



TER :

POINTS ENTIERS DANS LES POLYTOPES CONVEXES

FAVIER ANDRÉA
PLANQUE RAPHAËL
M1 Maths Fondamentales

*Encadrant : DELCROIX THIBAUT
Mai 2022*

Remerciements

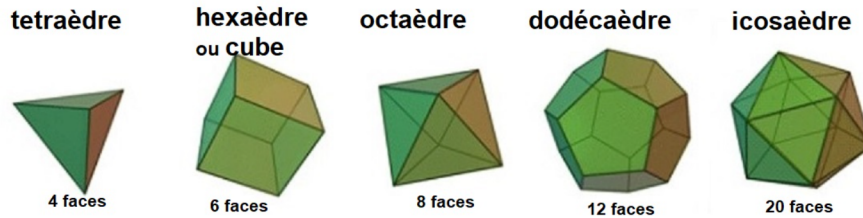
Nous tenons à remercier notre encadrant M. DELCROIX pour nous avoir fait découvrir ce sujet. Il a été présent du début à la fin, de la présentation des éléments clés auxquels il fallait s'intéresser, jusqu'à la finalisation de notre mémoire. De plus, il nous a apporté de précieux conseils, nous sommes reconnaissants de l'attention qu'il a porté à notre travail tout au long du semestre.

Sommaire

1	Introduction	1
2	Premières définitions et finitude du nombre de points entiers	2
3	Estimation du nombre de points entiers à partir du volume	6
4	Lien entre volume, points entiers et points entiers du bord	9
4.1	Dimension 2 et Théorème de Pick	9
4.2	Généralisation à toute dimension : Théorème d'Ehrhart	12
5	Estimation du nombre de points entiers à partir du nombre de points entiers intérieurs	16
5.1	Dimension 2 et Théorème de Scott	16
5.2	Généralisation à toute dimension : Théorème de Hensley	20
5.2.1	Enoncé du théorème	20
5.2.2	Coefficient de symétrie	20
5.2.3	Cas des simplexes	21
5.2.4	Généralisation à tout polytope	24
6	Polytope de Fano	25

1 Introduction

La connaissance des polytopes réguliers de dimension 2 et 3 remonte à des siècles. C'est aux mathématiciens grecs de l'Antiquité, notamment Euclide, qu'on en doit le plus ancien traitement mathématique connu. Ses travaux ont notamment permis d'identifier les cinq solides platoniciens que voici :



De nombreux siècles après lui, la définition des polytopes réguliers restait inchangée. Pourtant, cette définition sera ensuite progressivement élargie, de façon à englober de plus en plus d'objets nouveaux. Certains considèrent les polytopes comme les objets géométriques les plus importants et pensent que la plupart de la géométrie euclidienne est essentiellement réduite à la théorie des polytopes convexes. À l'heure actuelle, l'étude des polytopes a de nombreuses applications, notamment en infographie ou en programmation linéaire.

Le but de notre TER est l'étude de certains résultats sur les points entiers d'un polytope convexe. Nous commencerons d'abord par montrer qu'un polytope n'a qu'un nombre fini de points entiers. Puis nous verrons des méthodes pour estimer le nombre de points entiers, d'une part à l'aide du volume et d'autre part à partir du nombre de points entiers intérieurs. Enfin, nous étudierons le cas particulier des polytopes de Fano et certaines de leurs propriétés.

Ce mémoire est basé sur l'article de Debarre [De] qui présentait bien les différentes notions que nous allons aborder.

2 Premières définitions et finitude du nombre de points entiers

Nous allons introduire les principaux objets mathématiques que nous allons étudier tout au long de notre mémoire. Dans un premier temps, définissons rigoureusement ce qu'est un polytope, ainsi que ses principales subdivisions :

Définition 1 : L'enveloppe convexe d'un sous-ensemble Σ de \mathbb{R}^n , $n \in \mathbb{N}^*$ est l'intersection des sous-ensembles convexes de \mathbb{R}^n qui contiennent Σ : c'est le plus petit sous-ensemble convexe de \mathbb{R}^n qui contient Σ . C'est aussi l'ensemble des barycentres à coefficients positifs de points de Σ .

Définition 2 : Un **polytope** est l'enveloppe convexe d'un sous-ensemble fini de l'espace euclidien \mathbb{R}^n . Sa dimension est par définition celle de l'espace affine qu'il engendre.

Remarque : C'est donc un compact : en effet, il est borné car contenu dans une boule de centre un des points de Σ et de rayon $diam(\Sigma)$. De plus, il est fermé par la définition d'une enveloppe convexe et comme \mathbb{R}^n est un espace vectoriel de dimension finie, les compacts de \mathbb{R}^n sont les fermés bornés.

Définition 3 : On appelle **intérieur relatif** d'un polytope P son intérieur dans l'espace affine qu'il engendre. On le note P' .

Un point de P est un **sommet** s'il n'est intérieur à aucun segment entièrement contenu dans P .

Définition 4 : On appelle **face** d'un polytope P tout sous-ensemble de P défini comme $P \cap H$, où H est un hyperplan affine tel que P soit entièrement contenu dans un des deux demi-espaces fermés que H définit.

Remarque : Si on regarde un polytope P de dimension n dans \mathbb{R}^{n+1} , il est facile de trouver un hyperplan qui n'intersecte pas P . De même, P sera totalement contenu dans un hyperplan de dimension n . On peut donc considérer que \circlearrowleft et P lui-même sont des faces de P . Ces deux faces sont dites **impropres**, les autres sont dites **propres**.

Définition 5 : Une **facette** de P est une face de P de dimension $dim(P) - 1$. Enfin, un polytope est réunion disjointe des intérieurs relatifs de ses faces.

Exemples :

- Les faces de dimension 0 sont des sommets
- Les faces de dimension 1 sont des arêtes

Nous allons maintenant énoncer deux résultats qui seront très utiles pour caractériser les polytopes dans les démonstrations à venir :

Théorème de Carathéodory : Soit Σ un sous-ensemble de \mathbb{R}^n , $n \in \mathbb{N}^*$. Tout point de l'enveloppe convexe $Conv(\Sigma)$ est barycentre, avec des coefficients strictement positifs, d'un sous ensemble de Σ formé de points affinement indépendants.

Démonstration : Admise. C'est un résultat classique sur la convexité qui nous sert uniquement dans certaines démonstrations. Pour plus d'informations voir [Fr].

Proposition 1 : Les sommets d'un polytope P sont en nombre fini et leur enveloppe convexe est P .

Démonstration : Soit Σ un ensemble fini de cardinal minimal dont P est l'enveloppe convexe. Nous allons montrer que Σ est exactement l'ensemble des sommets de P .

Soit s un sommet de P . Le théorème de Carathéodory donne qu'il existe $m \in \mathbb{N}^*$, s_1, \dots, s_m des points affinement indépendants de Σ et $\lambda_1, \dots, \lambda_m \in \mathbb{R}_+^*$ vérifiant $\sum_{i=1}^m \lambda_i = 1$ tels que $s = \sum_{i=1}^m \lambda_i s_i$.

Procédons par l'absurde en supposant $m > 1$, si on pose $\gamma_1 = (1 - \lambda_3 - \dots - \lambda_m)s_1 + \lambda_3 s_3 + \dots + \lambda_m s_m$ et $\gamma_2 = (1 - \lambda_3 - \dots - \lambda_m)s_2 + \lambda_3 s_3 + \dots + \lambda_m s_m$ alors le point s est dans l'intérieur du segment joignant γ_1 et γ_2 . En effet, ces deux points sont dans $Conv(\Sigma)$ car se sont des barycentres à coefficients positifs de points de Σ , donc le segment $[\gamma_1 \gamma_2]$ est entièrement contenu dans P . On observe alors que si on pose $t = \frac{\lambda_1}{1 - \sum_{i=3}^m \lambda_i}$ alors $s = t\gamma_1 + (1 - t)\gamma_2$, ce qui définit bien un point du segment $[\gamma_1 \gamma_2]$. Mais alors s n'est plus un sommet de P .

CONTRADICTION $\implies m = 1$, c'est-à-dire $s \in \Sigma$.

Soit maintenant $s \in \Sigma$. Considérons $Conv(\Sigma \setminus \{s\}) \subset P$, que l'on note Q . La minimalité de Σ donne que $Q \neq P$. Notons x le point de Q le plus proche de s , $x \neq s$ et H l'hyperplan affine passant par x et orthogonal au segment $[xs]$. Son équation est $\phi(y) = \langle y - x, s - x \rangle = 0$, et ϕ est une fonction affine négative sur Q . De plus $\forall s' \in P \setminus Q : \phi(s) - \phi(s') = \langle s - x, s - x \rangle - \langle s' - x, s - x \rangle = \langle s - s', s - x \rangle \geq 0$ car $s' \in P \setminus Q$ d'où $\phi(s) - \phi(s') = 0 \iff s = s'$. Ainsi, s est le seul point de P où ϕ atteint son maximum, et donc s est un sommet de P .

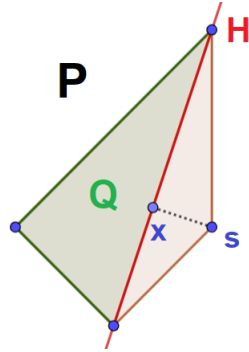


Figure 1: Exemple de la construction de H , Q et x en dimension 2

■

Remarque : Cette proposition nous permet de déduire que P n'a qu'un nombre fini de faces.

