POLYTOPES ET POINTS ENTIERS

par Olivier Debarre

École normale supérieure, Paris

RÉSUMÉ. *Un polytope est l'enveloppe convexe d'un ensemble fini de points de l'espace. Il est dit entier si ces points peuvent être choisis à coordonnées entières. Le thème général de ce texte est le comptage du nombre de points à coordonnées entières dans un polytope entier et la finitude de l'ensemble des types de polytopes entiers pour lesquels ce nombre est fixé non nul. Les techniques utilisées sont élémentaires. Outre leur intérêt propre, ces problèmes ont un lien très étroit avec des questions de géométrie algébrique.*

MOTS-CLÉS : *Polytopes, convexe, points à coordonnées entières, finitude.*

1. Introduction

Dans tout ce texte, un *polytope* est l'enveloppe convexe [1] d'un sous-ensemble fini de l'espace euclidien $\mathbb{R}^n$. C'est donc un compact (fermé et borné). Sa *dimension* est celle de l'espace affine qu'il engendre.

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.

Soit Σ un sous-ensemble de $\mathbb{R}^n$. Le théorème de Carathéodory énonce que *tout point de l'enveloppe convexe* $\mathrm{Conv}(\Sigma)$ *est barycentre, avec coefficients strictement positifs, d'un sous-ensemble de* Σ *formé de points affinement indépendants.*

1. L'enveloppe convexe d'un sous-ensemble Σ de $\mathbb{R}^n$ 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.

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. Par le théorème de Carathéodory, on peut écrire $s = \lambda_1 s_1 + \cdots + \lambda_m s_m$, avec $s_1, \ldots, s_m$ points de Σ affinement indépendants, $\lambda_i > 0$ et $\lambda_1 + \cdots + \lambda_m = 1$. Si $m > 1$, le point s est dans l'intérieur du segment joignant $(1 - \lambda_3 - \cdots - \lambda_m)s_1 + \lambda_3 s_3 + \cdots + \lambda_m s_m$ à $(1-\lambda_3-\cdots-\lambda_m)s_2+\lambda_3 s_3+\cdots+\lambda_m s_m$ ce qui est absurde. On a donc $m = 1$, c'est-à-dire $s \in \Sigma$.

Inversement, pour tout point s de Σ, notons $Q \subset P$ l'enveloppe convexe de $\Sigma - \{s\}$. On a $Q \neq P$ par minimalité de Σ. Notons x le point de Q le plus proche de 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, strictement positive en s. On en déduit que ϕ atteint son maximum sur P en le seul point s, qui est par conséquent un sommet de P.

□

Plus généralement, 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. En particulier, $\varnothing$ est une face de P. Il est aussi pratique de décréter que P est une face de P. Ces deux faces sont dites *impropres ;* les autres sont dites *propres.*

On montre que P n'a qu'un nombre fini de faces, et que chaque face est elle-même un polytope, enveloppe convexe des sommets de P qu'elle contient. 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.

2. Les simplexes

On appelle *r-simplexe* l'enveloppe convexe de $r+1$ points affinement indépendants dans $\mathbb{R}^n$. Les r-simplexes sont donc exactement les polytopes de dimension r avec $r+1$ sommets. 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. Soit s un sommet de P, soient $F_1, \ldots, F_r$ les faces (propres) de P ne contenant pas s et soient $F'_1, \ldots, F'_r$ leurs intérieurs relatifs. Les ensembles $\{s\}$, $\mathrm{Conv}(\{s\} \cup F'_1) - \{s\}, \ldots, \mathrm{Conv}(\{s\} \cup F'_r) - \{s\}$ forment une partition de P. En raisonnant par récurrence sur la dimension de P, on sait décomposer chaque F_i en réunion disjointe de simplexes ouverts dont les sommets sont des sommets de F_i, donc de P. En excluant les simplexes contenus dans $F_i - F'_i$, on obtient une décomposition de chaque F'_i en réunion disjointe de simplexes ouverts, donc aussi une telle décomposition de chaque $\mathrm{Conv}(\{s\} \cup F'_i) - \{s\}$.

□

Soit K un convexe compact d'intérieur non vide dans $\mathbb{R}^n$. Le volume euclidien de l'enveloppe convexe de points $s_0, \dots, s_n$ de $\mathbb{R}^n$ est

$$\frac{1}{n!}|\det(\overrightarrow{s_0s_1}, \dots, \overrightarrow{s_0s_n})|. \tag{1}$$

La fonction qui à $n+1$ points de K associe le volume de leur enveloppe convexe est donc continue. Elle atteint son maximum en $n+1$ points affinement indépendants et on peut parler d'un simplexe de volume maximal contenu dans K.

Un polytope P d'intérieur non vide dans $\mathbb{R}^n$ contient un simplexe de volume maximal dont les sommets sont des sommets de P. En effet, soit s un sommet d'un simplexe S de volume maximal contenu dans P. Considérons l'hyperplan affine H engendré par les autres sommets de S. Le point s est un point de P à distance maximale de H. L'intersection avec P de l'hyperplan affine parallèle à H et passant par s est par définition une face de P donc contient un sommet de P. On peut donc changer s en un sommet de P (sans changer les autres sommets de S). On procède ainsi pour chaque sommet de S.

Proposition 3. *Soit K un convexe compact d'intérieur non vide dans $\mathbb{R}^n$ et soit S un simplexe de volume maximal contenu dans K, de centre de gravité g_0. On a*

$$K \subset -nS + (n+1)g_0.$$

Démonstration. Quitte à effectuer une translation, on peut supposer $g_0 = 0$. Soient $s_0, \dots, s_n$ les sommets de S. Pour chaque i, on note H_i l'hyperplan affine passant par les sommets de S autres que s_i. Le convexe K est tout entier contenu dans la région R_i composée des points de $\mathbb{R}^n$ situés à distance moindre que $d(s_i, H_i)$ de H_i. Nous allons montrer que $\bigcap_{i=0}^{n} R_i$, qui contient donc K, est contenu dans $-nS$. En coordonnées barycentriques, on a

$$R_i = \Big\{ \sum_{j=0}^{n} \alpha_j s_j \;\Big|\; \sum_{j=0}^{n} \alpha_j = 1,\ |\alpha_i| \leqslant 1 \Big\},$$

puisque la distance d'un point $\sum_{j=0}^{n} \alpha_j s_j$ à H_i est $|\alpha_i|\, d\,(s_i, H_i)$. Posons $\beta_j = \dfrac{1-\alpha_j}{n}$. On a $\sum_{j=0}^{n} \beta_j = 1$ et comme $\sum_{j=0}^{n} s_j = 0$, on a aussi

$$R_i \subset \Big\{ -n \sum_{j=0}^{n} \beta_j s_j \;\Big|\; \sum_{j=0}^{n} \beta_j = 1,\ \beta_i \geqslant 0 \Big\}.$$

On en déduit $K \subset \bigcap_{i=0}^{n} R_i \subset -nS$.

□

3. Polytopes et points entiers

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 entiers. C'est un très vieux problème que d'estimer ou de relier le nombre de points entiers d'un tel polytope P, le nombre de points entiers dans son intérieur relatif P' et le volume de P.

Il est utile d'introduire le concept de base de $\mathbb{Z}^n$. La définition est la même que pour un espace vectoriel.

