BULLETIN DE LA S. M. F.

BERND BANK
JOOS HEINTZ
TERESA KRICK
REINHARD MANDEL
PABLO SOLERNÓ

Une borne optimale pour la programmation entière quasi-convexe

Bulletin de la S. M. F., tome 121, n° 2 (1993), p. 299-314
<http://www.numdam.org/item?id=BSMF_1993__121_2_299_0>

Bull. Soc. math. France,
121, 1993, p. 299–314.

UNE BORNE OPTIMALE POUR LA PROGRAMMATION ENTIÈRE QUASI-CONVEXE

PAR

BERND BANK [1], JOOS HEINTZ [2],

TERESA KRICK [2], REINHARD MANDEL [1],

PABLO SOLERNÓ [2]

RÉSUMÉ. — Soient $F_1, \ldots, F_s \in \mathbb{Z}[X_1, \ldots, X_N]$ des polynômes quasiconvexes de degré majoré par $d \geq 2$, et ℓ une borne pour la longueur binaire de leurs coefficients. On montre que si le système $F_1 \leq 0, \ldots, F_s \leq 0$ admet une solution entière, alors il existe une telle solution à longueur binaire majorée par $(sd)^{cn}\ell$ (où c est une constante, indépendante de s, d, n et ℓ). Le caractère simplement exponentiel de cette borne est intrinsèque au problème. On obtient aussi une borne similaire pour le problème de minimisation correspondant.

ABSTRACT. — Let $F_1, \ldots, F_s \in \mathbb{Z}[X_1, \ldots, X_n]$ be quasiconvex polynomials of degrees bounded by $d \geq 2$ and assume that the maximum binary length of the coefficients of these polynomials doesn't exceed a given natural number ℓ. We show that the system of polynomial inequalities $F_1 \leq 0, \ldots, F_s \leq 0$ admits an integer solution if and only if such a solution with binary length bounded by $(sd)^{cn}\ell$ exists. (Here c is a constant, independent on s, d, n and ℓ). The simply exponential nature of this bound is intrinsical to this problem. We obtain a similar geometrical bound for the corresponding minimisation problem.

Introduction et Notations

En 1983, L.G. KHACHIYAN et S.P. TARASOV (cf. [13], [6]) ont annoncé que si $F_1, \ldots, F_s$ sont des polynômes convexes en n indéterminées, de degré $d \geq 2$ et à coefficients entiers, tous de longueur binaire majorée par ℓ, alors le système d'inégalités polynomiales $F_1 \leq 0, \ldots, F_s \leq 0$ admet

Texte reçu le 13 avril 1992.
(1) Humboldt Universität, Sektion Mathematik, PSF 1297, 1086 Berlin.
(2) Working Group Noaï Fitchas, Univ. de Buenos Aires, Fac. de Ciencias Exactas, Departamento de Matemática, Ciudad Universitaria, 1428 Buenos Aires, Argentina.
Classification AMS : 90C10, 65K05.

BULLETIN DE LA SOCIÉTÉ MATHÉMATIQUE DE FRANCE 0037-9484/1993/299/$ 5.00

une solution *entière* si et seulement si il admet une solution entière contenue dans une boule centrée à l'origine et de rayon entier R, de longueur binaire majorée par $d^{c(\widetilde{n}+d)}n^{cd}\ell$ (où $\widetilde{n} := \min\{s, n\}$ et c est une constante indépendante des paramètres considérés). L'intérêt de cette question est qu'elle représente une solution effective pour le problème de stabilité correspondant au problème d'optimisation (de minimisation) pour la programmation entière à contraintes polynomiales convexes, généralisation naturelle du problème de la programmation linéaire entière.

Dans ce travail, nous nous intéressons en premier lieu à ce même problème de calcul d'une borne géométrique pour le cas des polynômes quasiconvexes.