Enfin, on va expliciter la notion de simplexe et donner une relation entre un polytope quelconque et les simplexes, puis finir cette section par une formule donnant le volume d'un polytope à partir de ses sommets :

Définition 6 : On appelle **r -simplexe** l'enveloppe convexe de $r + 1$ points affinement indépendants dans \mathbb{R}^n , $n \in \mathbb{N}^*$. Les r -simplexes sont donc exactement les polytopes de dimension r avec $r + 1$ sommets.

Définition 7 : On appelle **r -simplexe ouvert** l'intérieur relatif d'un r -simplexe. En particulier, un point est un 0-simplexe et un 0-simplexe ouvert.

Proposition 2 : Tout polytope P est réunion disjointe de simplexes ouverts dont les sommets sont des sommets de P .

Démonstration : On va raisonner par récurrence sur la dimension de P . Soit s un sommet de P , soient F_1, \dots, F_r les faces propres de P ne contenant pas s et soient F'_1, \dots, F'_r leurs intérieurs relatifs. Les ensembles $\{s\}$, $(\text{Conv}(\{s\} \cup F_1))'$, \dots , $(\text{Conv}(\{s\} \cup F_r))'$, F'_1, \dots, F'_r forment une partition de P . Comme $\forall i \in \{1, \dots, r\}$ $\dim(F_i) \leq \dim(P)$, on a donc par hypothèse de récurrence que chaque F_i se décompose en réunion disjointe de simplexes ouverts dont les sommets sont des sommets de F_i , et donc de P .

De plus, si on exclut les simplexes contenus dans $F_i - F'_i$, on obtient une décomposition de chaque F'_i en réunion disjointe de simplexes ouverts, qui induit une telle décomposition de $(\text{Conv}(\{s\} \cup F_i))' \forall i \in \{1, \dots, r\}$, et donc de P , ce qui termine la preuve.

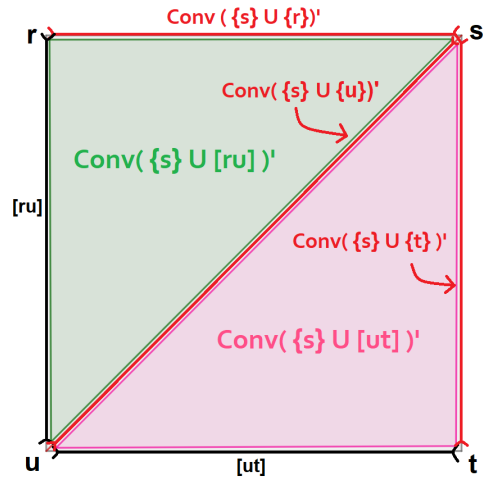


Figure 2: Illustration de la situation pour un carré

■

Exemple : Dans le plan, un carré est l'union de deux triangles (des 2-simplexes) et leur intersection est la diagonale du carré (un 1-simplexe).

On rappelle que le volume euclidien de l'enveloppe convexe de points s_0, \dots, s_n de \mathbb{R}^n est :

$$\frac{1}{n!} |\det(\overrightarrow{s_0 s_1}, \dots, \overrightarrow{s_0 s_n})| \quad (1)$$

3 Estimation du nombre de points entiers à partir du volume

Définition 8 : On appelle **point entier** dans \mathbb{R}^n un point dont toutes les coordonnées sont entières, c'est-à-dire un point de \mathbb{Z}^n . On appelle **polytope entier** un polytope dont tous les sommets sont des points entiers.

Définition 9 : On rappelle qu'une famille (x_1, \dots, x_n) de n vecteurs de \mathbb{Z}^n est un **base** si $\forall y \in \mathbb{Z}^n \exists (\mu_1, \dots, \mu_n) \in \mathbb{Z}^n$ tels que $y = \sum_{i=1}^n \mu_i x_i$.

Proposition 3 : Soient (x_1, \dots, x_n) des vecteurs de \mathbb{Z}^n qui forment une base de \mathbb{R}^n . On a alors équivalence entre :

- (i) la famille (x_1, \dots, x_n) est une base de \mathbb{Z}^n
- (ii) $\det(x_1, \dots, x_n) = \pm 1$ dans la base canonique de \mathbb{R}^n

On a aussi $\text{vol}(\text{Conv}(0, x_1, \dots, x_n)) = 1$

- (iii) le parallélépipède de sommets 0 et de côtés x_1, \dots, x_n ne contient aucun point entier autre que les 2^n points $\epsilon_1 x_1 + \dots + \epsilon_n x_n$ avec $\epsilon_i \in \{0, 1\}$

Démonstration : Soit A la matrice carrée entière dont les colonnes sont les coordonnées des vecteurs (x_1, \dots, x_n) dans la base canonique et soit B son inverse, c'est-à-dire la matrice dont les colonnes sont les coordonnées des vecteurs de la base canonique dans la base (x_1, \dots, x_n) de l'espace vectoriel \mathbb{R}^n .

(i) \implies (ii) : Supposons (i). Alors la matrice B est à coefficients entiers et $AB = I_n \Leftrightarrow \det(AB) = \det(I_n) \Leftrightarrow \det(A)\det(B) = 1 \Leftrightarrow \det(A) = \pm 1$ (car les seuls éléments inversibles dans l'anneau \mathbb{Z} sont ± 1).

(ii) \implies (i) : Supposons $\det(A) = \pm 1$, alors $B = A^{-1} = \frac{1}{\det(A)} \text{com}(A)^T$, où $\text{com}(A)^T$ désigne la transposée de la comatrice de A . On a donc $B \in \mathcal{M}_n(\mathbb{Z})$ puisque $A \in \mathcal{M}_n(\mathbb{Z})$ et $\det(A) = \pm 1$. On en déduit (i).

(iii) \implies (i) : Supposons (iii). Comme (x_1, \dots, x_n) est une base de \mathbb{R}^n , tout vecteur de \mathbb{Z}^n peut s'écrire $\sum_{i=1}^n \lambda_i x_i$, avec $\lambda_i \in \mathbb{R}$. On note $[\lambda_i]$ la partie entière inférieure de λ_i . On remarque que le point $\sum_{i=1}^n [\lambda_i] x_i$ est aussi un point de \mathbb{Z}^n , d'où le fait que le point $\gamma = \sum_{i=1}^n (\lambda_i - [\lambda_i]) x_i$ soit aussi un point de \mathbb{Z}^n (comme différence de points entiers). De plus, $\forall i \in \{1, \dots, n\} : 0 \leq \lambda_i - [\lambda_i] < 1$, d'où le fait que γ est dans le parallélépipède de sommet 0 construit sur les vecteurs (x_1, \dots, x_n) , et donc par (iii), $\lambda_i - [\lambda_i] = 0 \forall i \in \{1, \dots, n\}$. Donc (i) est vérifié.

(i) \implies (iii) : Supposons (i), alors tout point entier dans le parallélépipède de sommet 0 et de côtés (x_1, \dots, x_n) est combinaison linéaire de ceux-ci à coefficients entiers, qui valent donc nécessairement 0 ou 1. On a donc (iii).

On a donc bien (i) \iff (ii) et (i) \iff (iii), ce qui conclut la preuve. ■

Remarque : Lorsque l'on étudie les polytopes entiers, il faut tenir compte des transformations de l'espace euclidien \mathbb{R}^n préservant le réseau \mathbb{Z}^n (et donc les notions de point entier et de polytope entier) : ces transformations sont les translations par un vecteur entier et les transformations linéaires $x \mapsto Ax$, où A est une matrice de $\mathcal{GL}_n(\mathbb{Z})$, c'est-à-dire, par la proposition précédente, une matrice $n \times n$ à coefficients entiers et de déterminant ± 1 . Une telle transformation préserve donc aussi le volume euclidien. Deux polytopes qui diffèrent par une telle transformation seront dits **équivalents**.

Exemple : Même si les deux polytopes ci-dessous semblent très différents ils sont équivalents. En effet, ils sont tous les deux d'aire 4.5 et contiennent chacun 10 points entiers dont 1 seul intérieur.

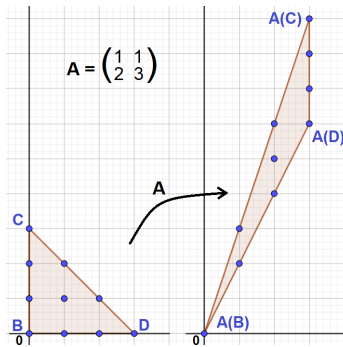


Figure 3: Deux polytopes équivalents en dimension 2

Les résultats énoncés jusqu'à présent vont maintenant nous servir à démontrer la majoration suivante, qui est un point clé de cette partie du mémoire.

Théorème de Blichfeldt ([De], Thm 1) : Soit K un compact convexe de l'espace euclidien \mathbb{R}^n tel que $K \cap \mathbb{Z}^n$ ne soit pas contenu dans un hyperplan. Alors on a :

$$\text{card}(K \cap \mathbb{Z}^n) \leq n + n! \text{vol}(K)$$

Démonstration : On commence par remarquer que K et l'enveloppe convexe de ses points entiers (que l'on note P) ont le même nombre de points entiers, on va donc montrer le résultat pour P .

P est donc un polytope entier de dimension n (car K n'est pas contenu dans un hyperplan), d'où $\text{card}(P \cap \mathbb{Z}^n) \geq n + 1$. On va procéder par récurrence sur $\text{card}(P \cap \mathbb{Z}^n)$.