Définition 1. *Une famille $(x_1, \dots, x_n)$ de n vecteurs de $\mathbb{Z}^n$ en est une base si tout vecteur de $\mathbb{Z}^n$ peut s'écrire comme combinaison linéaire de $x_1, \dots, x_n$ à coefficients entiers.*

Attention, n vecteurs de $\mathbb{Z}^n$ peuvent être libres dans l'espace vectoriel $\mathbb{R}^n$ sans former une base de $\mathbb{Z}^n$. On a les caractérisations suivantes.

Proposition 4. *Soient $x_1, \dots, x_n$ des vecteurs de $\mathbb{Z}^n$ qui forment une base du $\mathbb{R}$-espace vectoriel $\mathbb{R}^n$. Les conditions suivantes sont équivalentes :*
(i) *la famille $(x_1, \dots, x_n)$ est une base de $\mathbb{Z}^n$;*
(ii) *le déterminant de $(x_1, \dots, x_n)$ dans la base canonique de $\mathbb{R}^n$ est ± 1 ;*
(iii) *le parallélépipède de sommet 0 et de côtés $x_1, \dots, x_n$ ne contient aucun point entier autre que les 2^n points $\varepsilon_1 x_1 + \cdots + \varepsilon_n x_n$, $\varepsilon_i \in \{0, 1\}$.*

Démonstration. Soit A la matrice (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 $\mathbb{R}^n$.

Si (i) est vérifié, la matrice B est à coefficients entiers et $AB = I_n$. En prenant les déterminants (entiers), on obtient (ii). Inversement, si le déterminant de A est ± 1, la formule donnant les coefficients de l'inverse A^{-1} à partir des cofacteurs (entiers) de A montre que B est aussi à coefficients entiers. On en déduit (i). Donc (i) et (ii) sont équivalents.

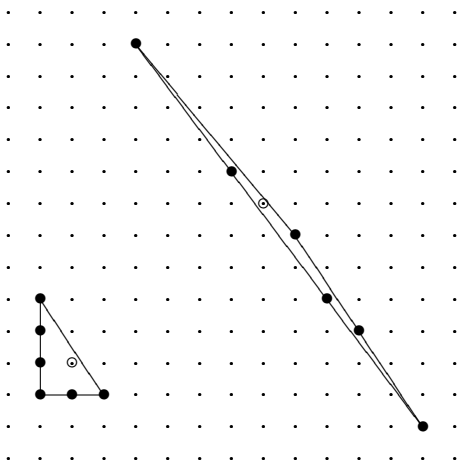
Supposons (iii) vérifié. Tout vecteur de $\mathbb{Z}^n$ peut s'écrire $\lambda_1 x_1 + \cdots + \lambda_n x_n$, avec $\lambda_1, \dots, \lambda_n \in \mathbb{R}$. Le point entier $(\lambda_1 - [\lambda_1])\, x_1 + \cdots + (\lambda_n - [\lambda_n])\, x_n$ est dans le parallélépipède construit sur les vecteurs $x_1, \dots, x_n$, donc $\lambda_i - [\lambda_i] = 0$ pour tout i et (i) est vérifié. Inversement, si (i) est vérifié, 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. Donc (i) et (iii) sont équivalents.

□

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 $\mathrm{GL}_n(\mathbb{Z})$ c'est-à-dire, par la proposition 4, 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*.

Attention, des polytopes équivalents peuvent sembler très différents, mais de notre point de vue, leurs propriétés sont les mêmes : même volume, même nombre de points entiers, même nombre de points entiers intérieurs. Les triangles suivants sont équivalents :



Ils sont chacun d'aire 3 et contiennent chacun 7 points entiers dont un seul intérieur.

L'inégalité suivante majore le nombre de points entiers en fonction du volume. C'est très important de notre point de vue : il nous « suffira » de majorer le volume d'un polytope entier ayant un nombre de points entiers intérieurs fixé.

Théorème 1 (Blichfeldt)**.** *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. On a*

$$\mathrm{card}(K \cap \mathbb{Z}^n) \leqslant n + n! \,\mathrm{vol}(K).$$

Démonstration. Quitte à remplacer K par l'enveloppe convexe de ses points entiers, on voit qu'il suffit de traiter le cas d'un polytope entier P de dimension n.

On procède par récurrence sur la quantité $\mathrm{Card}(P \cap \mathbb{Z}^n)$, qui est au moins égale à $n+1$. Si $\mathrm{Card}(P \cap \mathbb{Z}^n) = n+1$, le polytope P est un simplexe entier, donc de volume au moins égal à $\dfrac{1}{n!}$ par la formule (1).

Si P n'est pas un simplexe, il existe un sommet s de P tel que le polytope (entier) Q enveloppe convexe des sommets de P autres que s soit de dimension n. Le polytope Q est intersection de demi-espaces définis par ses facettes. Comme $s \notin Q$, il existe une de ces facettes, $F = Q \cap H$, telle que s et Q soient de part et d'autre de H. Soit R le polytope $\mathrm{Conv}(\{s\} \cup F)$. Les polytopes Q et R sont chacun de dimension n, ont strictement moins de

points entiers que P et ont au moins n sommets (entiers) en commun (ceux de F). De plus, $P = Q \cup R$ et $F = Q \cap R$. On en déduit, à l'aide de l'hypothèse de récurrence,

$$\begin{aligned} \mathrm{Card}(P \cap \mathbb{Z}^n) &\leqslant \mathrm{Card}(Q \cap \mathbb{Z}^n) + \mathrm{Card}(R \cap \mathbb{Z}^n) - n \\ &\leqslant n + n!\,\mathrm{vol}(Q) + n!\,\mathrm{vol}(R) \;=\; n + n!\,\mathrm{vol}(P), \end{aligned}$$

d'où le théorème.

□

Il n'y a bien sûr pas de majoration générale dans l'autre sens, puisqu'il existe des convexes compacts arbitrairement grands sans point entier. En revanche, pour certains polytopes, on peut obtenir une telle majoration. Ce sera l'objet du paragraphe 6.

4. Polygones entiers

Examinons tout d'abord le cas beaucoup plus simple des polygones (convexes), c'est-à-dire des polytopes de dimension 2. On souhaite estimer le nombre de points entiers sur le bord d'un polygone entier P en fonction du nombre de points entiers dans son intérieur $\overset{\circ}{P}$, ou encore sur son bord $\partial P = P - \overset{\circ}{P}$. Le premier résultat dans cette direction est le célèbre théorème de Pick.

Théorème 2 (Pick, 1900)**.** *Si $P \subset \mathbb{R}^2$ est un polygone (convexe) entier,*

$$\mathrm{vol}(P) = \mathrm{Card}(P \cap \mathbb{Z}^2) - \frac{1}{2}\,\mathrm{Card}(\partial P \cap \mathbb{Z}^2) - 1. \tag{2}$$

Démonstration. Considérons d'abord un triangle entier T dont les seuls points entiers sont les sommets. Les seuls points entiers du parallélogramme obtenu par symétrie de T par rapport au milieu d'un de ses côtés en sont les quatre sommets. Par la proposition 4, l'aire de T est donc 1/2 et la formule (2) est vérifiée dans ce cas.