Pour préciser les résultats, fixons tout d'abord les notations : dans ce qui suit, $\mathbb{R}$ représentera le corps des nombres réels et $\mathbb{Z}$ l'anneau des entiers. Soient $X_1, \ldots, X_n$ des indéterminées sur $\mathbb{R}$. On dit qu'un polynôme $F \in \mathbb{R}[X_1, \ldots, X_n]$ est *quasiconvexe* si pour tout $t \in \mathbb{R}$, l'ensemble de niveau $\{x \in \mathbb{R}^n : F(x) \leq t\}$ est un sous-ensemble convexe de $\mathbb{R}^n$. Pour un ensemble fini $V \subseteq \mathbb{Z}^n$ de vecteurs à coordonnées entières, nous noterons par $\ell(V)$ la longueur binaire maximale des coordonnées de tout vecteur de V. De même, si $\mathcal{F} \subseteq \mathbb{Z}[X_1, \ldots, X_n]$ est un ensemble fini de polynômes à coefficients entiers, $\ell(\mathcal{F})$ notera la longueur binaire maximale des coefficients des polynomes de $\mathcal{F}$.

La boule fermée de rayon $R \in \mathbb{R}_{\geq 0}$ et centrée à l'origine sera indiquée par $B(0, R)$. Nous adopterons aussi la notation standard $\mathrm{O}(n)$, $n \in \mathbb{N}$, pour désigner une fonction linéaire en n, c'est-à-dire, il existe une constante c, indépendante de n, telle que $\mathrm{O}(n) \leq cn$.

Passons maintenant à l'énoncé des résultats :

THÉORÈME 1. — *Soient $F_1, \ldots, F_s \in \mathbb{Z}[X_1, \ldots, X_n]$ des polynômes quasiconvexes à coefficients entiers, de degré majoré par $d \geq 2$ et tels que $\ell := \ell(\{F_1, \ldots, F_s\})$. Il existe un rayon $R \in \mathbb{N}$, de longueur binaire $\ell(R) = (sd)^{\mathrm{O}(n)}\ell$ tel que si l'ensemble $\{x \in \mathbb{Z}^n : F_1(x) \leq 0, \ldots, F_s(x) \leq 0\}$ est non vide, alors il contient un point (entier) dans la boule $B(0, R)$. Ce rayon R ne dépend pas du caractère particulier des polynômes $F_1, \ldots, F_s$ mais seulement des paramètres s, d, n, ℓ considérés.*

Étant donné que les polynômes convexes constituent un cas particulier des polynômes quasiconvexes, ce résultat généralise et améliore la borne annoncée par Khachiyan et Tarasov.

D'autre part, le caractère exponentiel de la borne obtenue est intrinsèque au problème, comme le prouve l'exemple suivant étudié dans [13] : les auteurs considèrent les polynômes quadratiques et convexes

$$F_1 = -X_1 + 2^\ell, F_2 = X_1^2 - X_2, \ldots, F_n = X_{n-1}^2 - X_n$$

et montrent que toutes les solutions du système $F_1(x) \leq 0, \ldots, F_n(x) \leq 0$ se trouvent en dehors de la boule $B(0,R)$, où $\ell(R) = 2^{n-1}\ell$. Ceci signifie que la borne du THÉORÈME 1 est optimale en fonction des paramètres considérés, en tant que mesure générale de complexité.

Ce théorème géométrique entraîne aussi le résultat algorithmique :

COROLLAIRE. — *On peut décider à l'aide d'une machine de Turing non déterministe si l'ensemble*

$$\{x \in \mathbb{Z}^n : F_1(x) \leq 0, \ldots, F_s(x) \leq 0\}$$

est non vide en temps $(sd)^{0(n)}\ell$. *En d'autres mots, le problème de la programmation entière à contraintes polynomiales quasiconvexes appartient à la classe de complexité* NEXPTIME (« *non deterministically simply exponential time* »). *Ceci signifie qu'on peut vérifier si un candidat à solution du système considéré est effectivement une solution en temps simplement exponentiel.*

Finalement, les méthodes appliquées pour montrer le THÉORÈME 1 entraînent aussi le résultat d'optimisation entière à contraintes polynomiales quasiconvexes correspondant :

