinéarité du volume mixte :

```
> read (‘mixvol.mpl‘):
> mixvol ( [ 12+x-y, 3-2*x^2+5*y^2 ] ) ;
 C program took 0sec, computed mixed volume = 2
                2
> s1 := mixvol ([ 3+x, 3-2*x^2+5*y^2 ]):
> s2 := mixvol ([ 4+y, 3-2*x^2+5*y^2 ]):
> s := mixvol ([ 12+x+y+x*y, 3-2*x^2+5*y^2 ]):
```

On doit avoir `s1+s2=s`. Trouvez des exemples pour montrer que le VM s'accroît avec les volumes des polytopes de Newton ainsi que quand l'ensemble des polytopes devient plus "mixte". □

La borne de Bernstein a été généralisée à une borne sur le nombre de racines dans certaines sous-espaces *affines* : On ajoute des termes constants aux polynômes qui en ont pas. Définissons un relèvement 0/1 du système élargi avec les origines artificielles tel que

$$l_i(p) = 0,\ \forall p \in Q_i,\ \forall i, \quad \text{et} \quad 0 \notin Q_i \Rightarrow l_i(0) = 1.$$

Considérons une subdivision mixte induite d'une enveloppe inférieure définie par ce relèvement.

Définition 2.50 *Pour $I \subset \{1, \ldots, n\}$, une cellule (maximale) est* I-stable *si la normale rentrante v de la facette correspondante n'a pas de coordonnées négatives ($v \in \mathbb{Q}^{n+1}_{\geq 0}$) et $v_i > 0 \Rightarrow i \in I$. Le* volume I-stable *du système original est la somme des volumes mixtes des cellules I-stables.*

Théorème 2.51 [HS97] *Pour $I \subset \{1, \ldots, n\}$, le volume I-stable borne le nombre de racines communes isolées dans*

$$\overline{K}_I = \{x \in \overline{K}^{|I|} \times (\overline{K}^*)^{n-|I|} \,:\, x_i = 0 \Rightarrow i \in I\}.$$

Pour des coefficients génériques, cette borne est exacte, pourvu que le nombre de racines est fini dans $\overline{K}_I$.

Preuve Posons $f'_i = f_i$ si $0 \in A_i$, et $f'_i = c_{i0}t + f_i$ si $0 \notin A_i$. Pour presque toutes les valeurs de $t \in K$, les racines du nouveau système sont dans $(\overline{K}^*)^n$. D'après la preuve du théorème 2.41, les racines du nouveau système, pour t proche à 0, sont de séries de Puiseux $x(t) = \gamma t^\lambda + \cdots$, où $\gamma \in (\overline{K}^*)^n$, $\lambda \in \mathbb{Q}^n$ est la normale d'une cellule de la subdivision induite par les l_i, et γ est une solution du système $\sum_{a \in F_i} \gamma^a = 0$, $i = 1, \ldots, n$, où F_i est la face de $Q_i \cup \{0\}$ soutenue par λ.

Une branche $x(t)$ approche une racine du système donné pour $t \to 0$ ssi chaque $\lambda_i \geq 0$. Si $\lambda > 0$, alors $x_i \to 0$ et $i \in I$. Donc $\sum_i F_i$ est une cellule I-mixte et le système a autant de solutions pour γ dans $(\overline{K}^*)^n$ que son volume mixte, par le théorème BKK. □

Quand chaque support donné contient l'origine, le volume stable est le volume mixte du système. Il est clair que, pour un système donné, $VM \leq VS \leq VM(A_i \cup \{0\})$, où VS représente le volume stable.

Exemple 2.52 [EV99] Considérons deux polynômes à coefficients génériques $ay + by^2 + cxy^3$, $ex + fx^2 + gx^3y$. Leurs supports augmentés relevés, obtenus par les relèvements affines $a \mapsto \langle(-2, 1), a\rangle - 1$ et $a \mapsto \langle(1, -2), a\rangle - 1$, sont :

$$\begin{bmatrix} 0 & 0 & 1 & 0 \\ 1 & 2 & 3 & 0 \\ 0 & 1 & 0 & M_1 \end{bmatrix} = \begin{bmatrix} a & b & c & d \end{bmatrix}, \quad \begin{bmatrix} 1 & 2 & 3 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & M_2 \end{bmatrix} = \begin{bmatrix} e & f & g & h \end{bmatrix}.$$

Les colonnes des matrices ci-dessus représentent les points relévés, notés avec les mêmes lettres que les coefficients correspondants. Les M_1, M_2 sont supposés suffisamment grands ; leur valeurs précises peuvent être déterminées au cours de l'algorithme [EV99] afin de les minimiser, voir figure 3 et table 2.52.

Les cellules (ad, fg), (bc, eh) ne sont stables pour aucun I. Il y 3 racines communes dans $\mathbb{C}^2_0$, deux avec exactement une coordonnée nulle, et une égale à $(0, 0)$. Donc, il y a 6 racines dans $\mathbb{C}^2$. □

Dans [EV99], l'algorithme 2.26 est modifié pour calculer le volume I-stable avec un seul relèvement par polytope de Newton. Enfin, il y a d'autres notions du "creux" chez les polynômes, comme le montre le suivant théorème de Khovanskii sur la théorie des "fewnomials".

Théorème 2.53 *Soit un système de n polynômes en n variables avec un nombre total de m monômes. Alors le nombre de racines communes isolées dans $\mathbb{R}^n_{>0}$ est borné par $2^{\binom{m}{2}}(n+1)^m$.*

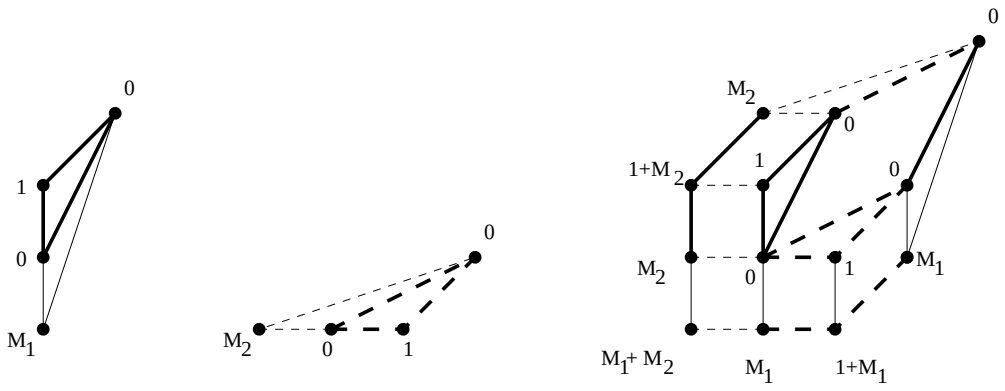


FIG. 3 – Subdivision régulière induite de la somme de Minkowski des supports augmentés pour l'exemple 2.52. Les points sont marqués par leur valeur de relèvement.

TAB. 1 – Cellules de la subdivision pour l'exemple 2.52, les contraintes qu'elles imposent aux M_1, M_2, et la normale rentrante correspondante, avant et après avoir calculé les M_1, M_2. La dernière colonne donne le plus petit ensemble I t.q. la cellule est I-stable.

cellule	normale	constraintes		volume	normal choisie	I-stable
(ac, eg)	$(0, 0, 1)$	$M_1 > 0$	$M_2 > 0$	3	$(0, 0, 1)$	$\emptyset$
(ad, fg)	$(-M_1 + 1, M_1, 1)$	$M_1 > 2$	–	1	$(-1, 1, 1)$	–
(ad, ef)	$(-1, M_1, 1)$	$M_1 > 2$	–	1	$(0, 1, 1)$	$\{2\}$
(ad, eh)	$(M_2, M_1, 1)$	–	–	1	$(1, 1, 1)$	$\{1, 2\}$
(ab, eh)	$(M_2, -1, 1)$	–	$M_2 > 2$	1	$(1, 0, 1)$	$\{1\}$
(bc, eh)	$(M_2, -M_2 + 1, 1)$	–	$M_2 > 2$	1	$(1, -1, 1)$	–

3 Le résultant creux

Le résultant, en général, est un seul polynôme qui exprime la solvabilité d'un système dans un corps algébriquement clos. On introduit le résultant creux en notant certaines relations avec les autres formulations du résultant. Des exposés générales se trouvent dans [EM99, CLO05, vdW50]. Cas du système de $n + 1$ équations linéaires en n variables : Le résultant est le déterminant de la matrice carrée de dimension $n + 1$ des coefficients.

Étant donnés les polynômes

$$f_0, \ldots, f_n \in (\mathbb{Q}[c])[x_1^{\pm 1}, \ldots, x_n^{\pm 1}] \; = \; (\mathbb{Q}[c])[x^{\pm 1}],$$

t.q. $c = (c_{00}, \ldots, c_{10}, \ldots, c_{n0}, \ldots)$ et tous les coefficients sont non-nuls : $f_i = \sum_{j=0}^{m_i} c_{ij} x^{a_i j}$, $c_{ij} \neq 0$. Soient $K = \mathbb{Q}[c]$, A_i le support de f_i et Q_i son polytope de Newton. Soient

$$Z_0 = \{c \mid \exists\, \alpha \in \left(\overline{K}^*\right)^n : f_i(\alpha) = 0, \forall i\} \; \subset \; \mathbb{P}^{m_0} \times \cdots \times \mathbb{P}^{m_n},$$

et $Z = \overline{Z_0}$ son adhérence Zariski dans $\mathbb{P}^{m_0} \times \cdots \times \mathbb{P}^{m_n}$.

Proposition 3.1 *Z est une sous-variété propre (de codimension positive) irréductible.*

Preuve [PS93] Considérons la variété W et ses deux projections canoniques

$$(\overline{K}^*)^n \xleftarrow{\pi_1} W = \{(x, c) \in (\overline{K}^*)^n \times \prod_{i=0}^{n} \mathbb{P}^{m_i} \; : \; f_i(x, c) = 0, \; \forall i\} \xrightarrow{\pi_2} \prod_{i=0}^{n} \mathbb{P}^{m_i}.$$

La projection π_1 de W dans $(\overline{K}^*)^n$ est surjective : Pour tout $\alpha \in (\overline{K}^*)^n$, $\pi_1^{-1}(\alpha) = \prod_i H_i$, où $H_i \subset \mathbb{P}^{m_i}$ est l'ensemble de vecteurs c_i orthogonaux au vecteur des valeurs des monômes A_i évalués à α ; puisque ce vecteur n'a aucune coordonnée nulle, $c_i \in \mathbb{P}^{m_i}$. $\mathrm{Im}(\pi_1) = (\overline{K}^*)^n$ est une variété quasi-projective irréductible.

Chaque H_i est un hyperplan alors, pour toute solution α, $\pi_1^{-1}(\alpha)$ est irréductible et de la même dimension, égale à $\sum_{i=0}^{n}(m_i - 1)$.

Nous pouvons maintenant déduire [Sha77, thm. I.6.8,p. 61] que W est irréductible est de dimension augmentée par n, c.à.d. $\sum_{i=0}^{n} m_i - 1$ (autrement dit de codimension $n+1$, ce qui est intuitif). Donc la projection π_2 est aussi irréductible et de dimension $\leq \sum_{i=0}^{n} m_i - 1 \Leftrightarrow \mathrm{codim}(Z_0) \geq 1$. □

Exercice 3.2 Montrez que $\mathrm{codim}(Z) \geq 1$ sans passer par la dimension des fibres de π et de W. Appliquez le théorème de Bernstein pour les $f_1, \ldots, f_n$ avec des coefficients génériques. □

Les variétés W et Z sont définies sur $\mathbb{Q}$, alors :

Définition 3.3 *Le* résultant creux *est, à un signe près, le polynôme irréductible $R \in \mathbb{Z}[c_{ij}]$ qui définit Z, si $codim(Z) = 1$. Si $codim(Z) > 1$, $R = 1$.*

Quand $\mathrm{codim}(Z) = 1$, le résultant évalue à zéro si, pour les coefficients spécialisés, il y a une solution dans $(\overline{K}^*)^n$. On peut fixer le signe en précisant que le résultant creux associé au système $f_i = x_i - 1$, pour $i = 1, \ldots, n$, et $f_0 = x_1 x_2 \cdots x_n - c_0$ est $R = c_0 - 1$.

Lemme 3.4 [PS93, sect.2] *$codim(Z) > 1$ ssi tous les volumes mixtes des sous-systèmes de dimension n sont nuls. C.à.d. que $codim(Z) = 1$ ssi il existe un sous-système $n \times n$ dont le volume mixte est positif.*

Preuve [⇒] $\mathrm{codim}(Z) = 1 \Rightarrow Z$ est la variété du polynôme R. Soit c_{ij} un coefficient qui apparaît dans R. Pour tous les c_{kl}, $k \neq i$, génériques R s'annule pour certaines valeurs de c_{ij}. Dans ce cas, le système $f_0, \ldots, f_{i-1}, f_{i+1}, \ldots, f_n$ a de solutions communes pour de coefficients génériques, alors son volume mixte est positif.
[⇐] Exercice 3.5. □

Exercice 3.5 Montrez la deuxième direction de la preuve : que $\mathrm{codim}(Z) = 1$ s'il existe un $VM > 0$. □

D'après l'exercice 2.7, $\dim \sum_{i \in I} Q_i = n$ implique que $\mathrm{codim}(Z) = 1$ pour un ensemble $I \subset \{0, \ldots, n\}$ où $|I| \geq n$.

Définition 3.6 *Pour $I \subset \{0, \ldots, n\}$, considérons le sous-réseau entier affine engendré sur $\mathbb{Z}$ par les A_i après les avoir translaté pour qu'ils contiennent l'origine :*

$$L(I) = L(\{A_i : i \in I\}) = \left\{ \sum_{i \in I} \lambda_i a_i : a_i \in A_i, \lambda_i \in \mathbb{Z}, \sum_{i \in I} \lambda_i = 1 \right\}.$$

Le rang *de I, noté $rg(I)$, est la dimension du $\mathbb{R}$-espace vectoriel dans $\mathbb{R}^n$ engendré par les vecteurs entre l'origine et les points dans $L(I)$.*

Le rang $= n$ ssi nous pouvons identifier le réseau engendré à $\mathbb{Z}^n$.
Une formule intéressante (et intuitive) est la suivante :

Proposition 3.7 [PS93] *Le résultant est exprimé par une formule du type* Poisson *comme suit :*

$$C_0 \cdot \prod_{\alpha} f_0(\alpha)^{k_\alpha}, \quad \alpha \in (\overline{K}^*)^n,\ f_1(\alpha) = \cdots = f_n(\alpha) = 0,$$

où k_α est la multiplicité de la racine α, et la constante C_0 est définis par de résultants de certains sous-systèmes qui n'incluent pas f_0, donc C_0 ne dépend que des c_{ij}, $i > 0$.