On traite maintenant le cas d'un triangle entier quelconque, en procédant par récurrence sur le nombre de points entiers qu'il contient. Si T est un triangle entier avec au moins 4 points entiers, on choisit un point entier x dans T qui ne soit pas un sommet. En le joignant aux 3 sommets, on décompose T en la réunion de 2 ou 3 triangles, selon que x est sur le bord de T ou non, triangles pour lesquels la formule (2) est connue. Dans le premier cas, si T_1 et T_2 sont ces triangles et s le sommet de T opposé à x, on a ainsi

$$\begin{aligned} \mathrm{vol}(T) &= \mathrm{vol}(T_1) + \mathrm{vol}(T_2) \\ &= \mathrm{Card}(T_1 \cap \mathbb{Z}^2) + \mathrm{Card}(T_2 \cap \mathbb{Z}^2) \\ &\qquad -\frac{1}{2}\,\mathrm{Card}(\partial T_1 \cap \mathbb{Z}^2) - \frac{1}{2}\,\mathrm{Card}(\partial T_2 \cap \mathbb{Z}^2) - 2 \\ &= \mathrm{Card}(T \cap \mathbb{Z}^2) + \mathrm{Card}([sx] \cap \mathbb{Z}^2) \\ &\qquad -\frac{1}{2}\,\mathrm{Card}(\partial T \cap \mathbb{Z}^2) + 2\,\mathrm{Card}(]sx[\cap \mathbb{Z}^2) + 2) - 2 \\ &= \mathrm{Card}(T \cap \mathbb{Z}^2) - \frac{1}{2}\,\mathrm{Card}(\partial T \cap \mathbb{Z}^2) - 1. \end{aligned}$$

On procède de façon analogue si l'on a 3 triangles.

Enfin, on peut traiter le cas des polygones entiers généraux en procédant par récurrence sur le nombre de sommets. Si s est un sommet d'un polygone entier P, on écrit P comme la réunion du triangle de sommets s et les sommets de P voisins de s, et du polygone $\mathrm{Conv}(P - \{s\})$, qui a un sommet de moins que P. On utilise ensuite le même raisonnement que celui employé ci-dessus.

□

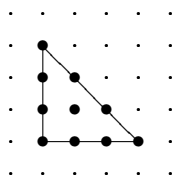
Si les seuls points entiers d'un polygone entier P sont sur son bord, on déduit de la formule de Pick l'égalité $\mathrm{Card}(P \cap \mathbb{Z}^2) = 2\,\mathrm{vol}(P) + 2$ et cette quantité n'est pas bornée comme le montre l'exemple du triangle de sommets $(0,0)$, $(0,1)$ et $(d,0)$ (d entier positif quelconque).

La situation est complètement différente pour les polygones entiers ayant au moins un point entier intérieur, comme le montre le résultat suivant.

Théorème 3 (Scott, 1976)**.** *Soit P un polygone (convexe) entier dont le nombre k de points entiers intérieurs n'est pas nul. On a*

$$\mathrm{Card}(P \cap \mathbb{Z}^2) \leqslant 3k + 6,$$

sauf si P est équivalent au triangle



avec un point entier intérieur et 10 points entiers.

On déduit de la formule de Pick la majoration

$$\mathrm{vol}(P) \leqslant 2k + 2,$$

sauf dans le cas exceptionnel ci-dessus.

Démonstration. Il s'agit de montrer que la quantité

$$\delta = \mathrm{Card}(P \cap \mathbb{Z}^2) - 3\,\mathrm{Card}(\overset{\circ}{P} \cap \mathbb{Z}^2) = 2(\mathrm{Card}(\partial P \cap \mathbb{Z}^2) - \mathrm{vol}(P) - 1)$$

est majorée par 6, sauf dans le cas du triangle ci-dessus.

On peut supposer que P est contenu entre les droites horizontales d'équation $y = 0$ et $y = h \geqslant 2$, qu'il rencontre la droite $y = 0$ le long du segment (entier) $S_0 = [0, a]$, ainsi que la droite $y = h$ le long d'un segment (entier) S_h de longueur $b \geqslant a$. On a

$$\mathrm{Card}(\partial P \cap \mathbb{Z}^2) \leqslant a + b + 2h \quad , \quad \mathrm{vol}(P) \geqslant \frac{1}{2}h(a+b)$$

donc

$$\delta \leqslant 2(a+b+2h) - h(a+b) - 2 = 6 - (a+b-4)(h-2).$$

On a $h \geqslant 2$ car P contient un point intérieur entier.

Si $h = 2$, on a terminé. Si $h = 3$ aussi, sauf si $a+b \leqslant 3$. Si $a+b \leqslant 2$, on a $\mathrm{Card}(\partial P \cap \mathbb{Z}^2) \leqslant 8$ et $\delta = \mathrm{Card}(\partial P \cap \mathbb{Z}^2) - 2\,\mathrm{Card}(P\mathbb{Z}^2) \leqslant 6$ puisque P contient (au moins) un point intérieur entier. Si $a+b = 3$, on a $\mathrm{Card}(\partial P \cap \mathbb{Z}^2) \leqslant 9$ et $\delta \leqslant 7$, avec égalité si et seulement si

$$\mathrm{Card}(\partial P \cap \mathbb{Z}^2) = 9\,, \quad \mathrm{Card}(\overset{\circ}{P} \cap \mathbb{Z}^2) = 1\,, \quad \mathrm{vol}(P) = \frac{9}{2} = \frac{1}{2}h(a+b).$$

Cette dernière égalité montre que P est un trapèze de bases S_0 et S_h. Si $a = 1$ (et $b = 2$), il y a au plus 7 points entiers sur le bord. Donc $a = 0$ et P est un triangle, équivalent au triangle ci-dessus.

Supposons donc $h \geqslant 4$ et $a + b \leqslant 3$. On peut aussi supposer que la plus grande différence h' entre abscisses de points de P est $\geqslant h$ (sinon, on échange les coordonnées). Appliquons une équivalence $A : (x, y) \mapsto (x + my, y)$, avec $m \in \mathbb{Z}$, de façon que le segment entier $A(S_h) - (0, h)$, porté par l'axe des x, soit le plus proche possible de S_0. La distance d entre ces deux segments entiers est alors $\frac{1}{2}(h - a - b)$. Si par hasard, h' est devenu $< h$, on échange les coordonnées et on recommence le processus (qui doit s'arrêter, puisqu'à chaque pas, l'entier $h + h'$ décroît strictement). On minore alors le volume de P par celui d'un quadrilatère pour obtenir

$$\mathrm{vol}(P) \geqslant \frac{1}{2}h(h' - d) \geqslant \frac{1}{4}h(h + a + b),$$

de sorte que

$$\begin{aligned} \delta &\leqslant 2(a+b+2h) - \frac{1}{2}h(h+a+b) - 2 \\ &= \frac{1}{2}h(8-h) - \frac{1}{2}(a+b)(h-4) - 2 \leqslant 6. \end{aligned}$$

Ceci termine la démonstration.

□

5. Le polynôme d'Ehrhart

Ce paragraphe est de nature un peu différente et n'est pas nécessaire pour la suite. Il est consacré à un très joli résultat qui généralise la formule de Pick en toute dimension et ne peut être passé sous silence.