THÉORÈME 2. — *Soient* $F, F_1, \ldots, F_s \in \mathbb{Z}[X_1, \ldots, X_n]$ *des polynômes quasiconvexes à coefficients entiers, de degré majoré par* $d \geq 2$ *tels que* $\ell := \ell(\{F, F_1, \ldots, F_s\})$ *et posons*

$$M := \{x \in \mathbb{R}^n : F_1(x) \leq 0, \ldots, F_s(x) \leq 0\}.$$

Si l'ensemble $M \cap \mathbb{Z}^n$ *est non vide et*

$$\inf\{F(x) : x \in M \cap \mathbb{Z}^n\} = m > -\infty$$

(*où* inf *note l'infimum*), *alors il existe un rayon* $R \in \mathbb{N}$, *de longueur binaire* $\ell(R) = (sd)^{0(n)}\ell$ *tel que*

$$m = \inf\{F(x) : x \in M \cap \mathbb{Z}^n \cap B(0,R)\}.$$

Preuves des résultats

Preuve du Théorème 1. — Ce théorème est une conséquence des nouveaux résultats en géométrie semi-algébrique algorithmique (élimination « rapide » des quantificateurs dans la théorie élémentaire des corps réels clos) qu'on trouve dans [12], [3], [4], [5] et [9], appliqués au problème

grâce à des techniques de réduction pour la programmation quasiconvexe développées dans [1, chapitres 4 et 5], et simplifiées dans [2]. Nous considérerons ici plus en détail les méthodes nouvelles particulières à notre problème, nous remettant aux travaux cités ci-dessus pour les démonstrations des résultats préliminaires qui y figurent. Une borne légèrement moins précise, avec les preuves complètes est aussi présentée dans [7].

Dans le but de fournir la démonstration la plus claire possible, nous la diviserons en différentes sections.

1. Propriétés fondamentales des polynômes quasiconvexes. — Nous décrivons ici quelques propriétés théoriques qui sont indispensables pour l'obtention de la borne annoncée.

Propriété « d'uniformité ». — *Soit* $F \in \mathbb{R}[X_1, \ldots, X_n]$ *un polynôme quasiconvexe. Soient* $x, u \in \mathbb{R}^n$, $u \neq 0$, *fixés. Si le polynôme* $F(x+Tu)$, *en l'indéterminée* T, *est strictement décroissant (respectivement constant) alors, pour tout* $y \in \mathbb{R}$, *le polynôme* $F(y+Tu)$ *est strictement décroissant (respectivement constant).*

Preuve. — Nous utiliserons la définition équivalente de polynôme quasiconvexe suivante, qui est plus opérative : $F \in \mathbb{R}[X_1, \ldots, X_n]$ est quasiconvexe ssi pour tout $x, y \in \mathbb{R}^n$ et pour tout $\alpha \in \mathbb{R}$, $0 \leq \alpha \leq 1$, on a :

$$F\big(\alpha x + (1-\alpha)y\big) \leq \max\big\{F(x), F(y)\big\}.$$

Il est facile de vérifier qu'un polynôme quasiconvexe non constant $F \in \mathbb{R}[X]$ (en une seule variable) n'admet pas de maximum local, et que donc, s'il est de degré pair, son coefficient conducteur est positif et s'il est de degré impair, la fonction qu'il définit est strictement croissante ou décroissante suivant le signe de son coefficient conducteur.

La preuve de la propriété « d'uniformité » suit maintenant de la définition de polynôme quasiconvexe qui implique que si $x, y, u \in \mathbb{R}^n$, $u \neq 0$, alors $F(x+Tu)$ et $F(y+Tu)$ sont ou bien tous deux constants ou bien de même degré $d \neq 0, -1$ et ont même coefficient conducteur. Voir [1, chap. 4], ou [2] pour les détails. □

Propriété de « linéarité » d'une forme homogène quasiconvexe. — *Soit* $P \in \mathbb{R}[X_1, \ldots, X_n]$ *une forme homogène quasiconvexe de degré* $d \geq 1$, *et soient* :

$$L := \big\{x \in \mathbb{R}^n : P(x) = 0\big\}, \quad K := \big\{x \in \mathbb{R}^n : P(x) \leq 0\big\}.$$

Alors :

- L *est un sous-espace linéaire de* $\mathbb{R}^n$.