Supposons que $\text{card}(P \cap \mathbb{Z}^n) = n + 1$. P est alors un simplexe entier, donc son volume est au moins égal à $\frac{1}{n!}$ par la formule (1) et l'inégalité voulue est vérifiée.

Maintenant, supposons que P ne soit pas un simplexe, c'est-à-dire que P a au moins $n + 2$ sommets. Alors, il existe un sommet s de P tel que l'enveloppe convexe des sommets de P autre que s soit de dimension n (toujours car P n'est pas contenu dans un hyperplan). On note Q cette enveloppe convexe, qui est donc un polytope entier. Q est donc l'intersection de demi-espaces définis par ses facettes, et comme $s \notin Q$, il existe H un hyperplan, et une facette $F = Q \cap H$ telle que s et Q soient de part et d'autre de H . On pose également $R = \text{Conv}(\{s\} \cup F)$.

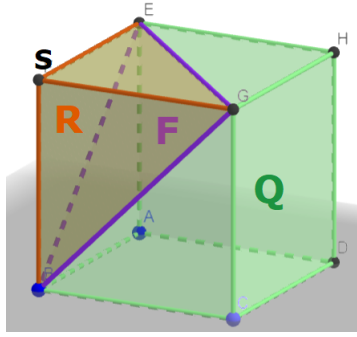


Figure 4: Illustration des polytopes F, Q et R en dimension 3

On a que Q et R sont tout deux de dimension n , ont tous les deux strictement moins de points entiers que P et au moins n sommets entiers communs (ceux de F). De plus, R est un $n + 1$ simplexe et si Q n'est pas un simplexe, on peut réitérer ce procédé jusqu'à n'avoir que des simplexes. On peut donc supposer que Q est aussi un $n + 1$ simplexe.

Enfin, comme $P = Q \cup R$, $F = Q \cap R$ et que l'inégalité est vraie pour les simplexes, on en déduit que :

$$\begin{aligned} \text{card}(P \cap \mathbb{Z}^n) &= \text{card}(Q \cap \mathbb{Z}^n) + \text{card}(R \cap \mathbb{Z}^n) - \text{card}(F \cap \mathbb{Z}^n) \\ &\leq n + n! \text{vol}(Q) + n + n! \text{vol}(R) - n \\ &\leq n + n! \text{vol}(P) \end{aligned}$$

Finalement, comme P et K ont le même nombre de points entiers, et que $\text{vol}(P) \leq \text{vol}(K)$, on obtient bien $\text{card}(K \cap \mathbb{Z}^n) \leq n + n! \text{vol}(K)$. ■

4 Lien entre volume, points entiers et points entiers du bord

4.1 Dimension 2 et Théorème de Pick

Nous commencerons par nous restreindre au cas des polytopes de dimension 2, plus simple à traiter. Il s'agit en fait des polygones. On définit $\partial P = P - P'$ comme étant la frontière de P .

Théorème de Pick ([De], Thm 2) : Si $P \subset \mathbb{R}^2$ est un polygone (convexe) entier on a :

$$vol(P) = card(P \cap \mathbb{Z}^2) - \frac{1}{2}card(\partial P \cap \mathbb{Z}^2) - 1 \quad (2)$$

Démonstration :

Etape 1 : Cas d'un triangle à 3 points entiers :

Nous allons commencer par traiter le cas d'un triangle T dont les seuls points entiers sont les sommets. On fabrique ensuite un parallélogramme par symétrie de T par rapport au milieu d'un de ses côtés. Les seuls points entiers de ce parallélogramme sont donc ses 4 sommets. Ainsi, par la proposition 3 et la formule (1), l'aire de T vaut $\frac{1}{2}$, et la formule (2) est ainsi vérifiée (en effet $vol(P) = card(P \cap \mathbb{Z}^2) - \frac{1}{2}card(\partial P \cap \mathbb{Z}^2) - 1 \Leftrightarrow \frac{1}{2} = 3 - \frac{1}{2} * 3 - 1$).

Etape 2 : Cas d'un triangle à n points entiers :

On considère maintenant le cas d'un triangle entier T quelconque. On va procéder par récurrence sur le nombre de point entier qu'il contient. C'est-à-dire qu'on va décomposer T en réunion de triangles entiers possédant strictement moins de points entiers que T . En effet, on peut supposer que T à au moins 4 points entiers. Soit donc $x \in T \cap \mathbb{Z}^2$ tel que x n'est pas un sommet de T . En joignant x à l'un des sommets de T , on découpe T en 2 ou 3 triangles, suivant si x est sur le bord de T ou non.

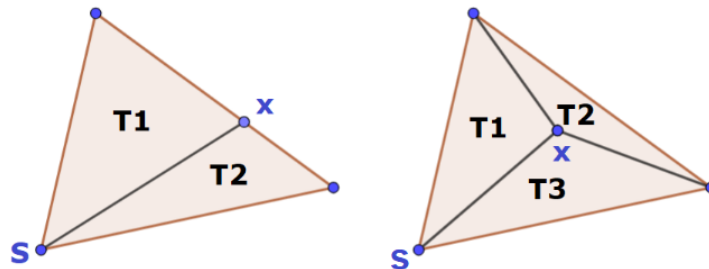
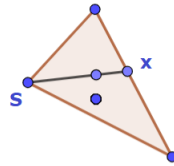


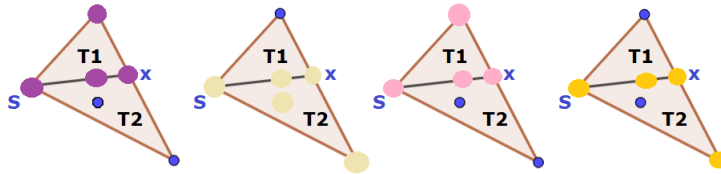
Figure 5: Illustration des deux découpages que l'on peut obtenir

Par hypothèse de récurrence, l'égalité est vraie pour ces triangles. En effet, dans le premier cas on note T_1 et T_2 les triangles qui composent T , et s le sommet de T opposé à x . Nous allons illustrer chacun des termes du calcul suivant. Chaque ligne de calcul sera suivie de son exemple illustré dans le cas du triangle ci-après (où chaque point bleu est un point entier). En effet les points entiers correspondant à chaque terme du calcul seront mis en évidence à l'aide d'une couleur :

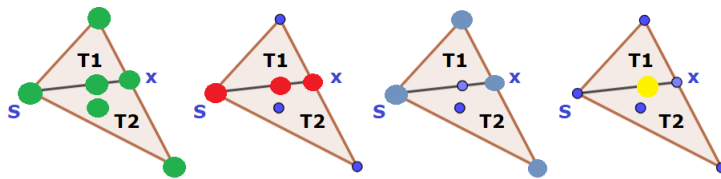


Le calcul nous donne donc :

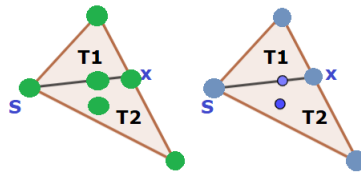
$$\begin{aligned} \text{vol}(T) &= \text{vol}(T_1) + \text{vol}(T_2) \\ &= \text{card}(T_1 \cap \mathbb{Z}^2) + \text{card}(T_2 \cap \mathbb{Z}^2) - \frac{1}{2}(\text{card}(\partial T_1 \cap \mathbb{Z}^2) + \text{card}(\partial T_2 \cap \mathbb{Z}^2)) - 2 \end{aligned}$$



$$= \text{card}(T \cap \mathbb{Z}^2) + \text{card}([sx] \cap \mathbb{Z}^2) - \frac{1}{2}(\text{card}(\partial T \cap \mathbb{Z}^2) + 2\text{card}([sx] \cap \mathbb{Z}^2) + 2) - 2$$



$$= \text{card}(T \cap \mathbb{Z}^2) - \frac{1}{2}\text{card}(\partial T \cap \mathbb{Z}^2) - 1$$



On a donc bien l'égalité dans le premier cas. Un raisonnement similaire permet de montrer l'égalité dans le deuxième cas.

Etape 3 : Généralisation à tout polytope :

Finalement, le cas d'un polytope entier quelconque se démontre par une récurrence sur son nombre de sommets. En effet, soit s un sommet d'un polytope entier P . P s'écrit comme réunion du polytope $Q = P \setminus \{s\}$ (qui a donc un sommet de moins que P) et du triangle de sommets s et les sommets de P qui sont voisins de s .

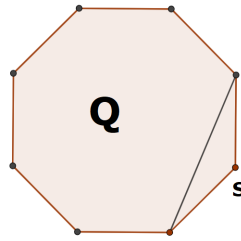


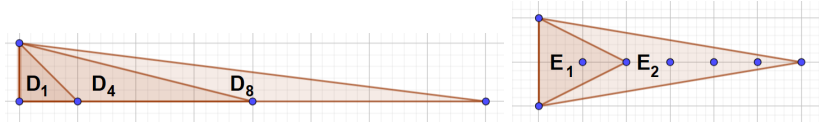
Figure 6: Illustration du cas général

Par hypothèse de récurrence, la formule est vraie pour les deux polytopes ainsi formés, le même raisonnement que précédemment montre que l'égalité reste vraie pour P .