Théorème 4 (Ehrhart, 1967)**.** *Soit P un polytope entier dans $\mathbb{R}^n$. La fonction*

$$\begin{aligned} \phi_P \quad : \quad & \mathbb{N} \longrightarrow \mathbb{N}^* \\ & m \longmapsto \mathrm{Card}(mP \cap \mathbb{Z}^n) \end{aligned}$$

est polynomiale, de degré la dimension r de P et de coefficient dominant le volume r-dimensionnel de P. On a d'autre part, pour tout entier $m > 0$,

$$\mathrm{Card}(mP' \cap \mathbb{Z}^n) = (-1)^r \phi_P(-m).$$

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

$$\begin{aligned} \phi_P(m) &= mq - mp + 1, \\ \phi_{P'}(m) &= mq - mp - 1 \;=\; -\phi_P(-m). \end{aligned}$$

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,

$$\begin{aligned} \phi_P(m) &= m^2 \,\mathrm{vol}(P) + \frac{m}{2}\,\mathrm{Card}(\partial P \cap \mathbb{Z}^n) + 1, \\ \phi_{P'}(m) &= \phi_P(m) - \mathrm{Card}(\partial(mP) \cap \mathbb{Z}^n) \\ &= m^2 \,\mathrm{vol}(P) - \frac{m}{2}\,\mathrm{Card}(\partial P \cap \mathbb{Z}^n) + 1 \;=\; \phi_P(-m). \end{aligned}$$

Inversement, on peut déduire la formule de Pick du théorème.

Démonstration du théorème 4. Grâce à la proposition 2, il suffit pour montrer la première moitié du théorème de traiter le cas d'un r-simplexe entier S, de sommets $0, s_1, \ldots, s_r$. L'ensemble mS est la réunion disjointe de ses sous-ensembles

$$S_{m,j} = \Big\{ \lambda_1 s_1 + \cdots + \lambda_r s_r \;\Big|\; \lambda_i \geqslant 0,\ \sum_{i=1}^r \lambda_i \leqslant m,\ \sum_{i=1}^r [\lambda_i] = m - j \Big\}$$

pour $j \in \{0, \ldots, m\}$. Le nombre de points entiers dans $S_{m,j}$ est le nombre de solutions entières positives de l'équation $\displaystyle\sum_{i=1}^r x_i = m - j$, c'est-à-dire $\binom{m-j+r-1}{r-1}$, fois le nombre a_j de points entiers de

$$\Big\{ \mu_1 s_1 + \cdots + \mu_r s_r \;\Big|\; \mu_i \in [0,1[\,,\ \sum_{i=1}^r \mu_i \leqslant j \Big\}.$$

Comme $a_j = a_r$ pour tout $j \geqslant r$, on en déduit

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

C'est donc bien un polynôme en m de degré r et de coefficient dominant $\dfrac{1}{r!}a_r$.

Pour tout convexe compact K dans $\mathbb{R}^n$, on a d'autre part

$$\frac{\mathrm{Card}(mK \cap \mathbb{Z}^n)}{m^n} = \mathrm{vol}\,\mathscr{C}_{\frac{1}{m}} \cdot \mathrm{Card}\Big(K \cap \frac{1}{m}\mathbb{Z}^n\Big),$$

où $\mathscr{C}_{\frac{1}{m}}$ est un cube de côté $\dfrac{1}{m}$. Lorsque m tend vers $+\infty$, cette quantité est supérieure au volume de la réunion des cubes de côté $\dfrac{1}{m}$ et de sommets dans $\dfrac{1}{m}\mathbb{Z}^n$ qui sont contenus dans K, et inférieure au volume de la réunion de ces cubes dont un sommet est dans K. On en déduit facilement que la limite est le volume (n-dimensionnel) de K.

Montrons maintenant la seconde partie du théorème, dite formule de réciprocité. Lorsque P est un r-simplexe, on vérifie directement, de façon analogue à ci-dessus, la formule $\phi_{P'}(m) = (-1)^r\phi_P(-m)$. Si P n'est pas un simplexe, on l'écrit comme dans la démonstration du théorème 1 comme $Q \cup R$, où Q et R sont des polytopes avec strictement moins de points entiers que P qui se rencontrent le long d'une facette commune F. On a alors

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

En faisant une récurrence sur le nombre des points entiers du polytope, on obtient

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

Ceci termine la démonstration. □

6. Points entiers dans des convexes compacts assez symétriques

Compter des points entiers dans des polytopes est à l'origine une question liée à « l'approximation diophantienne » (on désigne par cette expression les techniques fines permettant entre autres d'approcher un nombre irrationnel par une suite de nombres rationnels). Cette théorie ancienne progressa beaucoup à la fin du dix-neuvième siècle grâce à Minkowski. Elle permet de montrer l'existence de points entiers dans des compacts convexes symétriques de volume assez grand et, plus généralement, de montrer l'existence de points entiers intérieurs dans des compacts convexes de volume assez grand, en fonction d'un coefficient de symétrie que nous définissons plus bas.

Comme on l'a déjà remarqué, un compact convexe de grand volume peut ne contenir aucun point entier. En revanche, un translaté convenable contiendra obligatoirement de nombreux tels points. C'est l'objet du résultat suivant, élémentaire mais crucial.

Théorème 5 (Blichfeldt, 1914)**.** *Soit K un compact de l'espace euclidien $\mathbb{R}^n$ et soit k un entier positif. Si $\mathrm{vol}(K) \geqslant k$, il existe des points distincts $v_0, \ldots, v_k$ de K tels que $v_i - v_j \in \mathbb{Z}^n$ pour tous i et j.*

Démonstration. Posons

$$\mathscr{C} = [0,1[^n \subset \mathbb{R}^n.$$

Lorsque u décrit $\mathbb{Z}^n$, les $u+\mathscr{C}$ forment une partition de $\mathbb{R}^n$. Si on pose $K_u = \{x \in \mathscr{C} \mid u+x \in K\}$, on a donc $\mathrm{vol}(K) = \sum_{u\in\mathbb{Z}^n} \mathrm{vol}(K_u)$. Supposons d'abord $\mathrm{vol}(K) > k$. On a [2]

$$k < \mathrm{vol}(K) = \sum_{u\in\mathbb{Z}^n} \int_{\mathbb{R}^n} 1_{K_u} d\mu = \int_{\mathscr{C}} \sum_{u\in\mathbb{Z}^n} 1_{K_u} d\mu.$$

Comme le volume de $\mathscr{C}$ est 1, il existe un point x de $\mathscr{C}$ vérifiant $\sum_{u\in\mathbb{Z}^n} 1_{K_u} > k$, c'est-à-dire appartenant à au moins $k+1$ ensembles K_u. Autrement dit, il existe $u_0, \ldots, u_k$ distincts dans $\mathbb{Z}^n$ tels que $v_j = x + u_j \in K$, d'où le résultat dans ce cas. Le cas $\mathrm{vol}(K) = k$ se traite en remplaçant K par λK, avec $\lambda > 1$. Il existe des points distincts $v_0(\lambda), \ldots, v_k(\lambda)$ de λK tels que $v_i(\lambda) - v_j(\lambda) \in \mathbb{Z}^n$ pour tous i et j. Comme K est compact, on peut supposer que les limites $v_i = \lim_{\lambda\to 1} \frac{1}{\lambda} v_i(\lambda)$ existent dans K et cela prouve le théorème.

□

Le résultat suivant semble dû à Minkowski pour $k = 1$ (1891), et à Blichfeldt en général.