- *Si d est pair, $K = L$,*
- *Si d est impair, L est un hyperplan et K est l'un des demi-espaces limités par L.*

Preuve. — C'est une conséquence immédiate de la propriété antérieure (voir [1, chap. 4], ou [2]). □

Nous montrerons maintenant une version effective de cette propriété, qui exhibe une base $\mathcal{B}$ de L (et un système de générateurs $\mathcal{G}$ de K) construite à partir des coefficients de la forme homogène quasiconvexe P.

LEMME 1. — *Soit $P \in \mathbb{Z}[X_1, \ldots, X_n]$ une forme homogène quasiconvexe (à coefficients entiers) de degré d, et soit $\tilde{d} := \max\{2, d\}$. Alors le sous-espace linéaire $L = \{x \in \mathbb{R}^n : P(x) = 0\}$ admet une base entière $\mathcal{B}$ telle que $\ell(\mathcal{B}) = \tilde{d}^{0(r)}(\ell(P) + n)$ où $r := n - \dim_{\mathbb{R}} L$, et si d est impair, le demi-espace K admet un système de générateurs entier $\mathcal{G}$ (i.e. $K = \{\sum_{v \in \mathcal{G}} \lambda_v \cdot v, \lambda_v \geq 0\}$) tel que $\ell(\mathcal{G}) = \ell(\mathcal{B})$.*

Preuve. — On observe tout d'abord que si P est quasiconvexe, il existe une variable X_j telle que $\deg_{X_j} P = d$ (voir [1] ou [2] pour les détails). Sans perte de généralité, supposons que X_1 est cette variable. On procède par induction sur n.

Soit $n \geq 2$. Si $L \neq \{0\}$, soit $u \in L - \{0\}$. Le fait que pour tout $t \in \mathbb{R}$, $P(tu) = t^d P(u) = 0$ implique par la propriété «d'uniformité» que pour tout $x \in \mathbb{R}^n$, le polynôme $P(x + Tu)$ est constant comme polynôme en T; c'est-à-dire que pour tout $x \in \mathbb{R}^n$, $P(x) = P(x + u)$. Ainsi :

$$(*) \qquad P(X) = P(X + u) \quad \text{pour tout } u \in L.$$

Posons :

$$P(X_1, \ldots, X_n) = a_d(X_2, \ldots, X_n) X_1^d + a_{d-1}(X_2, \ldots, X_n) X_1^{d-1} + \cdots + a_1(X_2, \ldots, X_n) X_1 + a_0(X_2, \ldots, X_n)$$

où $a_d(X_2, \ldots, X_n) \neq 0$, et où $a_i(X_2, \ldots, X_n) \in \mathbb{Z}[X_2, \ldots, X_n]$ est une forme homogène de degré $(d - i)$ pour tout $0 \leq i \leq d$ (c'est-à-dire $a_d(X_2, \ldots, X_n) = a_d \in \mathbb{Z} - \{0\}$ et $a_{d-1}(X_2, \ldots, X_n) := \sum_{2 \leq k \leq n} b_k X_k$ est une forme linéaire entière).

Évaluons le polynôme P en $X + u := (X_1 + u_1, \ldots, X_n + u_n)$:

$$\begin{aligned} P(X + u) &= a_d \cdot (X_1 + u_1)^d + \Big\{ \sum_{2 \leq k \leq n} b_k \cdot (X_k + u_k) \Big\} \cdot (X_1 + u_1)^{d-1} \\ &\qquad + \cdots + a_0(X_2 + u_2, \ldots, X_n + u_n) \\ &= P(X) + X_1^{d-1} \Big\{ d a_d u_1 + \sum_{2 \leq k \leq n} b_k u_k \Big\} + \cdots + P(u) \end{aligned}$$

(où les termes compris dans les points de suspension sont de degré en X_1 inférieur à $(d-1)$). Par (*), on conclut que :

$$L \subseteq L^1 := \Big\{ u \in \mathbb{R}^n : da_d u_1 + \sum_{2 \le k \le n} b_k u_k = 0 \Big\}.$$

L'hyperplan L^1 admet la base entière

$$\big\{(-b_2, da_d, 0, \ldots, 0), \ldots, (-b_n, 0, \ldots, 0, da_d)\big\}$$

(qui se complète à une base $\mathcal{B}^1$ de $\mathbb{R}^n$ en ajoutant le vecteur $(1, 0, \ldots, 0)$, de manière que $\ell(\mathcal{B}^1) = \ell + \log_2 d$).