Théorème 3.8 *Supposons que $L(\{A_0, \ldots, A_n\})$ est identifiable à $\mathbb{Z}^n$. Le résultant creux R est homogène en les coefficients c_i pour chaque $i \in \{0, \ldots, n\}$ et son degré en les coefficients c_i de f_i est*

$$\deg_{f_i} R = VM(Q_0, \ldots, Q_{i-1}, Q_{i+1}, \ldots, Q_n).$$

Preuve Le réseau qui s'identifie à $\mathbb{Z}^n$ implique qu'il y a un sous-système $Q_0, \ldots, Q_{i-1}, Q_{i+1}, \ldots, Q_n$ dont la somme de Minkowski est de dimension n. Par l'exercice 2.7 ou l'observation qui le précède, le volume mixte est positif donc $\operatorname{codim}(Z) = 1$ (lemme 3.4). Il suffit maintenant d'utiliser la formule de Poisson et appliquer le théorème 2.41 avec f_i à la place de f_0. Pour de details, voir [GKZ94]. □

Exemple 3.9 Pour $f_0 = c_{01}x^2, f_1 = c_{11}x$, les deux volumes mixtes sont 0 donc $\operatorname{codim}(Z) > 1$ et le résultant $R = 1$. Le résultant creux des polynômes $f_0 = c_{00} + c_{01}x^2, f_1 = c_{10} + c_{11}x^2$ est $R = c_{00}c_{11} - c_{01}c_{10}$; notons que $\operatorname{codim}(Z) = 1$. Par contre, le déterminant de Sylvester (qui exprime la spécialisation du résultant projectif) est de degré 2 en les coefficients de chaque polynôme et vaut R^2. Cela vient en contradiction avec la conclusion du théorème ci-dessus parce que son hypothèse n'est pas satisfaite, notamment le réseau affine engendré par $\{0, 2\}$ est $2\mathbb{Z}$ et non pas $\mathbb{Z}$. Avec un changement de variable $x^2 \mapsto y$, on obtient des volumes mixtes égaux à 1. □

Exercice 3.10 Montrez que $R(f_0, \ldots, af_i, \ldots, f_n) = a^{VM(f_0,\ldots,f_{i-1},f_{i+1},\ldots,f_n)} R(f_0, \ldots, f_i, \ldots, f_n)$, pour un a scalaire. □

Théorème 3.11 [Stu94, thm.1.1] *La $\operatorname{codim}(Z)$ dans $\prod_i \mathbb{P}^{m_i - 1}$ est égale au* $\max\{|I| - rg(I)\}$ *maximisé sur tout $I \subset \{0, \ldots, n\}$.*

Corollaire 3.12 *$\operatorname{codim}(Z) = 1 \Leftrightarrow \exists! I \subset \{0, \ldots, n\}$ minimal, appelé* essentiel, *t.q. $rang(I) = |I| - 1$ et $J \subsetneq I \Rightarrow rang(J) \geq |J|$. Dans ce cas, le résultant creux du système original vaut $R(f_i, i \in I)$ après un changement de variables qui aboutit à $rg(I)$ variables indépendantes par le biais d'une forme normale de Smith.*

Preuve Exercise. □

Exemple 3.13 On remarque que c'est possible d'avoir un volume mixte nul, les autres non-nuls et $\operatorname{codim}(Z) = 1$. Par exemple, le système

$$f_0 = c_{00} + c_{01}x + c_{02}y, f_1 = c_{10} + c_{11}y, f_2 = c_{20} + c_{21}y^2,$$

a comme volumes mixtes : $0, 2, 1$. En fait, $Z = \{c : c_{10}^2 c_{21} + c_{11}^2 c_{20} = 0\}$ et le résultant creux est $R = c_{10}^2 c_{21} + c_{11}^2 c_{20}$. Notons, par ailleurs, que $Z_0 \subsetneq Z$ puisqu'il existe $c = (1, 2, 3, 0, 1, 0, 1) \in Z$ qui implique $y = 0$.

Cet exemple vérifie le corollaire 3.12 (voir aussi le lemme 3.4) puisque il existe $I = \{1, 2\}$, $\operatorname{rang}(I) = 1$ tandis que $I = \{0, 1, 2\}$ avec rang$= 2$ ne satisfait par la condition de minimisation. $R = R(f_1, f_2)$ est calculé par la matrice de Sylvester. □

Notons le paradoxe suivant. L'identité évidente

$$R(f_0'f_0'', f_1, \ldots, f_n) = R(f_0', f_1, \ldots, f_n)R(f_0'', f_1, \ldots, f_n)$$

n'est pas contradictoire à l'irréductibilité du résultant creux parce que les coefficients du polynôme f_0f_0' ne sont pas génériques. Cette identité est vraie si les supports de $f_0', \ldots, f_n$ et de $f_0'', \ldots, f_n$ engendrent $\mathbb{Z}^n$, sinon les deux derniers résultants ont un exposant égal à *l'indice* du sous-réseau affine engendré dans $L(\{A_0, \ldots, A_n\})$ [PS93, Prop.7.1]. En général, pour des réseaux entiers $L' \subset L$ (L est un raffinement), l'indice $[L : L']$ de L' dans L est donné par le volume du parallélotope fondamental de L normalisé dans L' ; voir le lemme 2.2.

Par définition, le résultant creux est une condition *nécessaire* pour l'existence de racines dans $(\overline{K}^*)^n$, mais pas suffisante en général. Sur la variété torique, le résultant creux donne une condition nécessaire et suffisante.

Définition 3.14 *Soient* $A = \{a_0, \ldots, a_m\} \subset \mathbb{Z}^n$ *et*

$$\phi : (\overline{K}^*)^n \to \mathbb{P}^m : (x_1, \ldots, x_n) \mapsto (x^{a_0} : \cdots : x^{a_m}).$$

La variété torique $\mathcal{X}_A$ *est une variété projective définie comme l'adhérence de l'image de* ϕ.

Alors $(\overline{K}^*)^n$ correspond à un sous-ensemble ouvert et dense de $\mathcal{X}_A$. Cette définition est généralisée dans [Ful93]. La variété torique est invariante par rapport aux translations des a_i. $\mathcal{X}_A$ est aussi notée $\mathcal{X}_Q$, si $Q = \mathrm{Conv}(A)$, ou même $\mathcal{X}_P$ pour tout polytope P dont les cônes normaux raffinent ceux de Q.

Théorème 3.15 [Ful93, GKZ94] *Pour un système aux supports* $A_0, \ldots, A_n$, *soit* $A = \sum_{i=0}^n A_i$. $R(c)$ *s'annule pour une spécialisation des coefficients ssi il y a une solution* α *commune aux polynômes* $f_0(\alpha) = \cdots = f_n(\alpha) = 0$, *t.q.* α *appartient à la variété torique* $\mathcal{X}_A$. *Cette variété peut être aussi notée* $\mathcal{X}_Q$, *associée à* $Q = Q_0 + \cdots + Q_n$.

Cela implique que le résultant creux exprime une forme de Chow pour la variété torique.

Exemple 3.16 Pour des systèmes linéaires, $\mathcal{X}_Q = \mathbb{P}^n$ puisque tous les Q_i, ainsi que Q, sont de simplexes. Par exemple, pour $n = 2$ et la spécialisation donnée en exemple 3.13 qui se trouve dans $Z \setminus Z_0$, il existe une solution $(x_0 : x : y) = (-c_{01}, c_{00}, 0) \in \mathcal{X}_Q \setminus (\mathbb{C}^*)^n$. □

Exercice 3.17 (1) Dans le cas complètement dense, les polytopes de Newton sont des simplexes d_iS, $VM(f_1, \ldots, f_n) = \prod_{i=1}^n d_i$, $d_i = \deg f_i$. (2) Montrez que $\mathcal{X}_S = \mathbb{P}^n_{\overline{K}}$: Considérer l'application injective de Veronese $V : \mathbb{P}^n \to \mathbb{P}^{\binom{d+n}{n}-1} : (x_0 : \cdots : x_n) \mapsto (\ldots, x^a, \ldots)$ pour tous les monômes a de degré total d. Alors $\phi(x_1, \ldots, x_n) = V(1 : x_1 : \cdots : x_n)$ donc $\mathcal{X}_A \subset V(\mathbb{P}^n)$. Vous devez montrer $\mathcal{X}_A = V(\mathbb{P}^n)$ en considérant le polynôme qui s'annule sur les deux variétés. Alors $\mathcal{X}_A \simeq \mathbb{P}^n$ où A sont les monômes a de degré d. (3) Montrez que les résultants classique et creux sont identiques. □

Le résultant creux spécifié par les polytopes de Newton divise le résultant projectif (classique) du système dense dans lequel on a spécialisé tous les coefficients absents des supports à zéro, voir exemple 3.9. Les résultants ne sont pas divisibles pour des coefficients génériques (à cause de l'irréductibilité).

Exemple 3.18 Pour des systèmes bilinéaires, $\mathcal{X} = \mathbb{P}^1 \times \mathbb{P}^1 \subset \mathbb{P}^3$. Considérez l'application injective de Segre $S : \mathbb{P}^1 \times \mathbb{P}^1 \to \mathbb{P}^3 : (u, s, v, t) \mapsto (uv, sv, ut, st)$ et montrez $\mathcal{X} = \mathrm{Im}(S)$. □

Nous présentons maintenant certaines propriétés dans le cas $A_0 = \cdots = A_n$, qui sont toutefois généralisables.

Théorème 3.19 [Jou97] *Supposons que tous les supports $A_0 = \cdots = A_n$ sont égaux (donc $Q_0 = \cdots = Q_n$) et l'hypothèse du théorème 3.8 est satisfaite. Si $g_i = \sum_{j=0}^n b_{ij} f_j$, $i = 0, \ldots, n$ et la matrice $(b_{ij})_{ij}$ est inversible, alors*

$$R(g_0, \ldots, g_n) = \det(b_{ij})_{ij}^{n!\mathrm{Vol}(Q_0)} R(f_0, \ldots, f_n).$$

Un corollaire immédiat donne le résultant d'un système linéaire surcontraint comme le déterminant de la matrice des coefficients b_{ij}, si on pose $f_i = x_i$, $i = 1, \ldots, n$ et $f_0 = 1$.

Corollaire 3.20 *Sous les hypothèses du théorème précédant, $m_0 = \cdots = m_n$. Soient $0 \leq k_0 \leq \cdots \leq k_n \leq m_0$, alors (le "bracket") $[k_0, \ldots, k_n]$ représente $\det(c_{ik_j})_{ij} \in \mathbb{Z}[c_{ij}]$, c.à.d. le mineur dans la matrices des coefficients défini par les colonnes $k_0, \ldots, k_n$. Le résultant (creux) est un polynôme en tous les $[k_0, \ldots, k_n]$.*

Exemple 3.21 Le résultant creux du système bilinéaire (1) : $f_i = c_{i0} + c_{i1}s + c_{i2}t + c_{i3}st$, $i = 0, 1, 2$ est $R = [013][023] - [012][123]$. Ces deux termes correspondent aux deux différentes triangulations du carrée Q_0. C'est une propriété générale de la formulation en fonction des mineurs (ou "brackets") [PS93, Stu94].

Montrez que le résultant projectif s'annule et que le résultant creux est

$$R_{cr} = \det \begin{bmatrix} c_{i0} & c_{i1} & c_{i2} & c_{i3} & 0_3 & 0_3 \\ 0_3 & c_{i0} & 0_3 & c_{i2} & c_{i1} & c_{i3} \end{bmatrix}, \quad \text{les colonnes } c_{ij} \in \mathbb{Q}^{3\times 1}, i = 0, \ldots, 2,$$

où la sous-matrice $[c_{ij}]_{i,j>0}$ est supposée régulière. □

Il y a une notion d'homogeneïsation torique basée sur Q_0 et la liste de ses normales rentrantes $v_j, j = 1, \ldots, k$. Soit a_j la valeur (minimale) du produit scalaire (v_j, Q_0) de v_j avec un point dans Q_0. En introduisant des nouvelles variables y_j associées aux facettes de Q_0, nous pouvons définir des nouveaux polynômes

$$F_i(y_1, \ldots, y_k) = f_i \left(x_t \mapsto \prod_{j=1}^k y_j^{v_{jt}} \right) \prod_{j=1}^k y_j^{a_j}, \quad i = 0, \ldots, n.$$

Chaque exposant $a \in \mathbb{Z}^n$ des x_t, vu comme un vecteur-colonne, s'associe à l'exposant $h(a) = Na$, où N est la matrice $k \times n$ dont les lignes sont les normales.

Théorème 3.22 [CLO05, Thm.3.13] *Les solutions* non-triviales *des F_i dans $\overline{K}^k$ (l'espace affine), sont celles pour lesquelles il y a un monôme $y^{h(a)}$ qui ne s'annule pas, pour quelque sommet a de Q. Si $\dim Q_0 = n$, alors il existe une solution non-triviale ssi le résultant creux des F_i s'annule.*

4 Formules matricielles dans le cas univarié

Le but serait de construire des matrices dont le déterminant est le résultant R ou, si cela est impossible, un multiple de R. Ces multiples s'appellent des *matrices du résultant* et constituent des conditions nécessaires pour l'existence des racines communes.

Si $B \subset \mathbb{Z}^n$, $P(B) = \{g \in K[x^{\pm 1}] : \mathrm{supp}(g) \subset B\}$ est un espace vectoriel sur K de dimension $|B|$. Étant donnés des $B_0, \ldots, B_n \subset \mathbb{Z}^n$, nous définissons (ayant transposé la matrice pour des raisons historiques)

$$\begin{aligned} M \ : P(B_0) \times \cdots \times P(B_n) \ &\to \ P\left(\bigcup_{i=0}^n A_i + B_i \right) \\ (g_0, \ldots, g_n) \ &\mapsto \ [g_0, \cdots, g_n]M = \left[\sum_{i=0}^n f_i g_i \right]. \end{aligned} \tag{3}$$

Cette transformation exprime aussi l'évaluation des multiples des f_i correspondant aux lignes de la matrice M aux points de $\overline{K}^n$. Soient

$$\{m_1, \ldots, m_t\} = \bigcup_{i=0}^{n} (B_i + \mathrm{supp}(f_i))$$

les monômes indexant les colonnes de la matrice M. Soient $b_{01} \in B_0$, $b_{nk} \in B_n$ et $v_\alpha = [\alpha^{m_1}, \ldots, \alpha^{m_t}]^T$, alors

$$\begin{array}{c} \\ x^{b_{01}} f_1(x) \\ \vdots \\ x^{b_{nk}} f_N(x) \end{array} \begin{array}{c} \begin{array}{ccc} x^{m_1} & \cdots & x^{m_t} \end{array} \\ \left[\begin{array}{ccc} & & \\ & M & \\ & & \end{array}\right] \end{array} \begin{array}{c} v_\alpha \\ \left[\begin{array}{c} \alpha^{m_1} \\ \vdots \\ \alpha^{m_t} \end{array}\right] \end{array} = \left[\begin{array}{c} \alpha^{b_{01}} f_1(\alpha) \\ \vdots \\ \alpha^{b_{nk}} f_N(\alpha) \end{array}\right],$$

où $x^b f_i(x) = \sum_a c_{ia} x^{b+a}$ signifie que c_{ia} est l'entrée de la colonne x^{b+a}.

Nous avons vu que le déterminant de la matrice des coefficients d'un système linéaire en n variables est son résultant (creux). Chaque $B_i = \{1\}$ et l'ensemble $\{1, x_1, \ldots, x_n\}$ (monômes des colonnes) est la base de l'espace du but de (3).

Lemme 4.1 *Pour des coefficients $c_0 \in Z_0$, la matrice $M(c_0)$ n'est pas surjective.*

Preuve $c_0 \in Z_0 \Rightarrow \exists$ solution $\alpha \in (\overline{K}^*)^n$. M surjective $\Rightarrow \exists$ monôme $x^q = \sum_i f_i g_i \Rightarrow \alpha^q = \sum_i f_i(\alpha) g_i(\alpha) = 0$: impossible. □

Pour identifier les racines communes M doit être génériquement surjective. La surjectivité de M implique une contrainte sur la dimension des domaines de départ et d'arrivée :

$$\sum_{i=0}^{n} \dim P(B_i) \;\geq\; \dim P\left(\bigcup_{i=0}^{n} A_i + B_i\right),$$

i.e., Nb lignes $\geq$ Nb colonnes. De plus, $|B_i|$ est égal au degré de $\det M$ en les coefficients de f_i, alors on doit avoir $|B_i| \geq \deg_{f_i} R = VM(Q_0, \ldots, Q_{i-1}, Q_{i+1}, \ldots, Q_n)$, supposons que le réseau des supports A_i est identifié à $\mathbb{Z}^n$. Le problème algorithmique qui se pose est de définir les supports B_i t.q. M est génériquement surjective. Dans ce cas M est une *matrice du résultant*.