Corollaire 1. *Soit K un compact convexe de l'espace euclidien $\mathbb{R}^n$, symétrique par rapport à 0, et soit k un entier positif. Si $\mathrm{vol}(K) \geqslant k2^n$, il existe k paires disjointes $\pm u_j$ de points non nuls appartenant à $K \cap \mathbb{Z}^n$.*

Pour tout réel x, notons $[x]_<$ le plus grand entier strictement inférieur à x. Le corollaire peut aussi s'exprimer ainsi : si K est un compact convexe symétrique par rapport à un point entier, on peut minorer de façon effective le nombre de points entiers intérieurs à K en fonction de son volume :

$$\mathrm{Card}(\overset{\circ}{K} \cap \mathbb{Z}^n) \geqslant 2\Big[\frac{\mathrm{vol}(K)}{2^n}\Big]_< + 1$$

(si $k = \Big[\frac{\mathrm{vol}(K)}{2^n}\Big]_<$, il suffit d'appliquer l'énoncé à λK, où $\lambda \in]0,1[$ est tel que $\mathrm{vol}(\lambda K) \geqslant k2^n$).

Démonstration. Appliquons le théorème de Blichfeldt à $\frac{1}{2}K$, compact de volume $> k$: il existe des points distincts $v_0, \ldots, v_k$ de K tels que $\frac{1}{2}v_i - \frac{1}{2}v_j \in \mathbb{Z}^n$. Quitte à réordonner les v_i et à changer les coordonnées, on peut supposer que la première coordonnée de v_0 est strictement inférieure à celle de chacun des autres v_i. Pour $i \in \{1, \ldots, k\}$, les $u_i = \frac{1}{2}\big(v_i + (-v_0)\big)$ sont dans $K \cap \mathbb{Z}^n$. Ils sont distincts, et si $u_i = -u_j$, on a $v_i + v_j = 2v_0$, ce qui est impossible puisque les premières coordonnées sont différentes.

---

2. Si A est une partie de $\mathbb{R}^n$, on note 1_A la *fonction caractéristique* de A, c'est-à-dire la fonction $\mathbb{R}^n \to \mathbb{R}$ définie par $1_A(x) = 1$ si $x \in A$, et $1_A(x) = 0$ sinon.

□

Nous allons étendre le résultat de Minkowski à des convexes quelconques. Pour cela, il sera pratique d'introduire la notion suivante. Soit K un convexe compact de l'espace euclidien $\mathbb{R}^n$ 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. On définit le *coefficient de symétrie* de K par rapport à x par

$$a(K,x) = \min_\ell \frac{\|x - x_\ell^+\|}{\|x - x_\ell^-\|}.$$

On a $0 < a(K,x) \leqslant 1$ et $a(K,x) = 1$ si et seulement si K est symétrique par rapport à x. Plus x est près du bord, plus $a(K,x)$ est petit. On a aussi

$$a(K,0) = \max\{a > 0 \mid -aK \subset K\}.$$

En particulier, si P est un polytope de sommets $s_1, \dots, s_r$,

$$a(P,0) = \min\{a > 0 \mid -as_i \in P \text{ pour tout } i\}.$$

Revenant au cas général d'un point intérieur x quelconque, si, pour chaque $i \in \{1, \dots, r\}$, on note y_i l'autre point d'intersection de la droite $s_i x$ avec le bord de P, on a

$$a(P,x) = \min_{1 \leqslant i \leqslant r} \frac{\|x - y_i\|}{\|x - s_i\|}. \tag{3}$$

On obtient facilement la généralisation suivante du corollaire 1.

Corollaire 2. *Soit K un compact convexe de l'espace euclidien $\mathbb{R}^n$ contenant au moins un point entier intérieur x. On a*

$$\mathrm{Card}(\overset{\circ}{K} \cap \mathbb{Z}^n) \geqslant 2\Big[\,\mathrm{vol}(K)\Big(\frac{a(K,x)}{a(K,x)+1}\Big)^n\Big]_< + 1.$$

On utilisera ce corollaire sous la forme plus faible

$$\mathrm{Card}(\overset{\circ}{K} \cap \mathbb{Z}^n) \geqslant \mathrm{vol}(K)\Big(\frac{a(K,x)}{2}\Big)^n.$$

Démonstration. La démonstration est exactement semblable à celle du corollaire 1. On peut supposer $x = 0$. Posons $a = a(K,0)$ et $k = \Big[\,\mathrm{vol}(K)\Big(\frac{a(K,x)}{a(K,x)+1}\Big)^n\Big]_<$. Pour $\lambda \in]0,1[$ suffisamment proche de 1, le convexe compact $K_\lambda = \dfrac{\lambda}{\frac{1}{a}+1} K$ est de volume $> k$. Le théorème 5 fournit alors $2k+1$ points distincts $v_0, \dots, v_k$ de K_λ tels que $v_i - v_j \in \mathbb{Z}^n$ pour tous i et j. Comme $-aK_\lambda \subset K_\lambda$ et que K_λ est convexe, les points

$$\frac{v_i - v_j}{\frac{1}{a}+1} = \frac{\frac{1}{a}(-av_j) + v_i}{\frac{1}{a}+1}$$

sont dans K_λ, donc les points entiers $0, \pm(v_1 - v_0), \ldots, \pm(v_k - v_0)$ sont dans $(\frac{1}{a} + 1)K_\lambda$, qui est contenu dans $\overset{\circ}{K}$. Si on choisit v_0 comme dans la démonstration du corollaire 1, on obtient ainsi $2k + 1$ points distincts, ce qui montre le corollaire.

□

7. Énoncé du théorème de Hensley sur les points entiers dans les polytopes entiers

Dans ce paragraphe, nous souhaitons estimer le nombre de points entiers sur le bord d'un polytope entier en fonction du nombre de points entiers à l'intérieur, généralisant ainsi en toute dimension le résultat de Scott (th. 3).

Théorème 6 (Hensley, 1983)**.** *Il existe une constante $B(k, n)$ ne dépendant que des entiers strictement positifs k et n, telle que, pour tout polytope entier P de dimension n avec exactement k points entiers intérieurs, on ait* $\mathrm{vol}(P) \leqslant B(k, n)$.

On en déduit immédiatement le résultat suivant à l'aide de l'inégalité de Blichfeldt.

Corollaire 3. *Soit P un polytope entier de dimension n avec exactement k ¿ 0 points entiers intérieurs. On a*

$$\mathrm{Card}(P \cap \mathbb{Z}^n) \leqslant n + n!B(k, n).$$

Autrement dit, le nombre de points entiers sur le bord d'un polytope entier de dimension n est contrôlé par le nombre de points entiers à l'intérieur de ce polytope... s'il y en a ! Une constante $B(k, n)$ est explicitement calculée par Hensley dans [H]. Elle est améliorée dans [LZ]] par Lagarias et Ziegler en $B(k, n) = k(7(k + 1))^{n2^{2^{n+1}}}$, qui n'est pas loin d'être optimal : il y a des exemples de polytopes entiers P de dimension n avec un unique point intérieur et

$$\mathrm{vol}(P) \geqslant \frac{1}{n!}2^{2^{n-1}} \quad , \quad \mathrm{Card}(P \cap \mathbb{Z}^n) \geqslant 2^{2^{n-2}}$$

(voir [ZPW] et [LZ]).

8. Le théorème de Hensley pour les simplexes

On commence par montrer que les points entiers intérieurs d'un simplexe entier ne peuvent pas être trop près du bord. En d'autres termes, le coefficient de symétrie d'un simplexe entier par rapport à un point entier intérieur n'est pas trop petit.