■

Si les seuls points entiers d'un polygone entier P sont sur son bord, on déduit de la formule de Pick l'égalité $\text{card}(P \cap \mathbb{Z}^2) = 2\text{vol}(P) + 2$, on a alors réussi à estimer le nombre de points entiers en fonction du volume de manière exacte. Cependant, cette quantité n'est pas bornée comme nous le montre l'exemple de gauche ci dessous avec le triangle D_d de coordonnées $(0,0)$, $(0,1)$ et $(d,0)$.

La situation sera complètement différente pour les polygones entiers ayant au moins un point entier intérieur, ce sera l'objet de la prochaine section. En effet, on voit avec la figure de droite ci-après que si on prend le triangle E_d (coordonnées $(0,0)$, $(0,2)$ et $(d,1)$) avec un seul point entier intérieur, on remarque que lorsque $d \rightarrow \infty$, E_d finira forcément par contenir un point entier intérieur supplémentaire.



4.2 Généralisation à toute dimension : Théorème d'Ehrhart

Théorème d'Ehrhart ([De], Thm 4): Soit P un polytope entier dans \mathbb{R}^n . La fonction

$$\phi_P = \begin{cases} \mathbb{N}^* \rightarrow \mathbb{N}^* \\ m \mapsto \text{card}(mP \cap \mathbb{Z}^n) \end{cases}$$

1. est polynomiale de degré la dimension r de P
2. son coefficient dominant est le volume r -dimensionnel de P
3. $\forall m \in \mathbb{N} : \text{card}(mP' \cap \mathbb{Z}^n) = (-1)^r \phi_P(-m)$.

Un polytope entier P dans \mathbb{R} est un intervalle $[p, q]$. Il contient $q - p + 1$ points entiers et

$$\phi_P(m) = mq - mp + 1$$

$$\phi_{P'}(m) = mq - mp - 1 = -\phi_P(-m)$$

On a de même $\phi_{[p,q]}(m) = mq - mp = m\phi_{[p,q]}(1)$. On a la même formule pour un segment entier semi-ouvert dans le plan. Lorsque P est de dimension 2, on en déduit $\phi_{\partial P}(m) = m\phi_{\partial P}(1)$ d'où, en utilisant la formule de Pick,

$$\phi_P(m) = \text{vol}(mP) + \frac{1}{2} \text{card}(\partial(mP) \cap \mathbb{Z}^n) + 1 = m^2 \text{vol}(P) + \frac{m}{2} \text{card}(\partial P \cap \mathbb{Z}^n) + 1$$

$$\phi_{P'}(m) = \phi_P(m) - \text{card}(\partial(mP) \cap \mathbb{Z}^n) = m^2 \text{vol}(P) - \frac{m}{2} \text{card}(\partial P \cap \mathbb{Z}^n) + 1 = \phi_P(-m)$$

De même, on peut déduire la formule de Pick du théorème.

Comme le théorème d'Ehrhart se divise en trois résultats différents, nous allons faire trois démonstrations distinctes.

Nous rappelons également la relation de pascal qui va nous servir dans la première démonstration : $\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}$ pour $k, n \in \mathbb{N}$ avec $0 \leq k \leq n-1$.

Démonstration 1: Pour montrer la première partie du théorème, on va traiter le cas d'un r -simplexe entier S , et la proposition 2 donnera le résultat pour tout polytope entier P de \mathbb{R}^n . Prenons donc S comme définit ci-dessus, de sommets $\{0, s_1, \dots, s_n\}$. On remarque que $\forall m \in \mathbb{N}^*$, il y a égalité entre l'ensemble mS et la réunion disjointe $\bigcup_{j=0}^m S_{m,j}$ avec $S_{m,j} = \{\lambda_1 s_1 + \dots + \lambda_r s_r \mid \forall i \in \{0, \dots, r\}, \lambda_i \geq 0, \sum_{i=1}^r \lambda_i \leq m, \sum_{i=1}^r [\lambda_i] = m - j\}$.

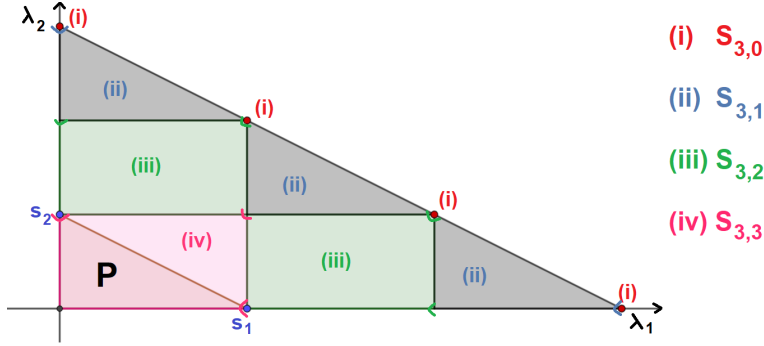


Figure 7: Visualisation des $S_{m,j}$ dans le cas $m = 3$ et P un triangle

On observe que $S_{m,j}$ peut se décomposer en une réunion disjointe d'ensembles possédant tous le même nombre a_j de points entiers que l'ensemble $\{\mu_1 s_1 + \dots + \mu_r s_r \mid \forall i \in \{1, \dots, r\}, \mu_i \in [0, 1[, \sum_{i=1}^r \mu_i \leq j\}$, et que le cardinal de cette réunion disjointe est le nombre de solution entière de l'équation $\sum_{i=1}^r x_i = m - j$, c'est à dire $\binom{m-j+r-1}{r-1}$. Le nombre de points entiers de $S_{m,j}$ est donc le produit de ces deux valeurs. Finalement, $a_j = a_r, \forall j \geq r$, on en déduit :

$$\begin{aligned}
 \text{card}(mS \cap \mathbb{Z}^n) &= \sum_{j=0}^m a_j \binom{m-j+r-1}{r-1} \\
 &= \sum_{j=0}^{r-1} a_j \binom{m-j+r-1}{r-1} + a_r \sum_{j=r}^m \binom{m-j+r-1}{r-1} \\
 &= \sum_{j=0}^{r-1} (a_j - a_r) \binom{m-j+r-1}{r-1} + a_r \sum_{j=0}^m \binom{m-j+r-1}{r-1}
 \end{aligned}$$

La relation du triangle de Pascal permet de calculer la deuxième somme :

$$\begin{aligned}
 &= \sum_{j=0}^{r-1} (a_j - a_r) \binom{m-j+r-1}{r-1} + a_r \sum_{j=0}^{m-2} \binom{m-j+r-1}{r-1} + \binom{r}{r-1} + \binom{r-1}{r-1} \\
 &= \sum_{j=0}^{r-1} (a_j - a_r) \binom{m-j+r-1}{r-1} + a_r \sum_{j=0}^{m-3} \binom{m-j+r-1}{r-1} + \binom{r+1}{r-1} + \binom{r+1}{r}
 \end{aligned}$$

On itère le procédé m fois pour obtenir :

$$\begin{aligned}
 &= \sum_{j=0}^{r-1} (a_j - a_r) \binom{m-j+r-1}{r-1} + a_r \left(\binom{m+r-1}{r-1} + \binom{m+r-1}{r} \right) \\
 &= \sum_{j=0}^{r-1} (a_j - a_r) \binom{m-j+r-1}{r-1} + a_r \binom{m+r}{r}
 \end{aligned}$$

Or $\sum_{j=0}^{r-1} (a_j - a_r) \binom{m-j+r-1}{r-1}$ est une somme de polynômes en m , où le j -ème terme de la somme est de degré j , et $a_r \binom{m+r}{r}$ est un polynôme de degré r en m , la somme de ces deux termes est donc un polynôme en m de degré r , et son coefficient dominant est donc celui de $a_r \binom{m+r}{r}$, à savoir $\frac{1}{r!}$. ■

Démonstration 2 : Montrons que le coefficient dominant correspond au volume r -dimensionnel de P .

Pour tout convexe compact K dans \mathbb{R}^n , on a que

$$\frac{\text{card}(mK \cap \mathbb{Z}^n)}{m^n} = \text{vol}(\mathcal{C}_{\frac{1}{m}}) * \text{card}(K \cap \frac{1}{m}\mathbb{Z}^n)$$

où $\mathcal{C}_{\frac{1}{m}}$ est un cube de coté $\frac{1}{m}$, donc $\text{vol}(\mathcal{C}_{\frac{1}{m}}) = \frac{1}{m^n}$ et $\text{card}(mK \cap \mathbb{Z}^n) = \text{card}(K \cap \frac{1}{m}\mathbb{Z}^n)$ car les deux ensembles $mK \cap \mathbb{Z}^n$ et $K \cap \frac{1}{m}\mathbb{Z}^n$ sont finis et $f : \begin{cases} mK \cap \mathbb{Z}^n & \rightarrow & K \cap \frac{1}{m}\mathbb{Z}^n \\ x & \mapsto & \frac{1}{m}x \end{cases}$ est bijective.

En effet, elle est injective car $\forall x, y \in mK \cap \mathbb{Z}^n, f(x) = f(y) \Rightarrow \frac{x}{m} = \frac{y}{m} \Rightarrow x = y$. De plus, elle est surjective car $\forall y \in K \cap \frac{1}{m}\mathbb{Z}^n$ on a : $y \in K \Rightarrow my \in mK$ et $y \in \frac{1}{m}\mathbb{Z}^n \Rightarrow my \in \mathbb{Z}^n$. Finalement, $my \in mK \cap \mathbb{Z}^n$ et $f(my) = y$.