Lemme 4.2 *Si $|B_i| \geq VM(Q_0, \ldots, Q_{i-1}, Q_{i+1}, \ldots, Q_n)$, alors $R \,|\, D$ dans $\mathbb{Z}[c]$, pour chaque mineur maximale D de M.*

Preuve D'après le lemme, chaque D s'annule pour tout $c_0 \in Z_0$, donc $Z_0 \subset V(D)$, où $V(D)$ est la variété de D. Comme $V(D)$ est fermée, l'adhérence $Z \subset V(D)$ et, par le Théorème des zéros de Hilbert, $D \in \sqrt{(R)}$. Z est irréductible $\Rightarrow$ l'idéal (R) est premier et donc radical. Alors $D \in (R) \;\Rightarrow R \,|\, D \in \mathbb{Z}[c]$. □

On obtient donc un multiple du résultant creux en utilisant le fait que les racines intéressantes sont $\alpha \in (\overline{K}^*)^n$. Cela évite de placer de contraintes sur les ensembles B_i, contrairement à ce qui se passe avec la matrice de Macaulay [Mac02] pour le résultant classique, où il existe B_i qui contient 1.

Nous examinerons les matrices de *Sylvester*, de *Macaulay*, de *Newton* (ou du résultant creux), de *Bézout* à une ou plusieurs variables, de *Dixon* ou de *Morley/Jouanolou* dans les cas respectifs.

Dans le cadre projectif, nous pouvons considérer les solutions dans une variété projective X autre que $\mathcal{X}$ (le cas classique est celui de $\mathbb{P}^n$). Nous aurions alors besoin d'une hypothèse supplémentaire :
(H1) *Pour tout $x \in X$, il existe un monôme dans un polynôme f_i qui ne s'annule pas sur x.*

4.1 Matrice de Sylvester

La matrice la plus facile est celle nommée d'après Sylvester, pour deux polynômes à une variable, $f_0 = a_{d_0}x^{d_0} + a_{d_0-1}x^{d_0-1} + \cdots + a_0$ et $f_1 = b_{d_1}x^{d_1} + b_{d_1-1}x^{d_1-1} + \cdots + b_0$, où $d_1, d_0 > 0$ et $a_{d_0}b_{d_1} \neq 0$. Sa formulation matricielle [Syl53] est donnée par le déterminant

$$R(f_0,f_1) = \begin{vmatrix} a_{d_0} & a_{d_0-1} & \cdots & a_0 & 0 & \cdots & & 0 \\ 0 & a_{d_0} & a_{d_0-1} & \cdots & a_0 & 0 & \cdots & 0 \\ \vdots & & \ddots & & & \ddots & & \\ 0 & & & a_{d_0} & a_{d_0-1} & \cdots & & a_0 \\ b_{d_1} & b_{d_1-1} & \cdots & & b_0 & 0 & \cdots & 0 \\ 0 & b_{d_1} & b_{d_1-1} & \cdots & & b_0 & 0 & 0 \\ \vdots & & \ddots & & & \ddots & & \\ 0 & & & b_{d_1} & b_{d_1-1} & \cdots & & b_0 \end{vmatrix}.$$

Les monômes des lignes sont $B_0 = \{1, x, \ldots, x^{d_1-1}\}$ et $B_1 = \{1, x, \ldots, x^{d_0-1}\}$. $\cup_i(A_i+B_i) = \{1, x, \ldots, x^{d_0+d_1-1}\}$, alors la dimension du domaine du départ ainsi que du but est de $d_0 + d_1$. Cette matrice et son déterminant sont disponibles sur plusieurs systèmes d'algèbre formelle, y compris MAPLE, MATHEMATICA et REDUCE.

Exemple 4.3 Soient $p_0 = a_0 + a_1x, p_1 = b_0 + b_1x + b_2x^2$. La matrice de Sylvester S est la suivante ; on montre aussi la multiplication par le vecteur des valeurs des monômes $1, x, x^2$ (qui indexent les colonnes).

$$S: \begin{matrix} p_0 \\ xp_0 \\ p_1 \end{matrix} \begin{bmatrix} a_0 & a_1 & 0 \\ 0 & a_0 & a_1 \\ b_0 & b_1 & b_2 \end{bmatrix} \begin{pmatrix} 1 \\ \alpha \\ \alpha^2 \end{pmatrix} = \begin{pmatrix} p_0(\alpha) \\ \alpha p_0(\alpha) \\ p_1(\alpha) \end{pmatrix}, \qquad \det S = a_0^2b_2 + a_1^2b_0 - a_0a_1b_1.$$

□

Lemme 4.4 *Le déterminant de Sylvester est le résultant creux des polynômes f_0, f_1 si au moins un polynôme a un coefficient constant non-nul et les A_0, A_1 engendrent $\mathbb{Z}$.*

Preuve S'il y a une solution $\alpha \in \overline{K}$, le vecteur $(1, \alpha, \ldots, \alpha^{d_0+d_1-1}) \neq 0$ appartient au noyau de la matrice, donc le déterminant s'annule.

Inversement, supposons que le déterminant s'annule. Alors il y a un vecteur non-nul dans le noyau à gauche qui exprime deux polynômes non-nuls g_0, g_1 de degré inférieur à d_1, d_0, tels que $f_0g_0 + f_1g_1 = 0$. Le ppcm est donc de degré $< d_0+d_1$, puisque f_0g_0 est un commun multiple. Utilisant ppcm$= f_0f_1/$pgcd on déduit que le degré du pgcd est positif, alors il y a une racine commune dans la clôture algébrique $\overline{K}$. Puisque au moins un coefficient constant est non-nul, $\alpha \neq 0$ donc $\alpha \in (\overline{K})^*$. □

Le résultant de Sylvester offre une condition nécessaire et suffisante même si $\mathcal{X}_Q = \mathbb{P}^1$ est un surensemble propre de $\overline{K}^*$. La raison est que si $(t:0) \in \mathbb{P}^1 \setminus \overline{K}^*$ est une racine, $c_{00}t = c_{10}t = 0 \Rightarrow t = 0$, ce qui est impossible. Le résultant est un polynôme de degré d_0 et d_1 en les coefficients de f_0 et f_1, respectivement.

4.2 Matrice de Bézout : cas d'une variable

L'autre alternatif dans le cas univarié, est nommé d'après Bézout. Soient $d_0 \geq d_1$ les degrés de $f_0, f_1 \in K[x]$. Il existe une prsentation du rsultant, lgrement plus complique que la matrice de Sylvester, qui est cependant plus ancienne. Elle a été introduite par E. Bézout vers 1779 et elle a l'avantage de fournir une matrice plus petite que celle de Sylvester, sa taille étant d_0^2 au lieu de $(d_0 + d_1)^2$.

Supposons que les polynômes sont denses. On définit

$$\delta(x,y) = \begin{vmatrix} f_0(x) & f_0(y) \\ f_1(x) & f_1(y) \end{vmatrix},$$

où y est une nouvelle indéterminée. $\delta(x,x) = 0 \Rightarrow x - y | \delta(x,y)$, donc

$$\Delta(x,y) = \frac{\delta(x,y)}{x-y} = \sum_{i=0}^{d_0-1} \theta_i(x) y^i$$

est un polynôme en x, y de degré total $d_0 + d_1 - 1$, symétrique et de degré $d_0 - 1$ en chaque variable.

Exercice 4.5 Écrivez Δ comme le déterminant d'une matrice 2×2. □

En décomposant les d_0 polynômes $\theta_i(x)$ par rapport à une base de monômes en x, on obtient une matrice Φ, de dimension $d_0 \times d_0$ (donc carrée) et symétrique. Nous verrons que $|\Phi|$ est un multiple du résultant, tandis que la matrice M ci-dessous donne exactement le résultant.

$$\begin{array}{r} \\ \theta_0 \\ \vdots \\ \theta_{d_1-1} \\ \theta_{d_1} \\ \vdots \\ \theta_{d_0-1} \end{array}
\overbrace{\begin{array}{cccc} 1 & \cdots & \cdots & x^{d_0-1} \\ \multicolumn{4}{c}{\multirow{6}{*}{Φ}} \\ \\ \\ \\ \\ \\ \end{array}}^{d_0}
\left.\vphantom{\begin{array}{c}a\\a\\a\\a\\a\\a\end{array}}\right\} d_0
\quad \rightsquigarrow \quad
\begin{array}{r} \\ \theta_0 \\ \vdots \\ \theta_{d_1-1} \\ f_1(x) \\ \vdots \\ x^{d_0-d_1-1} f_1(x) \end{array}
\overbrace{\begin{array}{cccc} 1 & \cdots & \cdots & x^{d_0-1} \\ \multicolumn{4}{c}{\multirow{6}{*}{M}} \\ \\ \\ \\ \\ \\ \end{array}}^{}$$

Exercice 4.6 Devinez (par ex. en s'expérimentant) ce que vaut chaque θ_i pour $d_0 > i \geq d_1$; le démontrez ensuite. Indication : $\theta_i(x)$ est un multiple d'un polynôme f_j, $j = 0, 1$. □

Théorème 4.7 *Les déterminants $|\Phi|$ et $|M|$ sont de multiples du résultant creux R. En particulier, $|\Phi| = RP$, où P est un facteur parasite de degré $d_0 - d_1$, et $|M| = R$.*

Preuve (Partielle). Si $\exists \alpha$ racine commune des $f_i \Rightarrow \delta(\alpha, y)$ est un polynôme en y identiquement nul, et pareil pour $\Delta(\alpha, y)$. Donc tous les termes $\theta_i(\alpha)$ doivent s'annuler. On peut maintenant définir le vectur $v := (1, \alpha, \ldots, \alpha^{d_0-1}) \neq 0$ t.q. $\Phi v^T = (\theta_0(\alpha), \ldots, \theta_{d_0-1}(\alpha))^T = 0$. Alors $|\Phi|$ et $|M|$ sont de multiples du résultant (creux).

Le degré des termes du résultant (creux) en les coefficients c_i de f_i, $i = 0, 1$ est égal à d_j, $\{i, j\} = \{0, 1\}$. Le degré des monômes dans $\delta(x, y)$ en les f_i est 1 (donc 2 en total), et pareil pour les θ_i. Alors $\deg \det \Phi = d_0$ en c_i, ce qui montre le degré du facteur parasite P. De plus, $\deg_{c_0} \det M = d_1, \deg_{c_1} \det M = d_0$ alors $\det M$ ne contient pas de facteur parasite. □

Avec la notation de (3), $B_i = \{1\}, i = 0, \ldots, d_0 - 1$ pour les polynômes $\theta_i(x), i = 0, \ldots, d_0 - 1$, au lieu des f_i. L'application Φ s'écrit

$$\Phi : P(\{1\}) \times \cdots \times P(\{1\}) \to P(\{1, \ldots, x^{d_0-1}\}).$$

Le déterminant donne $\det \Phi(f_0, f_1) = \prod_{f_1(\alpha)=0} f_0(\alpha)^{k_\alpha}$ à un scalaire près (forme de Poisson) où k_α est la multiplicité de la racine α.

La matrice de multiplication par f_0 dans l'anneau quotient de f_1 est $M_{f_0} = \Phi(f_0, f_1)\Phi^{-1}(1, f_1)$ [EM02]. Le corollaire de cette proposition est que le rang $\mathrm{rg}(\Phi(f_0, f_1)) = d_0 - \deg \gcd(f_0, f_1)$.

Exemple 4.8 Soient $p_0 = a_0 + a_1 x, p_1 = b_0 + b_1 x + b_2 x^2$.

$$\delta(x,y) = \begin{vmatrix} a_0 + a_1 x & a_1(y-x) \\ b_0 + b_1 x + b_2 x^2 & b_1(y-x) + b_2(y+x)(y-x) \end{vmatrix} \Rightarrow \Delta(x,y) = a_0 b_1 - a_1 b_0 + a_0 b_2 x + a_0 b_2 y + a_1 b_2 xy.$$

Notons que $\theta_1(x) = a_0 b_2 + a_1 b_2 x = b_2 p_0(x)$, tandis que $x\theta_0(x) = a_0 p_1(x) - b_0 p_0(x)$.

$$\Phi \; : \; \begin{matrix} \theta_0(x) \\ \theta_1(x) \end{matrix} \begin{bmatrix} a_0 b_1 - a_1 b_0 & a_0 b_2 \\ a_0 b_2 & a_1 b_2 \end{bmatrix}$$

est une matrice Hankel (antidiagonales constantes). La matrice de Bézout M est la suivante ; on montre aussi la multiplication par le vecteur qui exprime l'évaluation des monômes de colonnes.

$$\begin{matrix} \theta_0(x) \\ p_0(x) \end{matrix} \begin{bmatrix} a_0 b_1 - a_1 b_0 & a_0 b_2 \\ a_0 & a_1 \end{bmatrix} \begin{pmatrix} 1 \\ \alpha \end{pmatrix} = \begin{pmatrix} \frac{a_0 p_1(\alpha) - b_0 p_0(\alpha)}{\alpha} \\ p_0(\alpha) \end{pmatrix}.$$

□

5 Matrice de Newton à partir d'une subdivision mixte

La matrice de Newton a des entrées nulles ou égales à un coefficient du système d'entrée et ses lignes correspondent aux multiples des polynômes d'entrée. Son déterminant définit un multiple non-trivial du résultant creux.

Algorithme 5.1 (À partir d'une subdivision) [CE00]
1. Définir une subdivision mixte Δ de la somme (de Minkowski) $Q = Q_0 + \cdots + Q_n$. Ceci peut se faire en choisissant $n+1$ formes linéaires, suffisamment génériques.
2. Perturber la somme par un vecteur infinitésimal $\delta \in \mathbb{Q}^n$, alors pour toute cellule maximale σ

$$\mathcal{E} = (Q + \delta) \cap \mathbb{Z}^n : p \in \mathcal{E} \Rightarrow \exists\,! \, \sigma \in \Delta : p \in \sigma + \delta.$$

3. Définir

$$\mu \; : \mathcal{E} \to \bigcup_i A_i \; : \; p \mapsto a_{ij} \in A_i \quad \Leftrightarrow \quad p \in \sigma = F_0 + \cdots + a_{ij} + \cdots + F_n, \dim F_j > 0, \forall j > i.$$

Construction d'une matrice M (à la Macaulay) dont les lignes et les colonnes sont indexées par $\mathcal{E}$: pour $p, q \in \mathcal{E}$, l'élément (p,q) est le coefficient de x^q dans $x^{p-a_{ij}} f_i$, où $a_{ij} = \mu(p)$. Avec la notation précédente, $B_i = \{p - \mu(p) \; : \; p \in \mathcal{E}, \mu(p) \in A_i\}$.

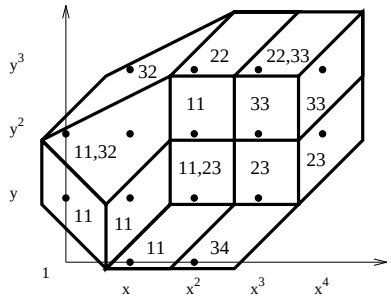


FIG. 4 – Subdivision mixte perturbée dans $\mathbb{R}^2$.