Proposition 5. *Pour tous entiers strictement positifs n et k, il existe une constante strictement positive $\varepsilon(k, n)$ telle que, pour tout n-simplexe entier S avec exactement k points intérieurs, et tout point entier intérieur x de S, on ait*

$$a(S, x) \geqslant \varepsilon(k, n).$$

La constante $\varepsilon(k,n)$ est explicite. La valeur obtenue par Hensley (dont nous suivons la démonstration plus bas) est de l'ordre de $(4k)^{-2n!}$. C'est cette proposition que Lagarias & Ziegler améliorent, obtenant $\varepsilon(k,n) \geqslant (7k+7)^{-2^{n+1}}$. Il existe des exemples où $\varepsilon(1,n)$ est de l'ordre de 2^{-2^n}. Le théorème de Hensley pour les simplexes se déduit immédiatement de la proposition grâce au corollaire 2.

Corollaire 4. *Pour tous entiers strictement positifs n et k, et tout n-simplexe entier S avec exactement k points intérieurs, on a*

$$\mathrm{vol}(S) \leqslant k\Big(\frac{2}{\varepsilon(k,n)}\Big)^n.$$

Démonstration de la proposition 5. Celle-ci nécessite plusieurs lemmes d'approximation. Le premier est classique.

Lemme 1 (Hermite, 1847)**.** *Soit $(x_1,\dots,x_n) \in \mathbb{R}^n$ et soit N un entier strictement positif fixé. Il existe des entiers $p_1,\dots,p_n,q$ avec $1 \leqslant q \leqslant N^n$ tels que $\big|x_i - \frac{p_i}{q}\big| \leqslant \frac{1}{Nq}$ pour chaque $i \in \{1,\dots,n\}$.*

Démonstration. Pour tout réel x, on note $\{x\} = x - [x]$ la partie fractionnaire de x. Au moins deux des N^n+1 vecteurs $(\{kx_1\},\dots,\{kx_n\})$ de $[0,1]^n$, lorsque k décrit $\{0,\dots,N^n\}$, 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 correspondantes, et posons $q = k_2 - k_1$. On a $0 < q \leqslant k_2 \leqslant N^n$. Soit p_i l'entier le plus proche de qx_i. On a

$$|qx_i - p_i| \leqslant |k_2x_i - k_1x_i - [k_2x_i] + [k_1x_i]| = |\{k_2x_i\} - \{k_1x_i\}| \leqslant \frac{1}{N},$$

d'où le lemme.

□

Le lemme suivant n'est qu'une petite adaptation.

Lemme 2. *Soit $(x_1,\dots,x_n) \in (\mathbb{R}^{+*})^n$, avec $\sum_{i=1}^n x_i = 1$, et soit $N \geqslant n$ un entier. Il existe des entiers $p_1,\dots,p_n,q$, avec $p_i \geqslant 0$, $q = \sum_{i=1}^n p_i$ et $1 \leqslant q \leqslant N^{n-1}$, tels que $|qx_1 - p_1| \leqslant \frac{n}{N}$, et $|qx_i - p_i| \leqslant \frac{1}{N}$ pour chaque $i \in \{2,\dots,n\}$.*

Démonstration. On applique le lemme 1 à $(x_2,\dots,x_n)$. Pour $i \in \{2,\dots,n\}$, on a $|qx_i - p_i| \leqslant \frac{1}{N}$ et $qx_i > 0$, donc en particulier $p_i \geqslant 0$. Posons $p_1 = q - \sum_{i=1}^{n-1} p_i$. On a

$$|qx_1 - p_1| = \Big|q - q\sum_{i=1}^{n-1} x_i + \sum_{i=1}^{n-1} p_i - q\Big| \leqslant \frac{n}{N}.$$

De nouveau, comme $qx_1 > 0$ et $\dfrac{n}{N} \leqslant 1$, on a $p_1 \geqslant 0$.

□

Voici maintenant le point essentiel.

Lemme 3. *Pour tous entiers strictement positifs n et k, il existe $\alpha(k,n) > 0$ tel que, pour tout $(x_1,\dots,x_n) \in (\mathbb{R}^{+*})^n$ tel que $1 > \sum_{i=1}^{n} x_i > 1-\alpha(k,n)$, il existe des entiers $p_1,\dots,p_n,q$, avec $p_i \geqslant 0$ et $q = \sum_{i=1}^{n} p_i > 0$, vérifiant $(kq+1)x_i > kp_i$ pour chaque $i \in \{1,\dots,n\}$.*

Avant de démontrer ce lemme, montrons comment il entraîne la proposition 5. Rappelons que nous avons affaire à un n-simplexe entier S (dont on peut supposer que les sommets sont $0, s_1,\dots,s_n$) contenant un point entier intérieur $x = \sum_{i=1}^{n} x_i s_i$, avec $x_i > 0$ et $\sum_{i=1}^{n} x_i < 1$. Montrons $\sum_{i=1}^{n} x_i \leqslant 1-\alpha(k,n)$. Si ce n'est pas le cas, on applique le lemme 3 et on considère pour chaque entier $j \geqslant 0$ le point entier

$$(jq+1)x - j\sum_{i=1}^{n} p_i s_i = \sum_{i=1}^{n}\big((jq+1)x_i - jp_i\big)s_i.$$

On a $\sum_{i=1}^{n}\big((jq+1)x_i - jp_i\big) < jq+1-jq = 1$. De plus, si $qx_i - p_i \geqslant 0$, on a $(jq+1)x_i - jp_i \geqslant x_i > 0$. Si $qx_i - p_i < 0$ et $j \leqslant k$, on a $(jq+1)x_i - jp_i \geqslant x_i + k(qx_i - p_i) > 0$. On obtient donc ainsi $k+1$ points entiers intérieurs à S, ce qui est absurde.

On a donc $\sum_{i=1}^{n} x_i \leqslant 1-\alpha(k,n)$. Si y est l'autre point d'intersection de la droite $0x$ avec S, cela signifie $\|x\| \leqslant \big(1-\alpha(k,n)\big)\|y\|$. Comme cela reste valable en remplaçant 0 par n'importe quel autre sommet de S, on déduit de la formule (3) l'estimation

$$a(S,x) \geqslant \frac{\alpha(k,n)}{1-\alpha(k,n)}.$$

Ceci termine donc la démonstration de la proposition 5.

□

Démonstration du lemme 3. On procède par récurrence sur n. Si $n=1$, on cherche un entier $q>0$ tel que $x > \dfrac{kq}{kq+1}$. C'est possible dès que $x > \dfrac{1}{k+1} = \alpha(k,1)$. Posons

$$\begin{aligned} N &= 1 + \max\Big\{\Big[\frac{4k}{\alpha(k,n-1)}\Big], 2kn(n+1)\Big\}, \\ \alpha(k,n) &= \frac{1}{4kN^{n-1}} \leqslant \frac{1}{2}\alpha(k,n-1). \end{aligned}$$

Prenons $x_1 \geqslant \cdots \geqslant x_n > 0$, posons $\sum_{i=1}^{n} x_i = 1 - \alpha$, et supposons $0 < \alpha < \alpha(k,n)$.

Si $x_n < \alpha(k,n-1) - \alpha$, on a $\sum_{i=1}^{n-1} x_i = 1 - \alpha - x_n > 1 - \alpha(k,n-1)$. On peut appliquer l'hypothèse de récurrence et prendre $p_1, \ldots, p_{n-1}, 0$ et q.