Or, lorsque $m \rightarrow +\infty$, $\text{vol}(\mathcal{C}_{\frac{1}{m}}) * \text{card}(K \cap \frac{1}{m}\mathbb{Z}^n)$ est supérieur au volume de la réunion des cubes à sommets dans $\frac{1}{m}\mathbb{Z}^n$, de cotés $\frac{1}{m}$ et contenus dans K , et inférieur au volume de la réunion de ces mêmes cubes, mais dont un sommet au plus est dans K . On voit alors que la limite de $\frac{\text{card}(mK \cap \mathbb{Z}^n)}{m^n}$ est bien le volume r -dimensionnel de K . ■

Démonstration 3 : On va maintenant montrer la dernière partie du théorème, appelée formule de réciprocity.

Déjà, si P est un r -simplexe, on démontre de manière analogue à ci-dessus, la formule $\phi_{P'}(m) = (-1)^r \phi_P(-m)$. Si P n'est pas un simplexe, on va faire une récurrence sur le nombre de points entiers de P , comme dans la démonstration du théorème de Blichfeldt. On décompose P en de deux polytopes Q et R ayant tout deux strictement moins de points entiers que P , et tels que $Q \cap R$ soit une facette commune de ces deux polytopes, que l'on appelle F . Alors on a :

$$\begin{aligned} \phi_P(m) &= \phi_Q(m) + \phi_R(m) - \phi_F(m) \\ \phi_{P'}(m) &= \phi_{Q'}(m) + \phi_{R'}(m) + \phi_{F'}(m) \\ &= (-1)^r \phi_Q(-m) + (-1)^r \phi_R(-m) + (-1)^{r-1} \phi_F(-m) \\ &= (-1)^r (\phi_Q(-m) + \phi_R(-m) - \phi_F(-m)) = (-1)^r \phi_P(-m) \end{aligned}$$

ce qui termine la preuve. ■

De plus, il est aussi relativement aisé de déterminer le deuxième coefficient du polynôme d'Ehrhart d'un polytope entier, et ce grâce à la formule de réciprocité. En effet, notons $\phi_P(m) = \sum_{k=0}^r a_k m^k$ le polynôme d'Ehrhart d'un polytope entier P de dimension r . On va s'intéresser au polynôme $\phi_P(m) - \phi_{P'}(m)$. Déjà, on observe que ce polynôme renvoie la valeur $\text{card}(\partial mP \cap \mathbb{Z}^n)$. Aussi, comme $\phi_{P'}(m) = (-1)^r \sum_{k=0}^r a_k (-1)^k m^k$, on a que le coefficient dominant de $\phi_P(m) - \phi_{P'}(m)$ est $2a_{r-1}$. Ainsi, en raisonnant de façon similaire à la démonstration précédente, on montre que $\lim_{m \rightarrow +\infty} \frac{\text{card}(\partial mP \cap \mathbb{Z}^n)}{m^n}$ est la somme des volumes $(r-1)$ -dimensionnel des facettes du polytope mP , que l'on note S . Finalement, on obtient que $a_{r-1} = \frac{S}{2}$.

Force est de constater qu'après tout ce cheminement, nous avons uniquement montré qu'un tel polynôme existe et nous en avons déterminé les deux premiers coefficients. Théoriquement, il s'agit d'un résultat clé qui nous montre une égalité entre volume, points entiers et points entiers intérieurs. Néanmoins, connaître la totalité du polynôme d'Ehrhart peut s'avérer très compliqué en fonction du polytope étudié. Nous allons donc concentrer la suite de ce mémoire sur des résultats peut-être un peu moins précis, mais plus facile à mettre en place et à étudier.

5 Estimation du nombre de points entiers à partir du nombre de points entiers intérieurs

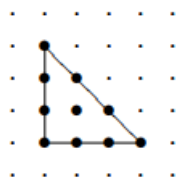
Intéressons nous désormais aux polygones qui contiennent au moins un point entier intérieur.

5.1 Dimension 2 et Théorème de Scott

Théorème de Scott ([De], Thm 3) : Soit P un polygone (convexe) entier dont le nombre k de points entiers intérieurs n'est pas nul. On a

$$\text{card}(P \cap \mathbb{Z}^2) \leq 3k + 6$$

sauf si P est équivalent au triangle



avec un point entier intérieur et 10 points entiers.

Avant de démontrer ce théorème, nous allons énoncer un lemme qui nous servira dans la preuve.

Lemme 1 : Soient $[AB]$ et $[CD]$ deux segments entiers de la droite d'équation $x = 0$, respectivement de longueur h et k . Soit $p \in \mathbb{N}$ tel que $p > h + k$. Alors il existe des points entiers P, R respectivement sur $[AB], [CD]$ tels que la distance PR vérifie $PR = mp + u$ avec $m \in \mathbb{N}^*$ et $u \in \mathbb{Z}$ vérifiant $|u| \leq \frac{1}{2}(p - h - k)$.

Démonstration : Soit $[AB]$ le segment $[0, h]$ et $[A'B']$ le segment $[p, p+h]$ obtenu en translatant $[AB]$ par p . On peut translater $[CD]$ par un multiple entier de p , pour obtenir le segment $[t, t+k]$, vérifiant $0 \leq t < p$. En fait, on peut même supposer que $h < t < p - k$, car sinon $[CD]$ chevaucherait l'un des deux segments entiers $[AB]$ ou $[A'B']$, et on aurait le résultat voulu avec $u = 0$.

Par conséquent, on peut supposer les points A, B, C, D, A', B' sont alignés dans cet ordre, le long de l'axe des abscisses. En posant $BC = x$ et $DA' = y$, on a alors que : $BA' = p - h = x + k + y$ d'où $x + y = p - h - k$. On observe que x et y ne peuvent pas être supérieurs à $\frac{1}{2}(p - h - k)$ simultanément, ce qui termine la preuve. ■

Démonstration du théorème de Scott: Soit P un polytope convexe entier dont le nombre de points entiers intérieurs est non nul. L'objectif de la démonstration est de majorer $\delta = 2(\text{card}(\partial P \cap \mathbb{Z}^2) - \text{vol}(P) - 1)$ par 6, excepté dans le cas du triangle ci-dessus. En effet on a :

$$\begin{aligned} \delta &= 2(\text{card}(\partial P \cap \mathbb{Z}^2) - \text{vol}(P) - 1) \\ (\text{Pick}) &= 2\text{card}(\partial P \cap \mathbb{Z}^2) - 2(\text{card}(P \cap \mathbb{Z}^2) - \frac{1}{2}\text{card}(\partial P \cap \mathbb{Z}^2) - 1) - 2 \\ &= 3\text{card}(\partial P \cap \mathbb{Z}^2) - 2\text{card}(P \cap \mathbb{Z}^2) \\ &= 3\text{card}(\partial P \cap \mathbb{Z}^2) - 2\text{card}(P \cap \mathbb{Z}^2) + (3\text{card}(P' \cap \mathbb{Z}^2) - 3\text{card}(P' \cap \mathbb{Z}^2)) \\ &= (3\text{card}(\partial P \cap \mathbb{Z}^2) + 3\text{card}(P' \cap \mathbb{Z}^2)) - 2\text{card}(P \cap \mathbb{Z}^2) - 3\text{card}(P' \cap \mathbb{Z}^2) \\ &= \text{card}(P \cap \mathbb{Z}^2) - 3\text{card}(P' \cap \mathbb{Z}^2) \end{aligned}$$

Donc $\delta = \text{card}(P \cap \mathbb{Z}^n) - 3k$, c'est pour cela que l'on souhaite le majorer par 6.

On peut supposer que P est contenu entre les deux droites d'équation $y = 0$ et $y = h \geq 2$ car P contient au moins un point entier intérieur par hypothèse. On peut supposer de plus que P rencontre la droite d'équation $y = 0$ le long du segment entier $S_0 = [0, a]$ et la droite $y = h$ le long du segment entier S_h de longueur $b \geq a$. On a alors que $\text{card}(\partial P \cap \mathbb{Z}^2) \leq a + b + 2h$ et $\text{vol}(P) \geq \frac{1}{2}h(a + b)$ ce qui correspond à l'aire du trapèze de base S_0 et S_h contenu dans P par hypothèse.

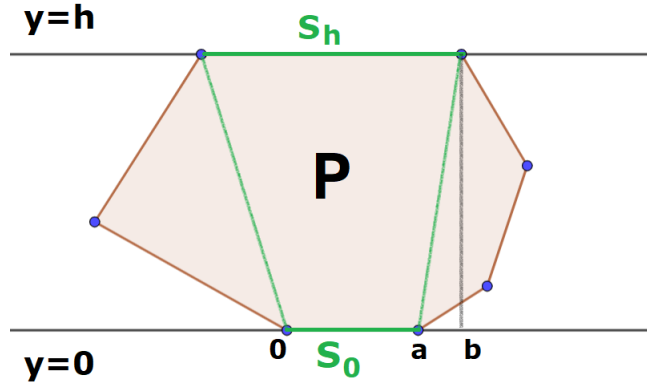


Figure 8: Illustration de la situation

On a donc $\delta \leq 2(a+b+2h) - h(a+b) - 2 = 6 - (a+b-4)(h-2)$. Il nous reste à étudier les différents cas possibles.