Exemple 2.21 (suite) La projection de l'enveloppe inférieure de la figure 2 définit la subdivision mixte de $Q \subset \mathbb{R}^2$; voir la figure 4. Cette dernière est montrée perturbée par $\delta = (-3/8, -1/8)$. Chaque cellule maximale σ est marquée par les indices des sommets de polytopes de Newton qui apparaissent dans la somme optimale unique $\sigma = F_0 + F_1 + F_2$. L'algorithme associe aux cellules qui ont plus qu'un sommet dans cette somme, le sommet F_i d'indice maximal. L'algorithme construit la matrice suivante, de dimension $4 + 4 + 7 = 15$, tandis que les volumes mixtes sont $VM(Q_0, Q_1) = 4$, $VM(Q_1, Q_2) = 4$, $VM(Q_2, Q_0) = 3$ donc $\deg R = 11$. Les lignes et les colonnes de la matrice sont indexées par les points dans $\mathcal{E}$.

	$1,0$	$2,0$	$0,1$	$1,1$	$2,1$	$3,1$	$0,2$	$1,2$	$2,2$	$3,2$	$4,2$	$1,3$	$2,3$	$3,3$	$4,3$
$1,0$	c_{00}	c_{03}	0	0	c_{01}	c_{02}	0	0	0	0	0	0	0	0	0
$2,0$	c_{20}	c_{23}	0	c_{21}	c_{22}	0	0	0	0	0	0	0	0	0	0
$0,1$	0	0	c_{00}	c_{03}	0	0	0	c_{01}	c_{02}	0	0	0	0	0	0
$1,1$	0	0	0	c_{00}	c_{03}	0	0	0	c_{01}	c_{02}	0	0	0	0	0
$2,1$	c_{13}	0	c_{10}	0	c_{12}	0	0	0	c_{11}	0	0	0	0	0	0
$3,1$	0	c_{13}	0	c_{10}	0	c_{12}	0	0	0	c_{11}	0	0	0	0	0
$0,2$	0	0	c_{20}	c_{23}	0	0	c_{21}	c_{22}	0	0	0	0	0	0	0
$1,2$	0	0	0	c_{20}	c_{23}	0	0	c_{21}	c_{22}	0	0	0	0	0	0
$2,2$	0	0	0	0	0	0	0	0	c_{00}	c_{03}	0	0	0	c_{01}	c_{02}
$3,2$	0	0	0	0	c_{20}	c_{23}	0	0	c_{21}	c_{22}	0	0	0	0	0
$4,2$	0	0	0	0	0	c_{13}	0	0	c_{10}	0	c_{12}	0	0	0	c_{11}
$1,3$	0	0	0	0	0	0	0	c_{20}	c_{23}	0	0	c_{21}	c_{22}	0	0
$2,3$	0	0	0	c_{13}	0	0	c_{10}	0	c_{12}	0	0	0	c_{11}	0	0
$3,3$	0	0	0	0	0	0	0	0	c_{20}	c_{23}	0	0	c_{21}	c_{22}	0
$4,3$	0	0	0	0	0	0	0	0	0	c_{20}	c_{23}	0	0	c_{21}	c_{22}

Exercice 5.2 Démontrer que l'élément M_{pp} est c_{ij} si $\mu(p) = a_{ij}$. M est carrée et de dimension $|\mathcal{E}| =$ (Nb de points dans $\mathcal{E}$). □

Lemme 5.3 *Soit $P \subset \mathbb{R}^n$ un parallélotope (= parallélépipède) aux sommets entiers et $\delta \in (\mathbb{Q}^*)^n$ infinitésimal. Le Nb de points entiers dans $P + \delta$ est égal au volume* $\mathrm{Vol}(P)$.

Preuve Utiliser le fait que le Nb de points est $n!\mathrm{Vol}(S)$, où S est la simplexe définie par les arêtes du parallélotope [Sta80, p. 335]. □

Lemme 5.4 *Pour tout $p \in \mathcal{E}$, définir $\widehat{p}_\delta$ comme l'intersection de la verticale qui passe par p avec l'enveloppe inférieure de $\widehat{Q} + \delta$, noté e.i.$(\widehat{Q} + \delta)$. Soit $a_{ij} = \mu(p)$ et $\widehat{a}_{ij} = (a_{ij}, l_i(a_{ij}))$ son relèvement par rapport à l_i. Alors le seul point commun entre $\widehat{p}_\delta - \widehat{a}_{ij} + \widehat{Q}_i$ et e.i.$(\widehat{Q} + \delta)$ est le point $\widehat{p}_\delta$.*

Preuve Indication : Pour tout $\widehat{q} \in \widehat{p}_\delta - \widehat{a}_{ij} + \widehat{Q}_i$, trouver un point $\widehat{q}'$ sur la même verticale t.q. $\widehat{q}'$ est dans $\widehat{Q} + \delta$. On prend $\widehat{p}'' = \widehat{p}_\delta - \epsilon(0, \ldots, 0, 1)$ et $\widehat{q}' = \widehat{q} - \epsilon(0, \ldots, 0, 1)$, pour $\epsilon > 0$ suffisamment petit, et on doit démontrer $\widehat{q}' \in \widehat{Q} + \delta$. Soit $\widehat{p}'$ l'intersection du segment $(\widehat{p}'', \widehat{q}')$ avec e.i.$(\widehat{Q} + \delta)$. Pour δ suffisamment générique p se trouve dans l'intérieur d'une cellule maximale $\sigma + \delta$ donc $\widehat{p}_\delta$ se trouve dans l'intérieur de la facette $\widehat{F} + \delta$ correspondant. Pour petit ϵ, $\widehat{p}'$ se trouve dans l'intérieur de la même facette.

Si $\widehat{p}_\delta = b_0 + \cdots + \widehat{a}_{ij} + \cdots + b_n + \tau(0, \ldots, 0, 1)$, pour $b_i \in \widehat{F}_i$, alors $\widehat{p}' = b'_0 + \cdots + \widehat{a}_{ij} + \cdots + b'_n + \tau(0, \ldots, 0, 1)$ pour $b'_i \in \widehat{F}_i$. □

Lemme 5.5 *Pour de coefficients génériques M est régulière.*

Preuve Indication : On transforme M en deux étapes. (i) $M(t)$ est obtenue en spécialisant chaque entrée c_{ij} de M en $t^{l_i(a_{ij})}$, pour une indéterminé réelle t. (ii) Deuxièmement, on multiplie la ligne qui correspond à $p \in \mathcal{E}$ par $t^{h(p) - l_i(a_{ij})}$, où $\mu(p) = a_{ij}$ et $h(p)$ et la distance verticale (avec signe) de p à

l'enveloppe inférieure de $\widehat{Q} + \delta$. □

Transformation (i) ci-dessus correspond à la spécialisation du système polynomial en $f_i = \sum_j t^{l_i(a_{ij})} x^{a_{ij}}$, qui est vu comme un polynôme en $n+1$ variables x, t. Le polytope de Newton du nouveau polynôme est $\widehat{Q}_i$. Transformation (ii) correspond à une translation de chaque $\widehat{Q}_i$ par $\widehat{p}_\delta - \widehat{a}_{ij}$.

Supposons maintenant que les supports A_i engendrent $\mathbb{Z}^n$.

Théorème 5.6 *M est carrée, génériquement non-singulière, et $R \mid \det M$, c.à.d. que $\det M$ s'annule sur les racines du système. De plus, $\deg_{f_0} \det M = \deg_{f_0} R$ et $\deg_{f_i} \det M \geq \deg_{f_i} R$ pour $i \geq 1$, donc on peut récupérer le résultant comme le PGCD de $n+1$ déterminants.*

Il est possible de construire des matrices pour des systèmes spécifiques en utilisant l'implémentation sur MAPLE accessible par la page Web de l'auteur.

Exercice 5.7 Trouver un relèvement et un vecteur δ pour que l'algorithme construise la matrice de Sylvester pour $n = 1$ et la matrice des coefficients pour un système linéaire. □

Théorème 5.8 [Emi96] *Si $m \geq |\{\text{sommets } Q_i\}|$ et le facteur scalaire du système est constant p.r.à. n et m, alors la complexité binaire totale pour construire la matrice de Newton M et calculer le résultant R est $O^*(e^n \deg R(nm)^6)$ ou $(\deg R)^{O(1)} e^{O(n)}$.*

Nous décomposons M par rapport à $\mathcal{E} \setminus B_0$ et B_0. Les B_0 sont les points dans les cellules 0-mixtes, c.à.d. les cellules exprimées comme une somme d'un sommet dans Q_0 et n arêtes dans $Q_i, i > 0$. Ils sont en bijection avec les points dans les cellules mixtes d'une subdivision mixte des $f_1, \ldots, f_n$ [ER94]. Soit $m = |B_0|$. Notons $b_1, \ldots, b_m$ les monômes dans B_0 (bloc en bas) et $q_c \in \mathcal{E} \setminus B_0$ (bloc en haut). Pour tout α dans la variété des $f_1, \ldots, f_n$,

$$M \begin{bmatrix} \vdots \\ \alpha^{q_c} \\ \vdots \\ \alpha^{b_i} \\ \vdots \end{bmatrix} = \begin{bmatrix} & \\ M_{11} & M_{12} \\ & \\ M_{21} & M_{22} \\ & \end{bmatrix} \begin{bmatrix} \vdots \\ \alpha^{q_c} \\ \vdots \\ \alpha^{b_i} \\ \vdots \end{bmatrix} = \begin{bmatrix} \vdots \\ 0 \\ \vdots \\ \alpha^{b_i} f_0(\alpha) \\ \vdots \end{bmatrix}. \tag{4}$$

Théorème 5.9 *B_0 constitue une base monomiale de l'anneau quotient $K[x^{\pm 1}]/I$ de l'idéal $I = (f_1, \ldots, f_n)$, pourvu que I est radical et zéro-dimensionnel.*

Preuve Nous suivons [ER94]. Premièrement, nous montrons que les vecteurs $v'_\alpha = [\alpha^{b_1}, \ldots, \alpha^{b_m}]$ sont des vecteurs propres de M', puisque $M' v'_\alpha = f_0(\alpha) v'_\alpha \Rightarrow (M' - f_0(\alpha) I_m)\, v'_\alpha = 0$ (ici I_m est la matrice identité $m \times m$). Puisque les racines sont distinctes, en choisissant f_0 de manière générique, nous avons m valeurs propres distinctes, donc m vecteurs propres indépendants. Si les b_i ne forment pas une base de $K[x^{\pm 1}]/I$. Alors la matrice des m vecteurs v'_α évalués aux m racines est singulière, ce qui contradit l'indépendance des vecteurs. □

Soit $M' = M_{22} - M_{21} M_{11}^{-1} M_{12}$.

Théorème 5.10 *Avec les notations du théorème précédant, le complément de Schur M' de la sous-matrice M_{11} qui correspond à $\mathcal{E} \setminus B_0$ (pourvu qu'elle est inversible) donne la matrice de multiplication par f_0 modulo l'idéal I.*

Preuve Les rangées de M' expriment les polynômes $x^{b_i} f_0 \bmod I$, pour quelque $b_i \in B_0$ [ER94]. Pour $g = \sum_{i=1}^m c_i x^{b_i}$,

$$gf_0 \bmod I = \sum_{i=1}^m c_i (x^{b_i} f_0 \bmod I) = \sum_{i=1}^m c_i \left(\sum_{j=1}^m M'_{ij} x^{b_j} \right) = \sum_{j=1}^m x^{b_j} \left(\sum_{i=1}^m c_i M'_{ij} \right).$$

Maintenant on constate que la dernière somme exprime $[c_1, \ldots, c_m]M'$ dans la base B_0. □

Algorithme 5.11 (Paresseux) [CP93] *Soient $L, C \subset \mathcal{E}$ les ensembles indiquant les lignes et les colonnes.*
1. Initialiser L à contenir un point quelconque de $\mathcal{E}$.
2. La fonction μ définit les B_i à partir de L, donc on peut calculer $C = \cup_i (A_i + B_i)$.
3. Si $L = C$ l'algorithme se termine. Sinon, on met $L = C$ et on revient à l'étape 2.

Cet algorithme construit une matrice du résultant creux (dont le déterminant est un multiple non-trivial) même si les A_i engendrent un sous-rśeau propre de $\mathbb{Z}^n$. Une implémentation en Maple se trouve sur la page Web de l'auteur.

5.1 Matrice de Macaulay

Exercice 5.12 Démontrez que le Nb de monômes en x de degré $\leq g$ est égal à $\binom{g+n}{n}$. □

Soit $\nu = \sum_{i=0}^n (d_i - 1) + 1$ le degré critique du système et $|(p_1, \ldots, p_n)| = p_1 + \cdots + p_n$ la norme L_1 d'un vecteur. Pour la construction de Macaulay nous prenons les monômes $\mathcal{E} = \{p \in \mathbb{Z}^n \,:\, |p| \leq \nu, p_i \geq 0, \forall i\}$. Il y a $\binom{\nu+n}{n} = O(e^n d^n)$ monômes dans $\mathcal{E}$, où $d = \max\{d_i\}$. Soit $e_i = (0, \ldots, 0, 1, 0, \ldots, 0) \in \mathbb{R}^n$ le i-ème vecteur canonique avec 1 à la position i.

$$\begin{aligned} B_n &= \{p - d_n e_n \,:\, p \in \mathcal{E}, p_n \geq d_n\}, \\ B_{n-1} &= \{p - d_{n-1} e_{n-1} \,:\, p \in \mathcal{E}, p_{n-1} \geq d_{n-1}, p_n < d_n\}, \\ &\vdots \\ B_0 &= \{p \in \mathcal{E} \,:\, p_i < d_i, \forall i \geq 1\}. \end{aligned}$$

Les $B_i + d_i e_i$ et B_0 sont alors disjoints et leur union est $\mathcal{E}$. La matrice de Macaulay M est maintenant bien définie. Puisque $\deg_{f_i} \det M = |B_i|$, on en déduit que

$$\deg_{f_0} \det M = \prod_{i=1}^n d_i = \deg_{f_0} R(f_0, \ldots, f_n).$$

Pour $i > 0$, $\deg_{f_i} \det M \geq \deg_{f_i} R(f_0, \ldots, f_n)$.

$\mathcal{E} + (1, \ldots, 1)$, où $\mathcal{E}$ est défini ci-dessus, est égal à $(Q + (\epsilon, \ldots, \epsilon)) \cap \mathbb{Z}^n = \{|p| \leq \sum_i d_i, p_i \geq 1\}$.

Exercice 5.13 Étant donnés de polynômes complètement denses, spécifiez un relèvement linéaire et un vecteur δ tels que la matrice de Newton construite à partir de la subdivision mixte correspondante est la matrice de Macaulay. □

Mettons $f_0 = 1, f_i = x_i^{d_i}, i = 1, \ldots, n$. La matrice de Macaulay est la matrice identité de taille $\binom{\nu+n}{n}$, ce qui montre que $\det M \not\equiv 0$. Le complément de Schur de la sous-matrice qui correspond à $\mathcal{E} \setminus B_0$ (pourvu qu'elle est inversible) donne la matrice de multiplication par f_0 dans l'idéal des $f_1, \ldots, f_n$. B_0 constitue une base monomiale de l'anneau quotient de cet idéal.

Théorème 5.14 [Mac02] *La formule de Macaulay précise une sous-matrice M' de M t.q. $R = \det M / \det M'$. M' est la sous-matrice carrée de M indexée par tous les monômes dans $\mathcal{E}$ divisibles par deux monômes différents de type $x_i^{d_i}$. Ceux-ci correspondent aux monômes des cellules* non-mixtes *dans une subdivision mixte.*

5.2 Propriétés du résultant creux et de sa matrice

Une question importante était la généralisation de la formule de Macaulay dans le cas torique (section 5.1). Dans [CE00], on avait énnoncé la conjecture suivante : Il existe une sous-matrice carrée M' de M t.q. $R = \det M / \det M'$ et M' correspond aux monômes des cellules *non-mixtes* de la subdivision mixte Des expériences sur cette conjecture se trouvent dans [CE00], voir aussi l'exemple suivant. Elle était vérifiée pour $n = 2, 3$ et certains choix des paramètres (relèvement, perturbation δ).