Supposons donc $x_n \geqslant \alpha(k,n-1) - \alpha$ et appliquons le lemme 2 à $\dfrac{x_i}{1-\alpha}$. On a

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

car $x_1 \geqslant \dfrac{1-\alpha}{n} \geqslant \dfrac{1}{n+1}$. Pour $i \geqslant 2$, on a de même

$$\begin{aligned}
(kq+1)x_i - kp_i &\geqslant \frac{1}{2}x_n - \frac{k}{N} \\
&\geqslant \frac{1}{2}\big(\alpha(k,n-1) - \alpha\big) - \frac{k}{N} \\
&\geqslant \frac{1}{4}\alpha(k,n-1) - \frac{k}{N} \;>\; 0,
\end{aligned}$$

et le lemme est démontré.

□

9. Le cas général du théorème de Hensley

On a déjà fait la partie la plus difficile : il est facile de déduire le cas général 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

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

Par le théorème de Carathéodory, il existe des sommets $s_1, \ldots, s_r$ de F (donc de P) affinement indépendants (donc avec $r \leqslant n$), tels que y se trouve dans l'intérieur relatif du $(r-1)$-simplexe qu'ils engendrent. Soit S le r-simplexe de sommets $s, s_1, \ldots, s_r$. Son intérieur relatif est contenu dans $\overset{\circ}{P}$ et contient exactement $k' \leqslant k$ points entiers, dont x. La proposition 5 entraîne

$$a(P,x) \geqslant a(S,x) \geqslant \varepsilon(k',r)$$

d'où, en utilisant le corollaire 2,

$$\mathrm{vol}(P) \leqslant k\Big(\frac{2}{\min_{1\leqslant k'\leqslant k,\ 1\leqslant r\leqslant n} \varepsilon(k',r)}\Big)^n,$$

ce qui montre le théorème 6.

10. Un résultat de finitude

Théorème 7 (Lagarias & Ziegler, 1991)**.** *Pour tous entiers strictement positifs k et n, il n'y a qu'un nombre fini de classes d'équivalence de polytopes entiers de dimension n avec exactement k points entiers intérieurs.*

Démonstration. Montrons d'abord que *tout simplexe entier S est équivalent à un simplexe contenu dans un parallélépipède « rectangle » de volume inférieur ou égal à $n!\,\mathrm{vol}(S)$*. Par translation entière, on peut supposer que l'origine est un sommet de S. Soient $s_1, \ldots, s_n$ les autres sommets et soit $M = (m_{ij})_{1\leqslant i,j\leqslant n}$ la matrice (entière) de leurs composantes dans la base canonique $(e_1, \ldots, e_n)$. Nous allons démontrer deux lemmes sur les matrices entières.

Pour $1 \leqslant i < j \leqslant n$, notons E_{ij} la matrice carrée d'ordre n dont tous les coefficients sont nuls, sauf celui de la i-ième ligne et j-ième colonne, qui vaut 1. Multiplier une matrice carrée d'ordre n à droite (resp. à gauche) par $I + mE_{ij}$ (élément de $\mathrm{GL}_n(\mathbb{Z})$) revient à ajouter à la j-ième colonne (resp. ligne) m fois la i-ième colonne (resp. ligne). On peut aussi changer le signe d'une colonne en multipliant à droite par un élément de $\mathrm{GL}_n(\mathbb{Z})$.

Lemme 4. *Étant donnés des entiers $a_1, \ldots, a_n$ premiers entre eux (dans leur ensemble), il existe une matrice de $\mathrm{GL}_n(\mathbb{Z})$ dont la première colonne est $a_1, \ldots, a_n$.*

Démonstration. On peut supposer tous les a_i positifs et on procède par récurrence sur leur somme. Si celle-ci vaut 1, c'est évident. Si elle est > 1, au moins deux des a_i sont non nuls, et on peut supposer par exemple $a_1 \geqslant a_2 > 0$. Il existe alors par hypothèse de récurrence une matrice $A \in \mathrm{GL}_n(\mathbb{Z})$ dont la première colonne est $a_1 - a_2, a_2, \ldots, a_n$. La matrice $(I_n + E_{12})A$ convient alors.

Lemme 5. *Étant donnée une matrice entière M à déterminant non nul, il existe $A \in \mathrm{GL}_n(\mathbb{Z})$ tel que*

$$MA = \begin{pmatrix} c_{11} & c_{12} & \cdots & \cdots & c_{1n} \\ 0 & c_{22} & \cdots & \cdots & c_{2n} \\ \vdots & 0 & \ddots & & \vdots \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 & c_{nn} \end{pmatrix},$$

avec $0 \leqslant c_{ij} < c_{ii}$ pour tous entiers i et j tels que $1 \leqslant i < j \leqslant n$.

Démonstration. Soient $s'_1, \ldots, s'_n$ les vecteurs colonnes (entiers) de la matrice obtenue à partir de M en supprimant sa première ligne. Ces n vecteurs sont liés dans $\mathbb{Q}^{n-1}$: il existe donc des rationnels $a_1, \ldots, a_n$ non tous nuls vérifiant $a_1 s'_1 + \cdots + a_n s'_n = 0$. En chassant les dénominateurs, on peut supposer les a_j entiers premiers entre eux. On applique le lemme précédent, qui fournit une matrice $A \in \mathrm{GL}_n(\mathbb{Z})$ de première colonne $a_1, \ldots, a_n$. La matrice MA est alors du type

$$\begin{pmatrix} c_{11} & c_{12} & \cdots & c_{1n} \\ 0 & c_{22} & \cdots & c_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & c_{n2} & \cdots & c_{nn} \end{pmatrix}.$$

On peut supposer $c_{11} > 0$ et, en faisant une récurrence sur n, que cette matrice est triangulaire supérieure avec $0 \leqslant c_{ij} < c_{ii}$ pour $2 \leqslant i < j \leqslant n$. Si on effectue la division euclidienne $c_{1j} = q_j c_{11} + r_j$, avec $0 \leqslant r_j < c_{11}$, on obtient, après avoir retiré à la j-ième colonne q_j fois la première, $0 \leqslant c_{1j} < c_{11}$, ce qui termine la démonstration du lemme.

Revenons à la démonstration du théorème. On a $s_j = \sum_i m_{ij} e_i$, d'où

$$A(s_j) = \sum_i m_{ij} A(e_i) = \sum_i m_{ij} \sum_k a_{ki} e_k = \sum_k c_{kj} e_k.$$

Les colonnes de la matrice MA sont donc, avec l'origine, les sommets du simplexe $A(S)$. La i-ième composante d'un élément de $A(S)$ s'écrit alors

$$\sum_j l_j c_{ij},$$

avec $l_j \geqslant 0$ et $\sum_j l_j \leqslant 1$. Celle-ci est inférieure à $\sum_j l_j c_{ii}$, donc à c_{ii}. Cela signifie que le simplexe $A(S)$ est contenu dans un parallélépipède de sommet l'origine et de côtés parallèles aux axes, de longueurs $c_{11}, \ldots, c_{nn}$, donc de volume

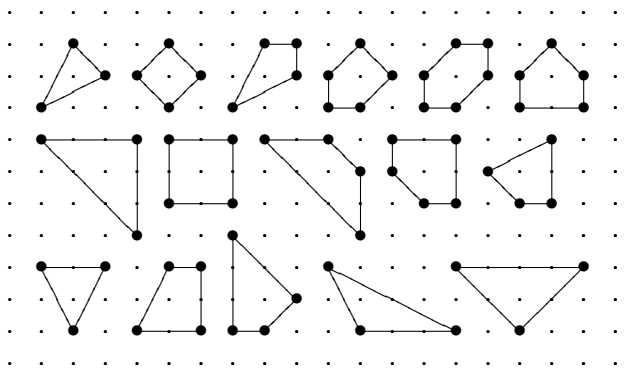
$$c_{11} \cdots c_{nn} = \det(AM) = |\det(M)| = n! \operatorname{vol}(S),$$

ce qui montre ce que l'on voulait.