- **Cas $h = 2$:** On a bien $\delta \leq 6$
- **Cas $h = 3$:** On a $\delta \leq 6 \Leftrightarrow a+b > 3$. Il faut donc regarder le cas $a+b \leq 3$.
 Si $a+b \leq 2$, on a alors $\text{card}(\partial P \cap \mathbb{Z}^2) \leq 8$, d'où $\delta = \text{card}(P \cap \mathbb{Z}^2) - 3\text{card}(P' \cap \mathbb{Z}^2) = \text{card}(\partial P \cap \mathbb{Z}^2) - 2\text{card}(P' \cap \mathbb{Z}^2) \leq 6$ ($\text{card}(P' \cap \mathbb{Z}^2) \geq 1$ par hypothèse).
 Si $a+b = 3$, on a alors que $\text{card}(\partial P \cap \mathbb{Z}^2) \leq 9$ d'où $\delta \leq 7$. On a égalité si et seulement si $\text{card}(\partial P \cap \mathbb{Z}^2) = 9$ et $\text{card}(P' \cap \mathbb{Z}^2) = 1$. Cela implique par le théorème de Pick que $\text{vol}(P) = \frac{9}{2} = \frac{1}{2}h(a+b)$, ce qui montre que P est un trapèze de base S_0 et S_h . On ne peut pas avoir $a = 1$ et $b = 2$ car dans ce cas $\text{card}(\partial P \cap \mathbb{Z}^2) \leq 7$. D'où $a = 0$ et $b = 3$, P est donc un triangle, équivalent au cas particulier évoqué dans le théorème.
- **Cas $h \geq 4$ et $a+b \leq 3$:** On va se servir du lemme 1. On peut supposer que P rencontre les droites $y = 0$ et $y = h$ respectivement le long des points p et r , et les droites $x = 0$ et $x = h'$ (avec h' la plus grande distance entre les abscisses des point de P) respectivement le long des points q et s . On peut supposer $h' \geq h$, autrement, on échange les coordonnées et on se retrouve dans un des deux cas précédent.

On a toujours $\text{card}(\partial P \cap \mathbb{Z}^2) \leq a+b+2h$. On va appliquer à P l'équivalence $A : (x, y) \mapsto (x+my, y)$ où $m \in \mathbb{Z}$ tel que le segment entier $A(S_h) - (0, h)$, porté par l'axe des x , soit le plus près possible de S_0 . Une telle application préserve l'aire de P , $\text{card}(\partial P \cap \mathbb{Z}^2)$, h et $a+b$, ainsi que la convexité de P . Si jamais h' devient plus petit que h , on échange les coordonnées et on recommence le même processus (qui s'arrête forcément puisque l'entier $h+h'$ décroît strictement).

Ainsi, chaque point de la droite $y = h$ subi une translation le long de cette droite par un multiple de h . Il est donc possible, d'après le lemme 1, de choisir les points P et R de manière que la différence entre leurs abscisses, notée d , vérifie $0 \leq d \leq \frac{1}{2}(h-a-b)$ après avoir appliqué A à P .

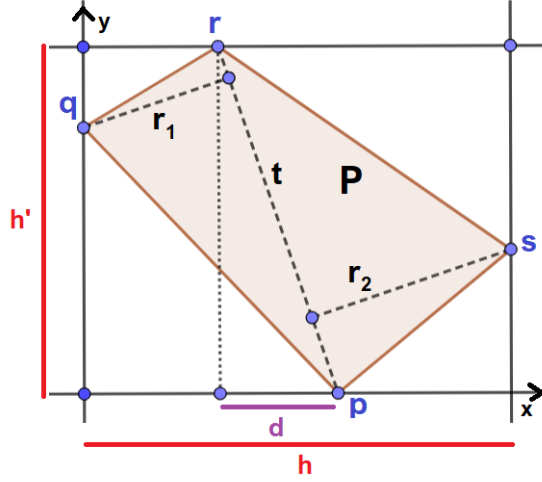


Figure 9: Illustration de la situation

Comme P est convexe, $A(P)$ l'est aussi et contient donc le quadrilatère $pqrs$ d'où :

$$vol(P) \geq vol(pqrs) = \frac{1}{2}t(r_1+r_2) \geq \frac{1}{2}h(h'-d) \geq \frac{1}{2}h(h-d) \geq \frac{1}{4}h(h+a+b)$$

D'où $\delta \leq 2(a+b+2h) - \frac{1}{2}h(h+a+b) - 2 = \frac{1}{2}h(8-h) - \frac{1}{2}(a+b)(h-4) - 2 \leq 6$ ce qui termine la preuve.

■

Proposition 4 : On en déduit de la formule de Pick la majoration

$$vol(P) \leq 2k + 2$$

(sauf dans le cas exceptionnel du triangle évoqué au théorème précédent).

Démonstration : La formule de Pick nous donne :

$$\begin{aligned} vol(P) &= card(P \cap \mathbb{Z}^2) - \frac{1}{2}card(\partial P \cap \mathbb{Z}^2) - 1 \\ &= card(P \cap \mathbb{Z}^2) - \frac{1}{2}card(P \cap \mathbb{Z}^2) - \frac{1}{2}card(P' \cap \mathbb{Z}^2) - 1 \\ &= \frac{1}{2}card(P \cap \mathbb{Z}^2) - \frac{1}{2}card(P' \cap \mathbb{Z}^2) - 1 \\ &\leq \frac{3k+6}{2} - \frac{k}{2} - 1 \leq 2k + 2 \text{ (Théorème de Scott)} \end{aligned}$$

■

5.2 Généralisation à toute dimension : Théorème de Hensley

5.2.1 Enoncé du théorème

Ce paragraphe va nous permettre de généraliser le théorème de Scott en toute dimension.

Théorème de Hensley ([De], Thm 6) : Soient $k, n \in \mathbb{N}^*$. Il existe une constante $B(k, n)$ ne dépendant que de k et n , telle que, pour tout polytope entier P de dimension n avec exactement k points entiers intérieurs, on ait

$$\text{vol}(P) \leq B(k, n)$$

À l'aide de l'inégalité de Blichfeldt on en déduit immédiatement le résultat suivant :

Corollaire 1 : Soit P un polytope entier de dimension n avec exactement $k > 0$ points entiers intérieurs. On a

$$\text{card}(P \cap \mathbb{Z}^n) \leq n + n!B(k, n)$$

Une constante $B(k, n)$ est explicitement calculée par Hensley. Elle est améliorée par Lagarias et Ziegler en $B(k, n) = k(7(k+1))^{n2^{n+1}}$, qui n'est pas loin d'être optimale. Ces démonstrations sont assez techniques, nous avons fait le choix de ne pas les détailler dans ce mémoire. Pour plus d'informations, voir [LZ].

5.2.2 Coefficient de symétrie

Avant de débiter la démonstration il est important d'introduire la notion de coefficient de symétrie d'un convexe. Soit K un convexe compact de \mathbb{R}^n et soit x un point intérieur à K . Toute demi-droite affine l issue de x coupe le bord de K en un point x_l^+ ; on note x_l^- le point analogue défini par la demi-droite opposée.

Définition 10 : Le **coefficient de symétrie** de K par rapport à x est :

$$\alpha(K, x) = \min_l \frac{\|x - x_l^+\|}{\|x - x_l^-\|}$$

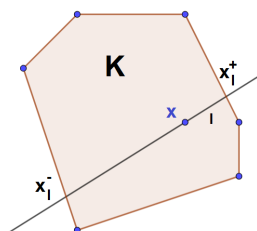


Figure 10: Visualisation des points x_l^+ et x_l^- en dimension 2

Pour un polytope P à r sommets $\{s_1, \dots, s_r\}$, revenant au cas général d'un point intérieur x quelconque, si, $\forall i \in \{1, \dots, r\}$, on note y_i , l'autre point d'intersection de la droite $(s_i x)$ avec le bord de P , on a

$$\alpha(P, x) = \min_{1 \leq i \leq r} \frac{\|x - y_i\|}{\|x - s_i\|} \quad (3)$$

Nous admettrons le résultat suivant qui va s'avérer utile dans la démonstration du théorème de Hensley.

Corollaire 2 : Soit K un compact convexe de \mathbb{R}^n contenant au moins un point entier intérieur x . On a :

$$\text{card}(\hat{K} \cap \mathbb{Z}^n) \geq \text{vol}(K) \left(\frac{\alpha(K, x)}{2} \right)^n$$

Les deux prochaines sous sections vont nous permettre de démontrer le théorème de Hensley.

5.2.3 Cas des simplexes

On va donc commencer par montrer que les points entiers intérieurs d'un simplexe entier ne peuvent pas être trop près du bord. C'est-à-dire que le coefficient de symétrie d'un simplexe entier par rapport à un point entier intérieur n'est pas trop petit.

Proposition 5 : $\forall k, n \in \mathbb{N}^* \exists \epsilon(k, n) > 0$ telle que, pour tout n -simplexe entier S avec exactement k points intérieur, et tout point entier intérieur x de S , on ait :

$$\alpha(S, x) \geq \epsilon(k, n)$$

La constante $\epsilon(k, n)$ est explicite. La valeur obtenue par Hensley est de l'ordre de $(4k)^{-2n!}$. C'est cette proposition que Lagarias et Ziegler améliorent, obtenant $\epsilon(k, n) \geq (7k + 7)^{-2^{n+1}}$. Pour plus de détails, voir [LZ]. Le théorème de Hensley pour les simplexes se déduit immédiatement de la proposition grâce au corollaire 2.