Exemple 2.21 (suite)

$$M' = \begin{bmatrix} c_{12} & 0 & 0 & 0 \\ 0 & c_{21} & c_{22} & 0 \\ c_{23} & 0 & c_{21} & 0 \\ 0 & 0 & 0 & c_{22} \end{bmatrix},$$

et $\det M / \det M' = R$, ce qui vérifie la conjecture pour cet exemple.

La conjecture a été démontrée par C. D'Andrea (Trans.AMS,2002) avec une définition recursive de la matrice, et des cellules (non)mixtes. Reste ouverte la question d'avoir un seul relèvement pour construire la matrice, ce que nous pouvons établir pour $n = 2$ et les systèmes réduits (un sommet soutenu pour au moins un polytope de Newton, pour chaque normale possible).

La version effective du théorème des zéros de Hilbert était établie par Brownawell et Kollàr. Pour l'idéal $(f_1, \ldots, f_r) = (1)$, $1 = \sum_i f_i g_i$ avec $\deg(f_i g_i) \leq 2(d+1)^n$, où d borne le degré des f_i.

Corollaire 5.15 [CE00] *Une version effective du théorème des zéros de Hilbert pour le cas creux générique : Si $(f_0, \ldots, f_n) = (1)$, le polytope de Newton de g_i est contenu dans $Q_0 + \cdots + Q_{i-1} + Q_{i+1} + \cdots + Q_n$.*

Conjecture 5.16 [CE00] *Le même résultat pour les polynômes aux coefficients arbitraires (pas génériques). De plus, pour un nombre arbitraire de polynômes ($r \neq n+1$).*

Commençons avec une généralisation de la construction de la subdivision mixte proposée par [Stu94] afin de démontrer certaines propriétés du polytope de Newton du résultant creux. Soit $m = \sum_i |A_i|$ et $w : \mathbb{Z}^m \to \mathbb{R}$ la fonction qui définit un relèvement (généralisé) $w \cdot (\ldots, \nu_{ij}, \ldots)$ pour chaque monôme de coefficients $\prod_{i,j} c_{ij}^{\nu_{ij}}$. Alors, on peut associer à chaque exposant $a_{ij} \in A_i$ le relèvement $w \cdot (0, \ldots, 0, 1, 0, \ldots, 0) = l_i(a_{ij})$, avec l'unité à la position (i, j).

Le relèvement généralisé s'applique ainsi à tous les monômes du résultant. On parle, donc, des termes les moins significatifs p.r.à un relèvement w ; ils définissent la forme "terminale" du résultant. C'est l'inverse de la forme initiale définie par la somme de tous les terms les plus significatifs.

Théorème 5.17 [Stu94] *Supposons que $\{A_0, \ldots, A_n\}$ est un ensemble essentiel. Soit w un relèvement suffisamment générique et Δ la subdivision mixte induite de $Q = \sum_i Q_i$. La forme terminale du résultant creux R p.r.à w est égale au terme :*

$$C \cdot \prod_{i=0}^{n} \prod_{F} c_{ij}^{\mathrm{Vol}(F)} \qquad : \qquad F \text{ cellule } i\text{-mixte de } \Delta,$$

où C est une constante, $F = F_0 + \cdots + a_{ij} + \cdots + F_n$, $a_{ij} \in A_i$.

Preuve Dans la preuve du théorème 2.41, nous avions défini

$$f_i'(x,t) = \sum_{a \in A_i} c_{ia} x^a t^{l_i(a)},$$

dont le polytope de Newton est $\widehat{Q}_i \in \mathbb{R}^{n+1}$. Soit R' le résultant des $f_i', i = 0, \ldots, n$, obtenu par R en remplaçant c_{ia} par $c_{ia} t^{l_i(a)}$. En regardant R' comme un polynôme en t, son terme terminal a pour

coefficient la forme terminale de R. Il suffit de montrer que ce coefficient est égal à $C_0 \prod_F c_{0j}^{\mathrm{Vol}(F)}$, pour toute cellule 0-mixte F, et C_0 ne dépend que des $c_{ij}, i > 0$. La formule de Poisson donne

$$R' = C_0 \prod_{\gamma(t)} f_0'(\gamma(t)) = C_0 \prod_{\gamma(t)} \sum_{a \in A_0} c_{0a} \gamma(t)^a t^{l_0(a)}, \tag{5}$$

où C_0 ne dépend que des $c_{ij}, i > 0$, et $\gamma(t)$ est un vecteur de séries de Puiseux dans $(\mathbb{C}((t))^*)^n$ qui exprime toutes les racines de $f_1' = \cdots = f_n' = 0$:

$$\gamma(t) = (\gamma_1 t^{\lambda_1}, \ldots, \gamma_n t^{\lambda_n}) + \text{ termes supérieurs en } t.$$

Il y a $VM(f_1, \ldots, f_n)$ racines, ce qui borne le nombre de $\gamma = (\gamma_1, \ldots, \gamma_n) \in (\mathbb{C}^*)^n$ et de $\lambda = (\lambda_1, \ldots, \lambda_n) \in \mathbb{Q}^n$. En remplaçant, on obtient

$$f_i' = \sum_{a \in A_i} c_{ia} \gamma^a t^{(\lambda, a) + l_0(a)} + \text{ termes supérieurs en } t, \tag{6}$$

pour $i = 1, \ldots, n$. Notons que l'exposant typique s'écrit $(\lambda, 1) \cdot (a, l_0(a))$. Soit $\widehat{F}_i$ la face de $\widehat{Q}_i$ où $(\lambda, 1)$ se minimise, $i = 0, \ldots, n$. Donc $F = \sum_i F_i$ est une cellule, de dimension $\leq n$, dans la subdivision Δ. Fixons un $\gamma(t)$: pour qu'il soit une solution, le système

$$\sum_{a \in A_i \cap F_i} c_{ia} \gamma^a = 0, \quad i = 1, \ldots, n,$$

doit avoir une solution pour γ, donc $\dim F_i \geq 1, i \geq 1$. Puisque le relèvement w est générique, F est 0-mixte. Maintenant, $f_0'(\gamma(t))$ dans (5) prend la forme de (6), et son terme terminal p.r.à t est égal à $c_{0F_0} \gamma^{F_0}$. Il y a $VM(F_1, \ldots, F_n) = \mathrm{Vol}(F)$ de telles racines, donc le terme terminal de R', pour cette cellule F, devient $c_{0F_0}^{\mathrm{Vol}(F)} C_0$, où C_0 est le produit des γ^{F_0} et ne dépend que des $c_{ij}, i > 0$. □

Ce théorème implique une *surjection* des subdivisions mixtes de $Q = \sum_i Q_i$ sur les monômes extrêmes du résultant R. Cela généralise un fait implicite au théorème 5.6 :

Corollaire 5.18 *Si la matrice de Newton est construite à partir d'une subdivision mixte de Q définie par l'enveloppe inférieure de $\widehat{Q}$, pour un relèvement généralisé w suffisamment générique, alors le terme le moins significatif du résultant creux divise le produit des entrées diagonales de la matrice. Cela implique que le coefficient de chaque monôme extrême de R est ± 1.*

D'autres propriétés, notamment sur le polytope de Newton de R, sont considérées par la suite.

Théorème 5.19 [Stu94] *Supposons que $\{A_0, \ldots, A_n\}$ est un ensemble essentiel. Soit w un relèvement* arbitraire *et Δ la subdivision mixte induite (pas forcement exacte) de $Q = \sum_i Q_i$. La forme terminale du résultant creux R p.r.à w est égale à :*

$$\pm \prod_F R(f_0|_{F_0}, \ldots, f_n|_{F_n})^{d_F}, \quad F = F_0 + \cdots + F_n \text{ est toute facette de } \Delta,$$

où $f_i|_{F_i}$ est f_i restreint à la face $F_i \subset Q_i$ et $d_F \in \mathbb{N}$ est t.q. $R(f_i|_{F_i})^{d_F}$ ait degré égal à $\sum_i VM(\ldots, F_{i-1}, F_{i+1}, \ldots)$.

Nous présentons maintenant un outil important de la théorie d'élimination, dit astuce de Cayley. Rappelons-nous que le *discriminant* d'un polynôme $F \in K[z_1^{\pm 1}, \ldots, z_N^{\pm 1}]$ est un polynôme en les coefficients de F et aux coefficients entiers, tel qu'il s'annule ssi F a une racine double dans $\overline{K}^N$ ou, de manière équivalente, quand $F = 0$ et $\partial F / \partial z_i = 0$, pour $i = 0, \ldots, N$. Si $A = \mathrm{supp}(F) \subset \mathbb{Z}^N$, une approche naive pour calculer le discriminant serait de prendre le résultant p.r.aux supports $A, A^* - e_i, i = 1, \ldots, n$; notons ce résultant $P(F)$. Mais le discriminant est un facteur propre de $P(F)$ [Stu94].

Proposition 5.20 (Astuce de Cayley) *Le résultant creux de $f_0, \ldots, f_n \in K[x_1, \ldots, x_n]$ est égal au discriminant de $F = f_0 + y_1 f_1 + \cdots + y_n f_n$, pour n nouvelles variables y_i.*

Preuve Quand les $f_i(x) = 0$ s'annulent, alors $F = 0$ et $\partial F/\partial y_j = f_j = 0$. De plus, il y a de y_j qui font annuler les n équations $\partial F/\partial x_i$, $i = 0, \ldots, n$. Inversement, si F et ses derivés s'annulent, alors les f_i s'annulent. □

Corollaire 5.21 *Les subdivisions mixtes (induites, cohérentes, et exactes ou régulières) de $A_0 + \cdots + A_n$ sont en bijection avec les triangulations régulières (c.à.d. induites, cohérentes et exactes) de l'ensemble de points*

$$C = \bigcup_{i=0}^{n} A_i \times \{e_i\} \subset \mathbb{Z}^{2n},$$

où les e_i forment une base affine de $\mathbb{Z}^n$.

Preuve Les A_i sont les supports des f_i et C est celui de F, dans la proposition 5.20. Une subdivision induite, cohérente, et exacte d'un ensemble de points n'est rien d'autre qu'une triangulation avec ces propriétés, autrement dit, régulière. □

Évidemment, $|C| = \sum_{i=0}^{n} |A_i|$. Pour toute triangulation T de C, on utilise la fonction de volumes comme fonction caractéristique :

$$\phi_T : C \to \mathbb{R} : c \mapsto \sum_{c \in \text{ sommets}(\sigma)} \text{Vol}(\sigma).$$

On définit le *polytope secondaire* Σ comme l'enveloppe convexe des vecteurs $\phi_T(C) \in \mathbb{R}^{|C|}$ pour toute triangulation T.

Théorème 5.22 [GKZ94, Th.7.1.7] *Le polytope secondaire Σ d'un ensemble $C \subset \mathbb{Z}^N$ est de dimension $|C| - N - 1$. L'ensemble des triangulations* régulières *de C correspondent aux sommets de Σ. Chaque cône normal à une face de Σ est précisemment un cône de relèvements qui induisent les triangulations correspondantes à cette face.*

De plus, Σ est le polytope de Newton de $P(F)$ [GKZ94, Stu94]. Alors le polytope de Newton $Q(R)$ du résultant creux R des f_i est un terme dans une décomposition de Minkowski de Σ. Mais $Q(R), \Sigma$ sont de la même dimension :

Théorème 5.23 *Soit $Q(R)$ le polytope de Newton du résultant creux. Sous la condition que l'ensemble des A_i soit essentiel (voir corollaire 3.12), alors*

$$\dim Q(R) = \sum_{i=0}^{n} |A_i| - 2n - 1$$

et il existe une transformation affine qui envoie $Q(R)$ au polytope de Newton du résultant creux d'un système essentiel pour lequel $|A_i| \geq 3, \forall i$.

Dans [MC00] les auteurs décrivent l'envellope convexe $\Sigma(A_0, \ldots, A_n)$ de toutes les subdivisions mixtes générales, c.à.d. les subdivisions de la somme de Minkowski $\sum_i A_i$ qui ne sont forcement ni induites, ni cohérentes, ni exactes (régulières). Les sommets de cette envellope correspondent aux subdivisions mixtes, c.à.d. induites (donc cohérentes) et exactes (régulières). Les $\Sigma(A_0, \ldots, A_n)$ et Σ doivent être isomorphes (via Cayley).

Considérons les configurations de cellules mixtes de $\sum_i A_i$, c.à.d. les classes de subdivisions mixtes (induites et exactes) qui contiennent les mêmes cellules mixtes. D'après le théorème 5.17, $Q(R)$ correspond justement au polytope dont les sommets sont ces configurations de cellules mixtes. [2]

Nous avons vu que $Q(R)$ est un terme dans la décomposition de Minkowski de $\Sigma(A_i)$. Il est logique (mais pas dit explicitement) que ces configurations forment le polytope $\Xi(A_i)$, défini dans [MC00, Th.6.6], voir aussi leur Figure 8. Ils montrent que $\Xi(A_i)$ est un terme dans la décomposition de Minkowski de $\Sigma(A_i)$, ce qui est attendu d'après la discussion ci-dessus. [3]

6 Autres formules

6.1 Matrice de Newton par construction incrémentale

Les lignes de M ci-dessus contiennent $x^b f_i : b \in \mathcal{E}_i = (Q_0 + \cdots + Q_{i-1} + Q_{i+1} + \cdots + Q_n + \delta) \cap \mathbb{Z}^n$.

Algorithme 6.1 (Incrémental) [EC95] *1. Trier les monômes $\mathcal{E}_i$, p.r.à la fonction $dist_v(p) := \max\{\lambda \in \mathbb{R}_{\geq 0} : p + \lambda v \in conv(\mathcal{E}_i)\}$ associée à un vecteur fixe $v \in \mathbb{Q}^n$.*
2. Construire M : les monômes $\{b \in \mathcal{E}_i : dist_v(b) > \beta\}$, pour une borne $\beta > 0$, définissent les lignes qui contiennent $x^b f_i$; colonnes définies par les lignes.
3. Ajouter des lignes (et des colonnes) en diminuant β. Arrêter quand M a au moins autant de lignes que de colonnes et $\det M$ est génériquement non-nulle.

Implémentation en `C` sur la page Web de l'auteur.

Théorème 6.2 *M est carrée, génériquement non-singulière, et $R \mid \det M$, c.à.d. $\det M$ s'annule sur les racines du système. De plus, on peut imposer $\deg_{f_1} \det M = \deg_{f_1} R$. La complexité est $e^{O(n)}(\deg R)^3$, en supposons qu'on trouve un bon vecteur v après un nombre constant d'essais.*

Le choix de v devient la question principale. En général, on choisit v de façon aléatoire, sauf dans certains cas où il y de choix qui garantissent la construction des matrices compactes.

Exercice 6.3 Démontrez que pour certains choix du vecteur v, l'algorithme incrémental construit la matrice de Sylvester pour $n = 1$ et la matrice des coefficients pour un système linéaire dense. □

On étudie maintenant des systèmes multi-homogènes. Si un système est non-mixte (supports identiques), on pose d_i le degré de chaque polynôme en X_i. On définit le type du système d'être $(l_1, \ldots, l_r; d_1, \ldots, d_r)$.