Pour traiter le cas général, on considère un simplexe S de volume maximal contenu dans notre polytope entier P. Comme on l'a vu au paragraphe 2, on peut choisir S de façon que ses sommets soient des sommets de P, donc entiers. Il existe une transformation $A \in \mathrm{GL}_n(\mathbb{Z})$ telle que $A(S)$ soit contenu dans un parallélépipède de volume $\leqslant n!\,\mathrm{vol}(S)$ à côtés parallèles aux axes. La proposition 3 entraîne que $A(P)$ est contenu dans un cube de côté $\leqslant nn!\,\mathrm{vol}(S) \leqslant nn!\,\mathrm{vol}(P) \leqslant nn!B(k,n)$ à côtés parallèles aux axes. Un tel cube ne contient qu'un nombre fini de points entiers, donc qu'un nombre fini de polytopes entiers.

□

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



(4)

Il n'y a actuellement pas de classification en dimension supérieure ou égale à 3 (il faut s'attendre à une liste très longue !).

11. Les polytopes de Fano

Nous nous intéressons maintenant à une classe de polytopes entiers très simples, qui présente un grand intérêt en gémétrie algébrique.

Définition 2. *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 $\mathbb{Z}^n$.*

Nous laissons au lecteur le soin de déterminer les 5 types de polygones de Fano parmi les 16 types de polygones entiers de la liste (4) ci-dessus.

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. Il résulte des résultats de finitude précédents qu'il n'y a qu'un nombre fini de classes d'équivalence de polytopes de Fano de dimension n ; en particulier, le nombre de sommets d'un tel polytope est majoré par une constante ne dépendant que de n.

En utilisant des résultats de classification, on montre qu'un polytope de Fano de dimension 1, 2, 3 ou 4 possède au plus 2, 6, 8 ou 12 sommets respectivement. Ces nombres ont inspiré une conjecture d'Ewald récemment démontrée par C. Casagrande.

Théorème 8 (Casagrande, 2004)**.** *Le nombre de sommets d'un polytope de Fano P de dimension n est plus $3n$. Il y a égalité si et seulement si n est pair et que P est équivalent au produit de $n/2$ copies du polytope de Fano plan à 6 sommets* [3].

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 (voir ci-dessous) est aussi entier.

Démonstration. Introduisons le polytope dual de P, défini par

$$P^* = \{y \in \mathbb{R}^n \mid \langle x, y\rangle \leqslant 1 \text{ pour tout } x \in P\},$$

où $\langle \cdot, \cdot \rangle$ est le produit scalaire usuel sur $\mathbb{R}^n$ (cette définition a un sens pour tout polytope, de Fano ou pas) [4]. On montre que c'est bien un polytope et que ses sommets sont en bijection avec les facettes de P par la correspondance

$$s^* \text{ sommet de } P^* \leftrightarrow F_{s^*} = \{x \in \mathbb{R}^n \mid \langle x, s^*\rangle = 1\}.$$

Si P est un polytope de Fano, P^* est encore un polytope entier, pas nécessairement de Fano, mais qui n'a qu'un seul point entier intérieur (l'origine) [5].

Soit s^* un sommet de P^*. Comme les facettes de P contiennent n sommets, il y a exactement n sommets s de P qui vérifient $\langle s, s^*\rangle = 1$.

Si s est un sommet de P qui vérifie $\langle s, s^*\rangle = 0$, on vérifie facilement que s forme avec $n-1$ des sommets de F_{s^*} une facette de P (*adjacente* à F_{s^*}). On a donc au plus n de ces sommets.

On peut maintenant commencer la démonstration. Comme l'origine est intérieure à P^*, on a une relation

$$0 = m_1 s_1^* + \cdots + m_r s_r^*,$$

où les m_i sont des entiers strictement positifs et $s_1^*, \ldots, s_r^*$ des sommets de P^*. Pour tout sommet s de P, on a

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

3. Le cinquième de la première ligne du tableau (4).

4. On peut aussi se placer dans l'espace vectoriel dual $(\mathbb{R}^n)^*$ et remplacer le produit scalaire par la dualité, d'où la terminologie.

5. Nous laissons au lecteur le soin de déterminer les duaux des 5 types de polygones de Fano parmi les 16 types de polygones entiers de la liste (4) ci-dessus.

de sorte que

$$\sum_{i=1}^{r} m_i \leqslant 2 \sum_{\langle s, s_i^* \rangle = 1} m_i + \sum_{\langle s, s_i^* \rangle = 0} m_i.$$

En sommant sur tous les sommets s et en notant σ le nombre de sommets de P, on obtient

$$\begin{aligned} \sigma \sum_{i=1}^{r} m_i &\leqslant 2 \sum_{s} \sum_{\langle s, s_i^* \rangle = 1} m_i + \sum_{s} \sum_{\langle s, s_i^* \rangle = 0} m_i \\ &= \sum_{i=1}^{r} m_i \operatorname{Card}\{s \mid \langle s, s_i^* \rangle = 1\} + \sum_{i=1}^{r} m_i \operatorname{Card}\{s \mid \langle s, s_i^* \rangle = 0\} \\ &\leqslant 3n \sum_{i=1}^{r} m_i, \end{aligned}$$

d'où le théorème. Pour le cas d'égalité, on renvoie le lecteur à [C].

□

Références

[B] Blichfeldt, H., A new principle in the geometry of numbers, with some applications, *Trans. Amer. Math. Soc.* **15** (1914), 227–235.

[Bo] Bonavero, L., Sur le nombre de sommets des polytopes entiers, Images des Mathématiques, 33–40, C.N.R.S., 2004.

[Br] Brion, M., Points entiers dans les polytopes convexes, Séminaire Bourbaki, Vol. 1993/94, Exp. No. 780, *Astérisque* **227** (1995), 145–169.

[C] Casagrande, C., The number of vertices of a Fano polytope, *Ann. Inst. Fourier* **56** (2006), 121–130.

[E] Ehrhart, E., Démonstration de la loi de réciprocité pour un polyèdre entier, *C. R. Acad. Sci. Paris* **265** (1967), 5–7.

[Ew] Ewald, G., *Combinatorial convexity and algebraic geometry*, Graduate texts in mathematics **168**, Springer-Verlag, 1996.

[F] Fulton, W., *Introduction to toric varieties*, Annals of mathematics studies **131**, Princeton University Press, 1993.

[H] Hensley, D., Lattice vertex polytopes with interior lattice points, *Pacific J. Math.* **105** (1983), 183–191.

[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.

[M] Minkowski, H., *Geometrie der Zahlen. I,* réédition, Chelsea Co., New York, 1953.

[P] Pick, G., Geometrisches zur Zahlenlehre, *Sitzungsber. Lotos Prag (2)* **19** (1900), 311–319.

[S] Scott, P. R., On convex lattice polygons, *Bull. Austral. Math. Soc.* **15** (1976), 395–399.

[ZPW] Zaks, J., Perles, M., Wilks, J., On lattice polytopes having interior lattice points, *Elem. Math.* **37** (1982), 44–46.