Corollaire 3 : $\forall k, n \in \mathbb{N}^*$ et tout n -simplexe entier S avec exactement k points intérieurs, on a :

$$\text{vol}(S) \leq k \left(\frac{2}{\epsilon(k, n)} \right)^n$$

Afin de démontrer la proposition précédente, nous allons d'abord énoncer et démontrer plusieurs lemmes.

Lemme 2 : Soient $(x_1, \dots, x_n) \in \mathbb{R}^n$ et soit $N \in \mathbb{N}^*$ fixé. $\exists (p_1, \dots, p_n, q) \in \mathbb{N}$ avec $1 \leq q \leq N^n$ tels que $|x_i - \frac{p_i}{q}| \leq \frac{1}{Nq} \forall i \in \{1, \dots, n\}$.

Démonstration : $\forall x \in \mathbb{R}$, on note $\{x\} = x - [x]$ sa partie fractionnaire. Au moins deux des $N^n + 1$ vecteurs (kx_1, \dots, kx_n) de $[0, 1]^n$, lorsque k décrit $[0, N^n]$, tombent dans le même cube de côté $\frac{1}{N}$ et à sommets dans $\frac{1}{N}\mathbb{Z}^n$. Notons k_1 et $k_2 > k_1$ les valeurs de k pour deux de ces points, et soit $q = k_2 - k_1$, il vient que $0 < q \leq k_2 \leq N^n$. Enfin, soit p_i l'entier le plus proche de qx_i . On a alors que $|qx_i - p_i| \leq |k_2x_i - k_1x_i - ([k_1x_i] - [k_2x_i])| = |\{k_2x_i\} - \{k_1x_i\}| \leq \frac{1}{N}$ ce qui conclut la preuve. ■

Lemme 3 : Soient $(x_1, \dots, x_n) \in (\mathbb{R}_+^*)^n$, avec $\sum_{i=1}^n x_i = 1$ et soit $N \geq n$ un entier. $\exists(p_1, \dots, p_n, q) \in \mathbb{N}$, $q = \sum_{i=1}^n p_i$ et $1 \leq q \leq N^{n-1}$, tels que $|qx_1 - p_1| \leq \frac{n}{N}$ et $|qx_i - p_i| \leq \frac{1}{N} \forall i \in \{2, \dots, n\}$.

Démonstration : On applique le lemme 2 à (x_2, \dots, x_n) . On a alors que $\forall i \in \{2, \dots, n\}$, on a $|qx_i - p_i| \leq \frac{1}{N}$ et $qx_i > 0$. On a donc $p_i \geq 0$ (sinon, $|qx_i - p_i| \geq 1$ ce qui amène à une contradiction). Si on pose $p_1 = q - \sum_{i=2}^n p_i$, on a alors $|qx_1 - p_1| = |q - q \sum_{i=2}^n x_i + \sum_{i=2}^n p_i - q| \leq \frac{n}{N}$. Finalement, comme $qx_1 > 0$ et $\frac{n}{N} \leq 1$, on a à nouveau que $p_1 \geq 0$, ce qui termine la preuve de ce lemme. ■

Lemme 4 : $\forall k, n \in \mathbb{N}^*$, $\exists \alpha(k, n) > 0$ tel que, $\forall (x_1, \dots, x_n) \in (\mathbb{R}_+^*)^n$ tel que $1 > \sum_{i=1}^n x_i > 1 - \alpha(k, n)$, $\exists(p_1, \dots, p_n, q)$ avec $p_i \geq 0$ et $q = \sum_{i=1}^n p_i > 0$, vérifiant $(kq + 1) > kp_i \forall i \in \{1, \dots, n\}$

Démonstration : On va procéder par récurrence sur n .

- **Initialisation, cas n = 1 :** On cherche un entier $q > 0$ tel que $x > \frac{kq}{kq+1}$. Un tel entier q existe $\Leftrightarrow x > \frac{kq}{kq+1} \Leftrightarrow kqx + x > kq \Leftrightarrow kq(x+1) > -x \Leftrightarrow q < \frac{-x}{k(x-1)} \Leftrightarrow \frac{-x}{k(x-1)} > 1$. Cela est équivalent à dire $-x < kx + x \Leftrightarrow k < kx + x \Leftrightarrow \frac{k}{k+1} < x$. Or x doit aussi vérifier $1 > x > 1 - \alpha(k, 1)$, d'où $1 - \alpha(k, 1) \geq \frac{k}{k+1} \Leftrightarrow -\alpha(k, 1) \geq \frac{-1}{k+1} \Leftrightarrow \alpha(k, 1) \leq \frac{1}{k+1}$. Le lemme est donc vrai $\forall r \in]0, \frac{1}{k+1}[$.

- **Hérédité :** On considère que le lemme est vrai au rang $n - 1$: Posons $N = 1 + \max\{\lceil \frac{4k}{\alpha(k, n-1)} \rceil, 2kn(n+1)\}$ et $\alpha(k, n) = \frac{1}{4kN^{n-1}} \leq \frac{1}{2}\alpha(k, n-1)$. Prenons $x_1 \geq \dots \geq x_n > 0$ tels que $\sum_{i=1}^n x_i = 1 - \alpha$ avec $0 < \alpha < \alpha(k, n)$. Supposons que $x_n < \alpha(k, n-1) - \alpha$, alors $\sum_{i=1}^{n-1} x_i = 1 - \alpha - x_n > 1 - \alpha(k, n-1)$. Par hypothèse de récurrence on a p_1, \dots, p_{n-1} et q satisfaisant le lemme pour x_1, \dots, x_{n-1} , et, en prenant $p_n = 0$ pour x_n , le lemme est vrai au rang n .

Supposons donc $x_n \geq \alpha(k, n-1) - \alpha$. On peut appliquer le lemme 3 à $\frac{x_i}{1-\alpha}$, $\forall i \in \{1, \dots, n\}$, ce qui donne l'existence de p_1, \dots, p_n, q entiers tels que $\forall i \in \{1, \dots, n\}$, $p_i \geq 0$, $\sum_{i=1}^n p_i = q$ et $1 \leq q \leq N^{n-1}$ tels que $|qx_1 - p_1| \leq \frac{n}{N}$ et $|qx_i - p_i| \leq \frac{1}{N} \forall i \in \{2, n\}$
On observe alors que :

$$\begin{aligned}
(kq+1)x_1 - kp_1 &= x_1 + k(qx_1 - p_1) = x_1(1 - kq\frac{\alpha}{1-\alpha}) + k(q\frac{x_1}{1-\alpha} - p_1) \\
&\geq x_1(1 - 2kq\alpha) - \frac{kn}{N} \\
&\geq x_1(1 - 2kN^{n-1}\alpha) - \frac{kn}{N} \\
&> \frac{1}{2}x_1 - \frac{kn}{N} \\
&\geq \frac{1}{2(n+1)} - \frac{kn}{N} > 0
\end{aligned}$$

car $x_1 \geq \frac{1-\alpha}{n} \geq \frac{1}{n+1}$.

De même, on a aussi $\forall i \in \{2, \dots, n\}$: $(kq+1)x_i - kp_i \geq \frac{1}{2}x_n - \frac{k}{N} \geq \frac{1}{2}(\alpha(k, n-1) - \alpha) - \frac{k}{N} \geq \frac{1}{4}\alpha(k, n-1) - \frac{k}{N} > 0$. Le lemme est ainsi démontré. ■

Démonstration de la proposition 5 : On travaille sur S , un r -simplexe entier. On peut supposer que ses sommets sont $\{0, s_1, \dots, s_n\}$ et qu'il contient un point entier intérieur $x = \sum_{i=1}^n x_i s_i$ avec $\forall i \in \{1, \dots, n\}$, $x_i > 0$ et $\sum_{i=1}^n x_i < 1$ (l'inégalité est stricte car sinon x pourrait être sur le bord de S).

On a alors $\sum_{i=1}^n x_i \leq 1 - \alpha(k, n)$. En effet, si le résultat était faux, on pourrait appliquer le lemme 3 et considérer $\forall j \in \mathbb{N}$ le point entier suivant : $(jq+1)x - j \sum_{i=1}^n p_i s_i = \sum_{i=1}^n ((jq+1)x_i - jp_i) s_i$. Or $\sum_{i=1}^n ((jq+1)x_i - jp_i) < jq+1 - jq = 1$. De plus si $qx_i - p_i \geq 0$, on a que $(jq+1)x_i - jp_i \geq x_i > 0$. Si $qx_i - p_i < 0$ et $j \leq k$, on a que $(jq+1)x_i - jp_i \geq x_i + k(qx_i - p_i) > 0$. On aurait donc $k+1$ points entiers intérieurs à S ce qui est une contradiction.