Théorème 6.4 [SZ94] *Soit un système multi-homogène non-mixte et dense t.q. pour chaque $i = 1, \ldots, r$, $l_i = 1$ ou $d_i = 1$. Alors, pour chaque permutation $\pi \in S(r)$, il existe une matrice (de type Sylvester) dont le déterminant est égal au résultant creux.*

Corollaire 6.5 [EC95] *L'algorithme incrémental construit toutes les matrices optimales décrite par le théorème ci-dessus.*

Cette classe de systèmes comprend :
- le cas $n = 1$, pour lequel on obtient le résultant de Sylvester,
- le cas $r = n$ et $d_i = 1, \forall i$, pour lequel le résultant est le déterminant des coefficients du système linéaire,

[2] Ces configurations sont calculées dans [MV99], sans exploiter leur plongement eventuel comme polytope.
[3] Par contre, le cas $n = d + 1$, où d est la dimension de l'espace ambient, est interdit dans [MC00, Th.6.6] ! (soit il s'agit d'une erreur, soit je n'ai pas compris).

– le cas $r = n = 2$, $l_1 = l_2 = 1$ traité par Dixon [Dix08]. La matrice proposée par Dixon donne le résultant exact dans le cas (dense) bi-homogène de type $(1, 1; d_1, d_2)$, c.à.d. $n = 2$. Chaque support contient $(d_1 + 1)(d_2 + 1)$ monômes. En prenant $B_i = \{p \in \mathbb{Z}^2 : p_1 < 2d_1, p_2 < d_2\}$, $i = 0, 1, 2$ nous construisons une matrice carrée de dimension $3|B_0| = 6d_1d_2$, puisque $B = B_i + A_i = \{p \in \mathbb{Z}^2 : p_1 < 3d_1, p_2 < 2d_2\}$. Son déterminant est égal au résultant. On pourrait aussi poser $B_i = \{p \in \mathbb{Z}^2 : p_1 < d_1, p_2 < 2d_2\}$, ce qui donne $B = \{p \in \mathbb{Z}^2 : p_1 < 2d_1, p_2 < 3d_2\}$ et une autre matrice de la même dimension et le même déterminant.

Sturmfels et Zelevinsky ont conjecturé qu'il n'existe pas de matrices optimales pour les systèmes denses t.q. $\exists i \ : l_i, d_i \geq 2$. Toutefois, en utilisant la même définition pour le vecteur v on arrive à construire de matrices dont la taille est proche à $\deg R$ [EC95].

Exercice 6.6 Dans un cas où tous les polytopes de Newton sont égaux est suffisament proche d'un parallélotope, la condition sur les nombres de lignes et de colonnes devient

$$(n+1) \cdot |\beta A_0 \cap \mathbb{Z}^n| \geq |(\beta+1)A_0 \cap \mathbb{Z}^n| \Leftrightarrow (n+1)\beta^n V(A_0) \geq (\beta+1)^n V(A_0) \Leftrightarrow n+1 \geq (1+\frac{1}{\epsilon})^n,$$

pour $0 < \epsilon = 1/\beta < 1$. Étudier les solutions de cette inegalité pour $n \leq 10, n \to \infty$. Pareil pour la rélation entre la dimension de la matrice et le degré total du résultant torique (cf. [Emi96]). □

6.2 La matrice de Bézout

Ici on considère $n + 1$ polynômes

$$f_0, \ldots, f_n \in K[x_1, \ldots, x_n] = K[x]$$

et on suppose qu'ils sont (denses) de degré total d_i. Notons $y = (y_1, \ldots, y_n)$ un nouveau ensemble de variables. On définit le Bézoutien :

$$\delta(x, y) = \begin{vmatrix} f_0(x) & f_0(y_1, x_2, \ldots, x_n) & \cdots & f_0(y) \\ f_1(x) & f_1(y_1, x_2, \ldots, x_n) & \cdots & f_1(y) \\ \vdots & \vdots & & \vdots \\ f_n(x) & f_n(y_1, x_2, \ldots, x_n) & \cdots & f_n(y) \end{vmatrix}.$$

Puisque $\delta(x_1, \ldots, x_{i-1}, y_i, x_{i+1}, \ldots, x_n, y) = 0$ pour $i = 1, \ldots, n$, $x_i - y_i \mid \delta$, donc

$$\Delta(x, y) = \frac{\delta(x, y)}{\prod_{i=1}^n x_i - y_i} = \sum_b \theta_b(x) y^b, \qquad b \in \mathbb{N}^n,$$

est un polynôme en x, y.

Lemme 6.7 *Le degré total de $\Delta(x, y)$ est $\sum_{i=0}^n d_i - n$. Si tous les $d_i = d$, le degré de $\Delta(x, y)$ en x et en y est égal à $nd - n$, donc la dimension de la matrice est de $\binom{nd}{n}$. De plus, le degré en les coefficients de f_i est $\deg_{f_i} \Delta(x, y) = 1$, pour $i = 0, \ldots, n$.*

Preuve Le degré total de $\delta(x, y)$ est $\sum_{i=0}^n d_i$. Son degré en x est $\deg_x \delta = nd$, si tous les polynômes ont le même degré total d. Le degré en les coefficients de f_i est $\deg_{f_i} \delta(x, y) = 1$. □

Si le monôme y^b est de degré total $\deg(y^b) = |b|$, alors $\theta_b(x)$ est de degré $\leq \sum_i \deg f_i - n - |b|$.

Exercice 6.8 Démontrez que si la matrice Φ, dont les lignes expriment les θ_b p.r.aux monômes en x, est carrée, alors $R \mid |\Phi|$. □

Proposition 6.9 [EM02] *Si l'idéal $I = (f_1, \ldots, f_n)$ est zéro-dimensionnel, les monômes en x (ou en y) dans le Bézoutien des $1, f_1, \ldots, f_n$ contiennent une base de l'anneau quotient $K[x]/I$ ou $K[x^{\pm 1}]/I$.*

Lemme 6.10 $\Delta(f_0,\dots,f_n) = f_0\Delta(1,f_1,\dots,f_n) + f_1\Delta(f_0,1,f_2,\dots,f_n) + \cdots + f_n\Delta(f_0,\dots,f_n,1)$.

La matrice de Bézout est liée au résidu algébrique. Tout mineur maximal non-nul de Φ est divisible par le résultant [CM96, EM02, Mou97].

Les avantages de l'approche de Bézout p.r.aux méthodes liées à la matrice de Newton : la petite taille de la matrice de Bézout la rend plus efficace dans le calcul du résultant R lui-même (par interpolation), elle peut être définie pour une spécialisation des coefficients, la symétrie en x et y rend la matrice de Bézout plus facile à comprimer.

Par contre, la matrice de Bézout, pour son calcul demande le développement d'un déterminant Δ, ses entrées sont des polynômes en les coefficients (donc en la variable cachée), et elle n'exploite pas forcement la structure géométrique des monômes.

6.3 Autres formulations

Dixon [Dix08] a proposé des matrices avec une partie à la Sylvester et une autre à la Bézout. En général, et comme pour le Bézoutien du cas $n = 1$, on peut construire une matrice M qui contient $\mu \in \mathbb{N}$ lignes correspondant aux $\theta_b(x)$ et ν lignes exprimant de multiples $x^t f_i(x)$ pour chaque polynôme $f_i(x)$, $i = 0,\dots,n$, suivant la notation de la section précédante. Une façon pour construire une matrice de résultant est de poser les contraintes combinatoires suivantes : $|b| \geq l \in \mathbb{N}$ et $|t| \leq k \in \mathbb{N}$, où les $t \in \mathbb{N}^n$ définissent les monômes qui multiplient chaque $f_i(x)$. $|b| \geq l \Rightarrow$ degré de monôme en $x \leq (n+1)d - n - l$. Pour que M soit carrée, on doit avoir :

$$\begin{aligned}
\text{nb lignes } = (\text{nb monômes } b \text{ choisis}) &\Leftrightarrow \mu + (n+1)\nu = \binom{(n+1)d-l}{n},\\
\exists \nu \text{ monômes distincts de degré } \leq k &\Leftrightarrow \nu \leq \binom{k+n}{n},\\
x^t f_i(x) \text{ exprimés en les monômes } b \text{ choisis} &\Leftrightarrow k + d \leq (n+1)d - n - l \Leftrightarrow k \leq nd - n - l.
\end{aligned}$$

De plus, pour que $|M| = R$ on doit avoir $\deg_{f_i} |M| = \deg_{f_i} R \Leftrightarrow \nu + \mu = d^n$.

Cela revient à un problème combinatoire qui a des solutions entières pour μ, ν, l, k seulement dans certains cas. Quelques-unes sont décrites dans [Jou97].

Exercice 6.11 Démontrez que si M est carrée, alors $\det M = R$. □

Exercice 6.12 Généraliser la discussion aux systèmes non-mixtes de polynômes denses dont le degré en x_i est d_i, c.à.d. multi-homogènes de type $(1,\dots,1;d_1,\dots,d_n)$. □

Une implémentation générale se trouve sur `http ://www-sop.inria.fr/galaad/Bernard.Mourrain`.

Nous pouvons utiliser le Jacobien (resp. torique) pour réduire la taille de la matrice de Macaulay (resp. Newton) [CDS98, Jou97]. Une autre façon pour construire des matrices de résultant est proposée par Morley [MC27], repris par Jouanolou [Jou97].

7 Structure des matrices

Définition 7.1 *Une matrice* (M_{ij}) *est* Toeplitz ou Töplitz *(resp.* Hankel*) si* $M_{ij} = M_{(i+k)(j+k)}$ $(M_{ij} = M_{(i+k)(j-k)})$ *pour tout* $i,j,k \in \mathbb{Z}$ *possible.*

Autrement dit, les matrices Toeplitz (resp. Hankel) ont des diagonales (anti-diagonales) constantes. L'entrée M_{ij} d'une matrice Toeplitz (resp. Hankel) ne dépend que de l'entier $i - j(i+j)$. La matrice de Sylvester contient deux blocs Toeplitz.

Exemple 7.2 Soit $A(x) = a_0 + a_1x + a_2x^2$ et $B(x) = b_{-2}x^{-2} + b_{-1}x^{-1} + b_0 + b_1x$ deux polynômes univariés de Laurent dans $K[x^{\pm 1}]$. Exprimons $A(x)$ comme un vecteur V dans la base monomiale canonique, et $B(x)$ par une matrice Toeplitz M, avec b_0 sur la diagonale.

$$[a_0, a_1, a_2] \begin{bmatrix} b_0 & b_1 \\ b_{-1} & b_0 \\ b_{-2} & b_{-1} \end{bmatrix} = [a_0b_0 + a_1b_{-1} + a_2b_{-2}, a_0b_1 + a_1b_0 + a_2b_{-1}].$$

Le produit $A(x)B(x)$ dans la base monomiale est le vecteur obtenu par la multiplication V^TM. □

La multiplication d'un vecteur avec une matrice Toeplitz exprime la multiplication de deux polynômes en une variable donc les deux opérations ont la même complexité. Le nombre d'opérations arithmétique élémentaires pour la multiplication de deux polynômes univariés, de degrés $\leq d$, est dans $O(d \log d)$. Cette borne est fondée sur la méthode d'évaluation et d'interpolation aux racines complexes de l'unité, dite méthode de la transformé de Fourier rapide (Fast Fourier Transform). Soit d une borne sur les dimensions d'une matrice Toeplitz. Si nous pouvons appliquer FFT, alors résoudre le système linéaire, calculer le déterminant ou les coefficients du polynôme caractéristique et inverser la matrice sont, respectivement, de complexité $O(d \log^2 d), O(d^2 \log d), O(d^2)$ [BP94].

Les matrices de Macaulay et de Newton sont des matrices quasi-Töplitz [EP97]. La multiplication d'un vecteur à gauche, vu comme le vecteur des coefficients de polynômes $g_0, \ldots, g_n$, est équivalent au calcul de la somme des produits $\sum_{i=0}^{n} f_i g_i$.

Exercice 7.3 Écrire la somme $\sum_{i=0}^{n} f_i g_i$ comme une seule multiplication de deux polynômes en $n+1$ variables, notées $x_1, \ldots, x_n, y$. □

Pour passer aux matrices Hankel, définissons une matrice $n \times n$, $J = J^{-1} = (J_{ij})$, $J_{i,n+1-i} = 1$ sinon $J_{ij} = 0$. Alors MJ, JM sont Hankel (resp. Toeplitz) si M est Toeplitz (resp. Hankel). Cette propriété réduit les calculs des matrices Hankel à ceux de matrices Toeplitz. La matrice de Bézout dans le cas univarié est liée à une matrice Hankel. Par exemple, pour $n = 1$ et $d_1 = 1$, Φ est une matrice Hankel. Avec plusieurs variables, la matrice de Bézout est liée à une matrice quasi-Hankel [MP00].

8 Résolution de systèmes algébriques

Supposons qu'un système bien-contraint est donné

$$f_1, \ldots, f_n \in K[x_1, \ldots, x_n],$$

dont la variété est de dimension zéro (racines isolées), c.à.d. on se pose dans le cas d'une suite régulière définissant une intersection complète. De plus, on suppose pour le moment que l'idéal $(f_1, \ldots, f_n)$ est radical (racines simples). Comment utiliser le résultant creux pour calculer les racines dans $(\overline{K}^*)^n$ (voire dans $\overline{K}^n$) ?

On définit un système surcontraint

– soit en ajoutant un polynôme linéaire

$$f_0 = r_1x_1 + \cdots + r_nx_n + u$$

dense et suffisamment générique pour $r_i \in K$ et u indéterminé,

– soit en "cachant" une variable x_i dans le corps des coefficients,

$$f_1, \ldots, f_n \in (K[x_n])\,[x_1, \ldots, x_{n-1}].$$

On revient, effectivement, à la situation de $n+1$ polynômes en n variables. Soit x la nouvelle variable u ou la variable cachée. On construit la matrice du résultant $M(x)$ par une des méthodes décrites c.à.d. un des trois algorithmes pour la matrice de Newton ou de Bézout, ou même la matrice de Macaulay. $M(x)$ est une matrice en une variable, de degré d; $d=1$ si on a ajouté un polynôme, sinon d est le degré maximal de la variable cachée dans les f_i.

Représentation univariée rationnelle : En ajoutant le polynôme f_0, le déterminant de nos matrices se factorise, à un scalaire près, en $\prod f_0(\alpha)$ (rappelez-vous de la forme de Poisson) [Rou98].

8.1 Valeurs et vecteurs propres

Théorème 8.1 *Supposons que $|M(x)| \neq 0$, où $M(x)$ est la matrice du résultant pour un système $f_0,\ldots,f_n$ en $x_1,\ldots,x_n$. Soient $x_i=\alpha_i$, $i=1,\ldots,n$, $x=\beta$ une solution commune et $v_\alpha = [\alpha^{m_1},\ldots,\alpha^{m_t}]^T$, alors $|M(\beta)|=0$ et $M(\beta)v_\alpha=0$, où v_α est l'évaluation à α des monômes indexant les colonnes de la matrice.*

Lemme 8.2 [Emi96] *Étant donné $v_\alpha=[\alpha^{m_1},\ldots,\alpha^{m_t}]^T$, on peut récupérer α en prenant de fractions des entrées du vecteur.*

Si $M(x)=M_dx^d+\cdots+M_1x+M_0$ et $|M_d|\neq 0$ le calcul de β, v_α se réduit au problème de valeurs et vecteurs propres classiques :

$$\det M(x) = \det M_d \det(I_N x^d + \cdots + M_d^{-1}M_1 x + M_d^{-1}M_0)$$

et $M(x)$ est singulière ssi x prend les valeurs propres de la matrice *compagnon* C. De plus, il y a une correspondance entre les v_α et les vecteurs propres de C :

$$M(\beta)v_\alpha = 0 \Leftrightarrow \left(\begin{bmatrix} 0 & I_N & & 0 \\ \vdots & & \ddots & \\ 0 & 0 & & I_N \\ -M_d^{-1}M_0 & \cdots & \cdots & -M_d^{-1}M_{d-1} \end{bmatrix} - \beta I_{Nd} \right) \begin{bmatrix} v_\alpha \\ \beta v_\alpha \\ \vdots \\ \beta^{d-1}v_\alpha \end{bmatrix} = 0.$$

Par contre, si $|M_d|=0$, on arrive au problème de valeurs et vecteurs propres généralisés [GV96] :

$$M(\beta)v_\alpha = 0 \Leftrightarrow \left(\begin{bmatrix} 0 & I_N & & \\ & & \ddots & \\ & & & I_N \\ -M_0 & -M_1 & \cdots & -M_{d-1} \end{bmatrix} - \beta \begin{bmatrix} I_N & & & \\ & \ddots & & \\ & & I_N & \\ & & & M_d \end{bmatrix} \right) \begin{bmatrix} v_\alpha \\ \beta v_\alpha \\ \vdots \\ \beta^{d-1}v_\alpha \end{bmatrix} = 0.$$

Exercice 8.3 Comment peut-on traiter le cas $M(x)=0$? □

Exercice 8.4 Assouplissez la condition que l'idéal doit être radical. Indication : le problème se pose quant aux espaces de vecteurs propres qui doivent être de dimension 1 pour qu'on puisse récupérer les α_i. □

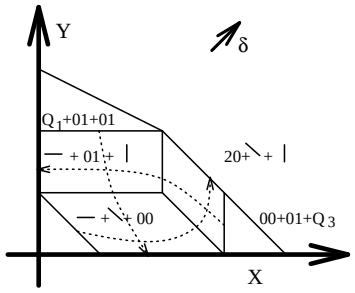
8.2 Applications

Exercice 8.5 Système [CLO05, sect.3.2,p.82] : $c_0+s+t+st, c_1+s+3t+st, c_2+s-t+st$, voir l'exemple 3.21. Montrez que son résultant projectif s'annule mais son résultant creux est non-nul. □

Exemple 8.6 Calculer les intersections d'une parabole arbitraire avec une ligne qui passe par l'origine sur le plan. Pour résoudre le système 2×2, on ajoute une forme linéaire en u.

$$f_0 = c_{00}x^2 + c_{01}x + c_{02} + c_{03}y,\ f_1 = c_{10}x + c_{11}y,\ f_2 = r_1x + r_2y + u.$$

On commence avec le premier algorithme de la matrice de Newton. La subdivision mixte de la somme $Q = Q_0 + Q_1 + Q_2$ utilisée pour construire la matrice M paraît ci-dessous, avec les expressions uniques pour chaque cellule maximale, comme somme de faces. Les flèches pointillées montrent le "chemin" de chaque face pour arriver au bord de Q. On voit aussi le vecteur de perturbation δ.



On construit la matrice de Newton pour le système générique en utilisant cette subdivision. Notons que la même matrice est obtenue si on utilise l'algorithme paresseux commençant par le point $(3,1)$.

		$(3,1)$	$(1,2)$	$(2,2)$	$(1,1)$	$(2,1)$
$(3,1)$	$X^{(3,1)-(2,0)} f_0 = xyf_0$	c_{00}	c_{03}	0	c_{02}	c_{01}
$(1,2)$	$X^{(1,2)-(0,1)} f_1 = xyf_1$	0	c_{11}	0	0	c_{10}
$(2,2)$	$X^{(2,2)-(0,1)} f_1 = x^2yf_1$	c_{10}	0	c_{11}	0	0
$(1,1)$	$X^{(1,1)-(0,0)} f_2 = xyf_2$	0	r_2	0	u	r_1
$(2,1)$	$X^{(2,1)-(0,0)} f_2 = x^2yf_2$	r_1	0	r_2	0	u

On observe que la matrice dans ce cas est exacte, puisque le nombre de lignes en f_0, f_1, f_2 est respectivement le degré du résultant creux en ces polynômes $VM(Q_1, Q_2) = 1, VM(Q_0, Q_2) = 2, VM(Q_0, Q_1) = 2$.

Exercice 8.7 Trouver un relèvement l_i qui aboutit à la subdivision montrée. □

Voici une session MAPLE pour une spécialisation du système :

```
with(linalg):
c00 := 1: c01 := 0: c02 := 0: c03 := 1:           # parabole y = -x^2
c10 := 2: c11 := 3:                               # droite 2x+3y=0
r1 := 82: r2 := 71:                               # aleatoires

M := matrix([
[ c00, c03, 0, c02, c01],
[   0, c11, 0,   0, c10],
[ c10, 0, c11,   0,   0],
[  0, r2,   0,   u,  r1],
[ r1,  0,  r2,   0,   u]
]);
det(M);                          # 9u^2 + 208u

read `maplib` :                  # disponible sur le Web
M0 := spec_matrix (M,5,u,0);     # arguments: matrice, dimension, variable, valeur
V0 := kernel(M0);                # {[ 0, 0, 0, 1, 0 ]}
x0 := V0[1][5] / V0[1][4]; y0 := V0[1][2] / V0[1][4];     # (0,0)
M1 := spec_matrix (M,5,u,-208/9);
V1 := kernel(M1);                # {[ -3/2, 3/2, 1, -27/8, -9/4 ]}
x1 := V1[1][5] / V1[1][4]; y1 := V1[1][2] / V1[1][4]; # (2/3,-4/9)
```

On arrive donc à calculer les deux points d'intersection. Maintenant, comparaisons avec l'algorithme incrémental. On choisit $v = (100, 101)$ et voici la partie intéressante des ensembles des points avec leur distance p.r.à v :

$$\begin{aligned}\mathcal{E}_0 &= \{(0,1;0.0049),(1,0;0.0049)\},\\ \mathcal{E}_1 &= \{(0,0;0.0132),(1,0;0.0099),(0,1;0.0066),(2,0;0.0049)\},\\ \mathcal{E}_2 &= \{(1,0;0.0099),(0,1;0.0066),(2,0;0.0049)\}.\end{aligned}$$

Ces ensembles définissent la matrice 9×7 `Minit`, en MAPLE, où les colonnes sont indexées par la séquence de monômes $[2,1],[1,1],[0,1],[0,2],[1,0],[2,0],[3,0]$:

```
Minit := matrix([
[ c00, c01, c02, c03, 0, 0, 0],
[ 0, c03, 0, 0, c02, c01, c00],
[ 0, 0, c11, 0, c10, 0, 0],
[ 0, c11, 0, 0, 0, c10, 0],
[ 0, c10, 0, c11, 0, 0, 0],
[ c11, 0, 0, 0, 0, 0, c10],
[ 0, r2, 0, 0, u, r1, 0],
[ 0, r1, u, r2, 0, 0, 0],
[ r2, 0, 0, 0, 0, u, r1]
]);
```

Dans cette matrice il y a une sous-matrice 7×7 M qui est non-singulière et donne, donc, un multiple du résultant. M est définie par les lignes $1,2,3,4,7,8,9$. Son déterminant est $-14768u - 639u^2 = 71R$, c.à.d. à cause de la taille de M on obtient simplement un facteur parasite mais pas des solutions artificielles. On calcule les noyaux $\{v\}$ pour $u = 0$ et $u = -208/9$ et on trouve les mêmes racines comme $x = v[2]/v[3],\ y = v[2]/v[5]$.

Notons que c'est un exemple exceptionnel car habituellement l'algorithme incrémental construit des matrices plus compactes que l'algorithme original. De plus, l'algorithme avait examiné une matrice 6×6, qui est la première matrice avec autant de lignes que de colonnes, mais cette matrice n'était pas retenue car elle était singulière pour de valeurs aléatoires des coefficients. □

Exemple 8.8 Strictement dit, les coefficients nuls doivent être connus dès le début. Sous cette condition, examinons une autre spécialisation du système ci-dessus.

$$f_0 = c_{00}x^2 + c_{01}y + c_{02},\ f_1 = c_{10}x + c_{11}y,\ f_2 = u + r_1x + r_2y.$$

Les volumes mixtes des sous-systèmes 2×2 sont $1,2,2$. Le résultant projectif a les mêmes degrés. L'algorithme à partir d'une subdivision mixte donne une matrice exacte :

		$(3,1)$	$(1,2)$	$(2,2)$	$(1,1)$	$(2,1)$
$(3,1)$	$X^{(3,1)-(2,0)}f_0 = xyf_0$	c_{00}	c_{01}	0	c_{02}	0
$(1,2)$	$X^{(1,2)-(0,1)}f_1 = xyf_1$	0	c_{11}	0	0	c_{10}
$(2,2)$	$X^{(2,2)-(0,1)}f_1 = x^2yf_1$	c_{10}	0	c_{11}	0	0
$(1,1)$	$X^{(1,1)-(0,0)}f_2 = xyf_2$	0	r_2	0	u	r_1
$(2,1)$	$X^{(2,1)-(0,0)}f_2 = x^2yf_2$	r_1	0	r_2	0	u

L'algorithme incrémental pour $v = (100, -1)$ donne la même M avec différents B_i : $B_0 = \{y\}, B_1 = \{y, xy\} = B_2$.

On peut résoudre pour la spécialisation $f_0 = x^2 - y - 1,\ f_1 = 2x + 3y,\ f_2 = 82x + 71y + u$.

$$x^3y \quad xy^2 \quad x^2y^2 \quad xy \quad x^2y$$

$$\det M = \begin{vmatrix} c00 & c01 & 0 & c02 & 0 \\ 0 & c11 & 0 & 0 & c10 \\ c10 & 0 & c11 & 0 & 0 \\ 0 & r2 & 0 & u & r1 \\ r1 & 0 & r2 & 0 & u \end{vmatrix} = 9\,u^2 - 208\,u - 10816$$

$$\begin{aligned} M\left(\frac{104}{9}(1+\sqrt{10})\right) v_\alpha = 0 : v_\alpha &= \left[-\frac{1}{3} - \frac{1}{3}\sqrt{10}, \frac{-2}{3}, \frac{2}{9} + \frac{2}{9}\sqrt{10}, \frac{1}{3} - \frac{1}{3}\sqrt{10}, 1,\right] \\ \Rightarrow \alpha &= (-1.387425886, 0.9249505914)\,. \end{aligned}$$

$$\begin{aligned} M\left(\frac{104}{9}(1-\sqrt{10})\right) v_\alpha = 0 : v_\alpha &= \left[-\frac{1}{3} + \frac{1}{3}\sqrt{10}, \frac{-2}{3}, \frac{2}{9} - \frac{2}{9}\sqrt{10}, \frac{1}{3} + \frac{1}{3}\sqrt{10}, 1,\right] \\ \Rightarrow \alpha &= (0.7207592197, -0.4805061470)\,. \end{aligned}$$

Continuons avec la matrice de Bézout.

$$\Delta = \begin{vmatrix} x^2 - y - 1 & a + x & -1 \\ 2x + 3y & 2 & 3 \\ 82x + 71y + u & 82 & 71 \end{vmatrix} = 2u + 104 + 3ux + a(104x + 3u), \quad \Rightarrow$$

$$M = \begin{bmatrix} 2u + 104 & 3u \\ 3u & 104 \end{bmatrix} \Rightarrow \det M = -9u^2 + 208u + 10816.$$

$$M\left(\frac{104}{9}(1+\sqrt{10})\right) v_\alpha = 0 : v_\alpha = \left[\frac{1}{3} - \frac{1}{3}\sqrt{10}, 1\right] \Rightarrow \alpha_x = -1.387425886,$$

$$M\left(\frac{104}{9}(1-\sqrt{10})\right) v_\alpha = 0 : v_\alpha = \left[1 - \frac{1}{3} + \frac{1}{3}\sqrt{10}\right] \Rightarrow \alpha_x = 0.7207592197.$$

□

Exercice 8.9 Construire la matrice de Newton pour le système suivant, qui est déjà sur-contraint. Faites la comparaison entre les deux algorithmes (paresseux et incrémental). Puis, construire la matrice de Bézout et la comparer.

```
#Distance (T) de l'intersection (x,y) de 2 coniques (q1,q2) de l'origine.
#Eliminer x,y
q0:=a0*x^2+b0*x*y+c0*y^2+d0*x+e0*y+f0;
q1:=a1*x^2+b1*x*y+c1*y^2+d1*x+e1*y+f1;
q2:=x^2+y^2-T;
```

□

Exercice 8.10 $f_0 = c_{00} + c_{01}x + c_{02}y, f_1 = c_{10} + c_{11}y + c_{12}x + c_{13}xy, f_2 = c_{20} + c_{21}y$.
(a) Construire la matrice de Newton par l'algorithme original. Pour $\delta = (\epsilon, \epsilon)$ vous devez trouver une matrice 6×6. Quelles sont les tailles de M différentes pour des vecteurs δ différents ? Quelle est la taille optimale ? (b) Mêmes questions avec l'algorithme paresseux. Calculer le résultant creux à partir d'une de ces matrices. Proposer une règle pratique pour trouver le δ optimal de manière expérimentale. (c) Utiliser l'algorithme incrémental, puis (d) construire Δ et M de Bézout et faire la comparaison entre toutes les matrices. □

8.3 Racines cycliques

Un problème standard en calcul formel, utilisé dans la comparaison des logiciels ("benchmark"), est le système de n-racines cycliques (ou racines de l'unité). Notre logiciel du volume mixte a confirmé les bornes existantes pour $n \leq 7$ [BF91], tandis que pour $n = 9, 10, 11$, où la méthode des bases de Gröbner utilisée auparavant est impraticable, on a obtenu les premières bornes supérieures [EC95]. Notamment, pour $n = 11$, le volume mixte vérifie une conjecture ainsi que la borne obtenue via les variétés toriques [Pot95].

Ci-dessous, des expériences avec le logiciel Relever-Élaguer sur un DEC Alpha 3000 (67 SpecInt92, 77 SpecFP92).

n	Nb. zéros isolés	VM	temps de calcul
3	6	6	0s
4	0	16	0s
5	70	70	0s
6	156	156	2s
7	924	924	27s
8	1152	2560	4m 19s = 259s
9	inconnu	11016	40m 59s = 2459s
10	inconnu	35940	4h 50m 14s = 17414s
11	inconnu	184756	38h 26m 44s = 138404s

Exercice 8.11 On étudie le système de n-racines cycliques.

$$\begin{aligned} x_1 + x_2 + \cdots + x_n &= 0 \\ x_1x_2 + x_2x_3 + \cdots + x_nx_1 &= 0 \\ &\vdots \\ x_1 \cdots x_{n-1} + \cdots + x_nx_1 \cdots x_{n-2} &= 0 \\ x_1x_2 \cdots x_n &= 1. \end{aligned} \tag{7}$$

Calculez le volume mixte pour $n = 3, 4, 5, 6, 7$. Puis, introduisez les variables $y_i = x_i/x_n$ pour $i = 1, \ldots, n-1$. Comment peut-on réduire le nouveau système à un système de dimension $n-1$? Calculer les volumes mixtes du nouveau système pour $3 \leq n \leq 7$ et comparer avec les volumes mixtes originaux. Vous pouvez modifier la routine `cycsys2` dans le fichier `maplib` pour construire le nouveau système en Maple. □

Exercice 8.12 Pour obtenir un système surcontraint on peut ajouter une forme linéaire

$$f_0 = c_{01}x_1 + \cdots + c_{0n}x_n + c_{00}$$

au système 7. Pour $n = 3$, calculez une matrice du résultant creux par l'algorithme paresseux. Atteint-elle la taille optimale ?