On a donc bien $\sum_{i=1}^n x_i \leq 1 - \alpha(k, n)$. Si on note y l'autre point d'intersection de la droite $(0x)$ avec S , on a alors $\|x\| \leq (1 - \alpha(k, n))\|y\|$. Ce résultat est vrai pour toute droite (sx) où s est n'importe quel autre sommet de S . La formule (3) nous donne alors l'estimation $\alpha(S, x) \geq \frac{\alpha(k, n)}{1-\alpha(k, n)}$, ce qui termine la preuve. ■

5.2.4 Généralisation à tout polytope

Le plus dur est fait, il est simple de déduire le cas général à partir du cas des simplexes. On rappelle qu'il suffit de minorer le coefficient de symétrie de P par rapport à un point entier intérieur x . Il découle de la formule (3) que celui-ci est "atteint" en un sommet s : si F est une facette de P contenant l'autre point d'intersection y de la droite (sx) avec le bord de P , on a :

$$\alpha(P, x) = \frac{\|x - y\|}{\|x - s\|}$$

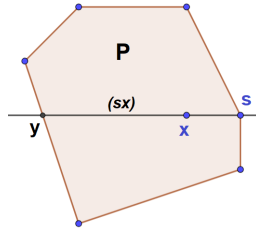


Figure 11: Visualisation des points x et y en dimension 2

Par le théorème de Carathéodory, il existe des sommets $\{s_1, \dots, s_r\}$ de F (donc de P) affinement indépendants (donc $r \leq n$), tels que y se trouve dans l'intérieur relatif du $(r - 1)$ -simplexe qu'ils engendrent. Soit S le r -simplexe de sommets $\{s, s_1, \dots, s_r\}$. Son intérieur relatif est contenu dans P' et contient exactement $k' \leq k$ points entiers, dont x . La proposition précédente entraîne

$$\alpha(P, x) \geq \alpha(S, x) \geq \epsilon(k', r)$$

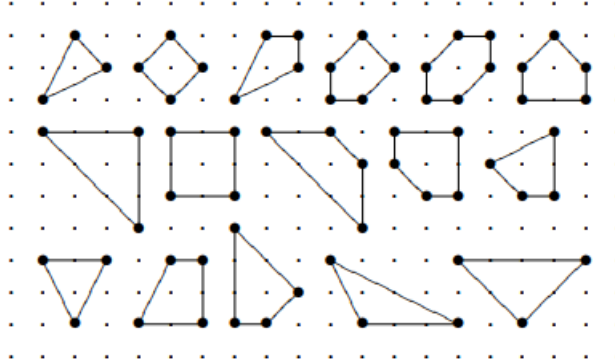
D'où, en utilisant le corollaire 2,

$$\text{vol}(P) \leq k \left(\frac{2}{\min_{1 \leq k' \leq k, 1 \leq r \leq n} \epsilon(k', r)} \right)^n$$

On a donc trouvé $B(k, n) = k \left(\frac{2}{\min_{1 \leq k' \leq k, 1 \leq r \leq n} \epsilon(k', r)} \right)^n$ ce qui montre le théorème de Hensley.

6 Polytope de Fano

Dans le cas particulier de la dimension deux, il y a, modulo les translations entières et l'action de $\mathcal{GL}_2(\mathbb{Z})$, exactement 16 polygones entiers possédant exactement un point entier intérieur. Ce sont les suivants :



Nous nous intéressons maintenant à une famille de polytopes entiers élémentaire, qui présente un grand intérêt en géométrie algébrique.

Définition 11 : Un polytope entier de dimension n est dit **polytope de Fano** s'il possède 0 comme seul point intérieur et si chacune de ses facettes a exactement n sommets, ceux-ci formant une base de \mathbb{Z}^n .

Avec cette définition il est simple de trouver qu'il y a 5 polytopes de Fano parmi les 16 de la liste ci-dessus, il s'agit en fait des 5 suivants :



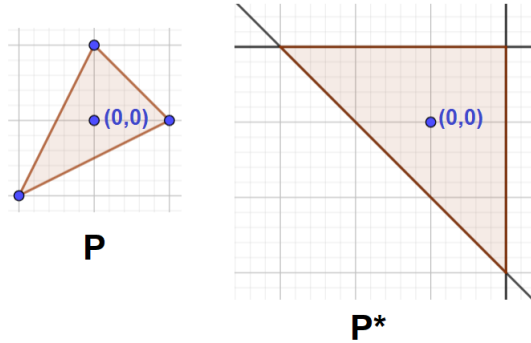
Remarque : Si P est un polytope de Fano et si f est le nombre de ses facettes, P est réunion de f n -simplexes ayant 0 comme sommet commun. De plus, les points entiers du bord de P sont exactement les sommets.

Si nous avons choisi d'aborder la notion de polytope de Fano, c'est parce qu'il nous permettent d'obtenir le résultat qui permet d'affiner encore plus notre étude.

Définition 12 : Si P est un polytope alors son **polytope dual**, noté P^* , est défini comme :

$$P^* = \{y \in \mathbb{R}^n \mid \langle x, y \rangle \leq 1, \forall x \in P\}$$

Exemple : En dimension 2, prenons $\{e_1, e_2\}$ une base d'un polytope $P = \text{Conv}(e_1, e_2, -e_1 - e_2)$, son polytope dual sera alors $P^* = \text{Conv}(e_1 + e_2, -2e_1 + e_2, e_1 - 2e_2)$ comme on peut le voir sur l'image ci-après.



Proposition 6 : Le dual d'un polytope de Fano est encore un polytope entier.

Démonstration : Soit P un polytope de Fano, P^* son dual et s^* un sommet de P^* . Comme chaque sommet de P^* est défini par une facette de P , on considère F la facette de P correspondant à s^* . Comme P est un polytope de Fano, on sait par définition que F a n sommets, que l'on va noter $s_i, \forall i \in \{1, \dots, n\}$, et que ces n sommets forment une base de \mathbb{Z}^n . On alors que $\forall i \in \{1, \dots, n\}$, $\langle s_i, s^* \rangle = 1$ (c'est la caractérisation du fait que s^* corresponde à la facette F).

On considère maintenant e_j un élément de la base canonique de \mathbb{Z}^n . On a alors qu'il existe des entiers n_i vérifiant $e_j = \sum_{i=1}^n n_i s_i$. Or la j -ème coordonnée s_j^* de s^* vérifie $s_j^* = \langle e_j, s^* \rangle = \langle \sum_{i=1}^n n_i s_i, s^* \rangle = \sum_{i=1}^n n_i \langle s_i, s^* \rangle = \sum_{i=1}^n n_i$, d'où chaque coordonnées de s^* est entière, s^* est donc un point entier, et P^* est un polytope entier. ■

Théorème de Casagrande ([De], Thm 8): Le nombre de sommets d'un polytope de Fano P de dimension n est au plus $3n$.

Remarque : Cette borne est bien plus petite que celle donnée par le résultat de Hensley. Elle est en fait valable pour tous les polytopes entiers dont les facettes sont toutes des simplexes et dont le polytope dual est aussi entier.

Démonstration : Considérons le polytope dual de P , noté P^* . Comme P est supposé de Fano, P^* est encore un polytope entier (pas forcément de Fano), qui n'a comme seul point entier intérieur 0. Donc $\exists m_1, \dots, m_r \in \mathbb{N}^*$ tels que $0 = m_1 s_1^* + \dots + m_r s_r^*$, où s_1^*, \dots, s_r^* sont les sommets de P^* . Ainsi, pour tout sommet s de P , on a :

$$\begin{aligned}
0 &= \sum_{i=1}^n m_i \langle s, s_i^* \rangle \\
&= \sum_{\langle s, s_i^* \rangle=1} m_i \langle s, s_i^* \rangle + \sum_{\langle s, s_i^* \rangle \leq 1} m_i \langle s, s_i^* \rangle \\
&\leq \sum_{\langle s, s_i^* \rangle=1} m_i - \sum_{\langle s, s_i^* \rangle=0} m_i
\end{aligned}$$

Puis, en notant S l'ensemble des sommets de P , et σ le cardinal de S , on obtient en sommant sur S :

$$\begin{aligned}
\sigma \sum_{i=1}^n m_i &\leq 2 \sum_{s \in S} \sum_{\langle s, s_i^* \rangle=1} m_i + \sum_{s \in S} \sum_{\langle s, s_i^* \rangle=0} m_i \\
&= 2 \sum_{i=1}^n m_i \text{card}\{s \in S \mid \langle s, s_i^* \rangle = 1\} + \sum_{i=1}^n m_i \text{card}\{s \in S \mid \langle s, s_i^* \rangle = 0\} \\
&\leq 3n \sum_{i=1}^n m_i
\end{aligned}$$

On se retrouve donc avec $\sigma \sum_{i=1}^n m_i \leq 3n \sum_{i=1}^n m_i \Leftrightarrow \sigma \leq 3n$ ce qui termine la preuve. ■

Il faut savoir qu'il existe une version plus précise de cet énoncé proposé par Batyrev en 1988. Elle donne notamment une majoration optimale dans le cas des polytopes de dimension impaire. Cependant, elle demande tout un développement sur les notions de variétés toriques que nous n'aborderons pas ici. Ces notions sont très bien abordées dans la référence [Ma].

References

- [Bo] Bonavero, L., Sur le nombre de sommets des polytopes entiers, Images des Mathématiques, 33–40, C.N.R.S., 200
- [De] Debarre, O., Polytope et points entiers. Revue de la Filière Mathématique RMS, 124e année, no1, octobre 2013.
- [E] Ehrhart, E., Demonstration de la loi de réciprocité pour un polyèdre entier, C. R. Acad. Sci. Paris 265 (1967), 5–7.
- [Fr] Francinou, S., Gianella, H., Nicolas, S., exercices de Mathématiques Oraux X-ENS, algèbre 3. Partie 4.44
- [LZ] Lagarias, J., Ziegler, G., Bounds for lattice polytopes containing a fixed number of interior points in a sublattice, Canad. J. Math. 43 (1991), 1022–1035.
- [Ma] Marnat, A., De l'étude des polytopes convexes, 4-Liens entre polytopes et variétés algébriques toriques (2010).
- [Sc] Scott, PR., On convex lattice polygons (1976).