Homogénéisez le système en posant $x_i = z_i/z_0$ et calculer le résultant de Macaulay. Quelle est la taille optimale pour la matrice du système homogène ? Comparez les tailles de la matrice paresseuse avec celle de Macaulay.

Répétez pour $n = 4, 5$. □

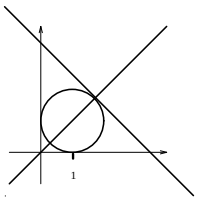
Exercice 8.13 Considérez le système de n-racines cycliques comme un système surcontraint de n polynômes en $n-1$ variables, en cachant une variable dans les coefficients. Appliquez l'algorithme paresseux aux deux formulations de racines cycliques (en x, puis en y) pour $n = 3, 4, 5$. Comparez les temps d'exécution et les tailles des matrices. □

Exercice 8.14 Considérez le système de n-racines cycliques comme un système surcontraint de n polynômes en $n-1$ variables, en cachant une variable dans les coefficients. Appliquez l'approche incrémentale et calculer les matrices de Bézout pour $n = 3, 4, 5$. Comparez les temps de calcul et les tailles des matrices. □

9 Directions de recherche

Racines multiples calculées par le résultant [MS95]. Racines non-isolées par le résultant [Cha93, EM02]. Systèmes surcontraints résolus par une matrice de Newton incrémentale.

Exemple 9.1 Voici un système surcontraint résolu par une matrice de Newton *incrémentale.*



$$\begin{array}{ll} (\text{cercle}) f_0 = & x^2 - 2x + (y-1)^2 \\ (\text{droite}) f_1 = & x - y \\ (\text{droite}) f_2 = & x + y - 2 - \sqrt{2}, \end{array} \quad \rightarrow \quad M(y) = \begin{bmatrix} 1 & -2 & (y-1)^2 \\ 0 & 1 & -y \\ 0 & 1 & y - 2 - \sqrt{2} \end{bmatrix}. \quad \begin{array}{l} f_0 \\ f_1 \\ f_2 \end{array}$$

$\det M(\beta) = 0 \Rightarrow \beta = 1 + \sqrt{2}/2$. $v_\alpha = [3 + 2\sqrt{2}, 2 + \sqrt{2}, 2]/2 \Rightarrow \alpha = (2 + \sqrt{2})/2$. □

Remerciement

Je remercie Alicia Dickenstein pour sa lecture attentive du brouillon.

Références

[Ber75] D.N. Bernstein. The number of roots of a system of equations. *Funct. Anal. and Appl.*, 9(2) :183–185, 1975. Translated from *Funktsional'nyi Analiz i Ego Prilozheniya,* 9(3) :1–4, 1975.

[BF91] G. Björck and R. Fröberg. A faster way to count the solutions of inhomogeneous systems of algebraic equations, with applications to cyclic n-roots. *J. Symbolic Computation*, 12 :329–336, 1991.

[BMS94] C. Burnikel, K. Mehlhorn, and S. Schirra. How to compute the Voronoi diagram of line segments : Theoretical and experimental results. In *Proc. Europ. Symp. Algorithms*, volume 855 of *Lecture Notes in Computer Science*, pages 227–237. Springer, 1994.

[BP94] D. Bini and V.Y. Pan. *Polynomial and Matrix Computations*, volume 1 : Fundamental Algorithms. Birkhäuser, Boston, 1994.

[CDS98] E. Cattani, A. Dickenstein, and B. Sturmfels. Residues and resultants. *J. Math. Sci. Univ. Tokyo*, 5 :119–148, 1998.

[CE00] J.F. Canny and I.Z. Emiris. A subdivision-based algorithm for the sparse resultant. *J. ACM*, 47(3) :417–451, May 2000.

[Cha93] M. Chardin. The resultant via a Koszul complex. In F. Eyssette and A. Galligo, editors, *Computational Algebraic Geometry*, volume 109 of *Progress in Mathematics*, pages 29–39. Birkhäuser, Boston, 1993. (Proc. MEGA '92, Nice).

[CLO05] D. Cox, J. Little, and D. O'Shea. *Using Algebraic Geometry.* Number 185 in GTM. Springer, New York, 2nd edition, 2005.

[CM96] J.-P. Cardinal and B. Mourrain. Algebraic approach of residues and applications. In J. Renegar, M. Shub, and S. Smale, editors, *The Mathematics of Numerical Analysis*, volume 32 of *Lectures in Applied Math.*, pages 189–210. AMS, 1996.

[CP93] J. Canny and P. Pedersen. An algorithm for the Newton resultant. Technical Report 1394, Comp. Science Dept., Cornell University, 1993.

[Dix08] A.L. Dixon. The eliminant of three quantics in two independent variables. *Proc. London Math. Society*, 6 :49–69, 209–236, 1908.

[EC95] I.Z. Emiris and J.F. Canny. Efficient incremental algorithms for the sparse resultant and the mixed volume. *J. Symbolic Computation*, 20(2) :117–149, 1995.

[EM99] I.Z. Emiris and B. Mourrain. Computer algebra methods for studying and computing molecular conformations. *Algorithmica, Special Issue on Algorithms for Computational Biology*, 25 :372–402, 1999.

[EM02] M. Elkadi and B. Mourrain. *Géométrie Algébrique Effective en dimension 0 : de la théorie à la pratique*. Notes de cours, DEA de Mathématiques, Univ. de Nice, 2002.

[Emi96] I.Z. Emiris. On the complexity of sparse elimination. *J. Complexity*, 12 :134–166, 1996.

[EP97] I.Z. Emiris and V.Y. Pan. The structure of sparse resultant matrices. In *Proc. Annual ACM Intern. Symp. on Symbolic and Algebraic Computation*, pages 189–196, Maui, Hawaii, July 1997.

[ER94] I.Z. Emiris and A. Rege. Monomial bases and polynomial system solving. In *Proc. Annual ACM Intern. Symp. on Symbolic and Algebraic Computation*, pages 114–122, Oxford, July 1994.

[EV99] I.Z. Emiris and J. Verschelde. How to count efficiently all affine roots of a polynomial system. *Discrete Applied Math., Special Issue on Comput. Geom.*, 93(1) :21–32, 1999.

[EV09] I.Z. Emiris and A. Varvitsiotis. Counting the number of embeddings of minimally rigid graphs. In *Proc. Europ. Workshop Computat. Geometry*, Brussels, 2009.

[Ewa96] G. Ewald. *Combinatorial Convexity and Algebraic Geometry*. Springer, New York, 1996.

[Ful93] W. Fulton. *Introduction to Toric Varieties*. Number 131 in Annals of Mathematics. Princeton University Press, Princeton, 1993.

[GKZ94] I.M. Gelfand, M.M. Kapranov, and A.V. Zelevinsky. *Discriminants, Resultants and Multidimensional Determinants*. Birkhäuser, Boston, 1994.

[GV96] G.H. Golub and C.F. Van Loan. *Matrix Computations*. The Johns Hopkins University Press, Baltimore, Maryland, 3rd edition, 1996.

[HS95] B. Huber and B. Sturmfels. A polyhedral method for solving sparse polynomial systems. *Math. Comp.*, 64(212) :1542–1555, 1995.

[HS97] B. Huber and B. Sturmfels. Bernstein's theorem in affine space. *Discr. and Computational Geometry*, 17(2) :137–142, March 1997.

[Jou97] J-P. Jouanolou. Formes d'inertie et résultant : Un formulaire. *Adv. in Math.*, 126 :119–250, 1997. Also : Tech. Report 499/P-288, IRMA, Strasbourg, 1992.

[Kho78] A.G. Khovanskii. Newton polyhedra and the genus of complete intersections. *Funktsional'nyi Analiz i Ego Prilozheniya*, 12(1) :51–61, Jan.–Mar. 1978.

[Kus75] A.G. Kushnirenko. The Newton polyhedron and the number of solutions of a system of k equations in k unknowns. *Uspekhi Mat. Nauk.*, 30 :266–267, 1975.

[Mac02] F.S. Macaulay. Some formulae in elimination. *Proc. London Math. Soc.*, 1(33) :3–27, 1902.

[MC27] F. Morley and A.B. Coble. New results in elimination. *American J. Math.*, 49 :463–488, 1927.

[MC00] T. Michiels and R. Cools. Decomposing the secondary cayley polytope. *Discr. Comput. Geometry*, 23 :367–380, 2000.

[Mou97] B. Mourrain. Isolated points, duality and residues. *J. Pure Applied Algebra. Special Issue on Algorithms for Algebra*, 117 & 118 :469–494, May 1997.

[MP00] B. Mourrain and V.Y. Pan. Multivariate polynomials, duality and structured matrices. *J. Complexity*, 16(1) :110–180, 2000.

[MS95] H.M. Möller and H.J. Stetter. Multivariate polynomial equations with multiple zeros solved by matrix eigenproblems. *Numer. Math.*, 70 :311–329, 1995.

[MV99] T. Michiels and J. Verschelde. Enumerating regular mixed-cell configurations. *Discr. Comput. Geometry*, 21(4) :569–579, 1999.

[Pot95] L. Pottier. Bounds for degree of the n-cyclic system. Manuscript. INRIA Sophia-Antipolis, France, 1995.

[PS93] P. Pedersen and B. Sturmfels. Product formulas for resultants and Chow forms. *Math. Zeitschrift*, 214 :377–396, 1993.

[Rou98] F. Rouillier. Solving zero-dimensional polynomial systems through the rational univariate representation. Technical Report 3426, INRIA–Lorraine, 1998.

[Sha77] I.R. Shafarevich. *Basic Algebraic Geometry*. Springer-Verlag, Berlin, 1977.

[Sta80] R.P. Stanley. Decompositions of rational convex polyhedra. In J. Srivastava, editor, *Combinatorial Mathematics, Optimal Designs and Their Applications, Annals of Discrete Math. 6*, pages 333–342. North-Holland, Amsterdam, 1980.

[Stu94] B. Sturmfels. On the Newton polytope of the resultant. *J. of Algebr. Combinatorics*, 3 :207–236, 1994.

[Syl53] J.J. Sylvester. On a theory of syzygetic relations of two rational integral functions, comprising an application to the theory of Sturm's functions, and that of the greatest algebraic common measure. *Philosophical Trans.*, 143 :407–548, 1853.

[SZ94] B. Sturmfels and A. Zelevinsky. Multigraded resultants of Sylvester type. *J. of Algebra*, 163(1) :115–127, 1994.

[vdW50] B.L. van der Waerden. *Modern Algebra*. F. Ungar Publishing Co., New York, 3rd edition, 1950.

A Solutions aux exercices

Solution 2.3 [CLO05] □

Solution 2.5 Par récurrence sur n en utilisant le lemme 2.2 [CLO05]. □

Solution 2.7 Deuxième partie : Si $|I| = n+1$ il existe $k \in \{0,\dots,n\}$ tel que $\dim(\sum_{i\neq k} Q_i) = n$. Alors on revient au cas $|I| = n$. □

Solution 2.12 Dans le polynôme $V(\lambda_1 Q_1 + \cdots + \lambda_k Q_k + \lambda'_k Q'_k + \cdots + \lambda_n Q_n)$, il y a exactement deux termes multi-linéaires de degré n en les $\lambda_i, i \neq k$: $\lambda_1 \cdots \lambda_k \cdots \lambda_n VM(Q_1,\dots,Q_k,\dots,Q_n)$ et $\lambda_1 \cdots \lambda'_k \cdots \lambda_n VM(Q_1,\dots,Q'_k,\dots,Q_n)$. En posant $\lambda_k = \lambda'_k$, le polynôme aura un seul tel terme : $\lambda_1 \cdots \lambda_k \cdots \lambda_n\ VM(Q_1,\dots,Q_k+Q'_k,\dots,Q_n)$, ce qui montre la linéarité de VM p.r.à l'addition.

En posant $\lambda'_k = 0$ et $\lambda_k \leftarrow \lambda\mu$, le terme multi-linéaire est $\lambda_1 \cdots \lambda\mu \cdots \lambda_n VM(Q_1,\dots,Q_k,\dots,Q_n)$. Si $\lambda_k \leftarrow \lambda, Q_k \leftarrow \mu Q_k$, le même terme devient $\lambda_1 \cdots \lambda \cdots \lambda_n VM(Q_1,\dots,\mu Q_k,\dots,Q_n)$, ce qui montre la linéarité p.r.à la multiplication scalaire. □

Solution 2.22 [CE00] □

Solution 2.28 Par analogie au volume normalisé, défini au lemme 2.2, et la formule pour $\mathrm{Vol}_n(\cdot)$ [CLO05]. □

Solution 2.32 Dans le livre de Burago-Zallgaler, la preuve est attribuée à Fedotov (1978). Une preuve générale est donnée par Steffens-Theobald (Euro-CG, 2008). Dans le cas de polytopes aux sommets entiers, il suffit d'appliquer BKK. □

Solution 2.42 Soit $W = V^{-1}$. Considérons le système $\prod_j G_j^{W_{jl}} = 1$, $l = 1,\dots,n$. Nous démontrons que chaque équation est égale à I_l :

$$\prod_{j=1}^{n}\prod_{k=1}^{n} c_k^{V_{kj}W_{jl}} \prod_{j=1}^{n}\prod_{i} x_i^{H_{ij}W_{jl}} = \prod_{k=1}^{n} c_k^{(VW)_{kl}} \prod_{i=1}^{n} x_i^{\sum_j H_{ij}W_{jl}} = c_l \prod_{i=1}^{n} x_i^{A_{il}}.$$

□

Solution 3.2 Les $f_1, \ldots, f_n$ génériques ont un nombre fini de solutions. Pour n'importe quelle valeur des coefficients $c_{01}, \ldots, c_{0n}$, nous pouvons choisir c_{00} pour que les $f_0, \ldots, f_n$ n'aient aucune solution, alors Z_0 ne peut pas être de dimension maximale. □

Solution 3.5 Posons $f_1, \ldots, f_n$ le système avec $VM > 0$. Pour des coefficients génériques, ils ont une solution $\alpha \in (\overline{K}^*)^n$. Si $f_0(\alpha) \neq 0$ et pour que $f_0(\alpha) = 0$, avec des coefficients c_{0j} arbitraires, il suffit de choisir/fixer un seul coefficient, soit c_{00}. Donc $\operatorname{codim}(Z_0) \leq 1$, alors $\operatorname{codim}(Z_0) = 1$. □

Solution 3.10 Considérer $R(a_0 f_0, \ldots, a_i f_i, \ldots, a_n f_n)$ pour a_i des scalaires. □

Solution 5.7 Pour les systèmes linéaires, $\delta = (1/n, \ldots, 1/n)$ et une subdivision qui place n copies de Q_i aux sommets de $Q = (n+1)S$ autres que l'origine (c.à.d. aux $(n+1)e_i$) et une copie de Q_i le plus loin dans la direction $(1, \ldots, 1)$, dont les sommets sont les points dans $\mathcal{E}$. Il y a $n+1$ points dans $\mathcal{E} = \{|p| \leq n+1, p_i \geq 1\}$. □

Solution 6.6 Partielle : $n = 8 \Rightarrow \beta \geq 3.3$? Pour $n \to \infty$ on prend des limites et on applique la règle de L'Hopital. □

Solution 6.8 S'il y a une solution commune α, elle annule tous les θ_i ; de plus, elle définit un vecteur non-nul aux monômes de colonnes qui se trouve dans le noyau de la matrice Φ, donc $\det \Phi = 0$. Alors $Z_0 \subset V(\det \Phi) \Rightarrow R | \det \Phi$. □

Solution 7.3 Écrire $F = \sum_{i=0}^{n} f_i y^i, G = \sum_{i=0}^{n} g_i y^{-i}$. La somme en question est le terme constant de FG. □