Si la forme homogène P restreinte à L^1 n'est pas la forme nulle (c'est-à-dire si $L \neq L^1$), on pose

$$P^1\big(Y_1, \ldots, Y_{n-1}\big) := P\big(-b_2 Y_1 - \cdots - b_n Y_{n-1}, da_d Y_1, \ldots, da_d Y_{n-1}\big)$$

et on obtient la forme homogène quasiconvexe P^1 en $(n-1)$ variables, qui représente (dans la base $\mathcal{B}^1$) la forme P restreinte à L^1.

P^1 vérifie l'estimation suivante (où c est une constante universelle) :

$$\begin{aligned} \ell(P^1) &\le \ell(P) + d\big(\log_2 d + \ell(\mathcal{B}^1)\big) + n \log_2(d+1) \\ &= (d+1)\ell(P) + 2d \log_2 d + n \log_2(d+1) \\ &= \tilde{d}^c\big(\ell(P) + n\big). \end{aligned}$$

Étant donné que $L \neq L^1$, la forme quasiconvexe P^1 n'est pas la forme nulle et on répète la procédure avec elle.

Supposons que $L = L^r$, pour un certain $0 \le r \le n$, c'est-à-dire que la forme P^{r-1} restreinte à L^r est la forme nulle, alors $\dim_{\mathbb{R}} L = n - r$ et $\ell(P^{r-1}) \le \tilde{d}^{c(r-1)}(\ell(P) + (r-1)n)$. De plus, on a :

$$\ell(\mathcal{B}^r) \le \ell(P^{r-1}) + \log_2 d = \tilde{d}^{c(r-1)}\big(\ell(P) + (r-1)n\big)$$

(où $\mathcal{B}^r$ est la base correspondante de L, écrite en termes de la base $\mathcal{B}^{r-1}$ de L^{r-1}).

On récupère finalement l'écriture canonique $\mathcal{B}$ de la base $\mathcal{B}^r$ de L en multipliant r matrices de passage, à coefficients de longueurs binaires contrôlées par $\tilde{d}^{c(r-1)}(\ell(P) + (r-1)n)$, obtenant ainsi :

$$\begin{aligned} \ell(\mathcal{B}) &\le (r-1)\log_2 n + r\big(\tilde{d}^{c(r-1)}\big(\ell(P) + (r-1)n\big)\big) \\ &= \tilde{d}^{0(r)}\big(\ell(P) + n\big). \end{aligned}$$

La borne pour $\ell(\mathcal{G})$, si d est impair, est claire. □

Ce lemme a la conséquence suivante :

COROLLAIRE. — *Soit* $F = \sum_{0\leq i\leq d} P_i \in \mathbb{Z}[X_1,\dots,X_n]$ *un polynôme quasiconvexe écrit comme somme de formes homogènes de degré* i, *et soit* $\tilde{d} := \max\{2,d\}$. *Alors, pour tout* $0 \leq i \leq d$, *l'ensemble*

$$L_i(F) := \big\{x \in \mathbb{R}^n : P_d(X) = 0,\dots,P_i(x) = 0\big\}$$

est un sous-espace linéaire de $\mathbb{R}^n$, *qui admet une base entière* $\mathcal{B}_i$ *avec* $\ell(\mathcal{B}_i) = \tilde{d}^{0(n)}\ell(F)$ *et l'ensemble*

$$K_i(F) := \big\{x \in \mathbb{R}^n : P_d(x) = 0,\dots,P_{i+1}(x) = 0, P_i(x) \leq 0\big\}$$

est ou bien un demi-sous-espace de $\mathbb{R}^n$, *qui admet un système de générateurs entier* $\mathcal{G}_i$ *avec* $\ell(\mathcal{G}_i) = \tilde{d}^{0(n)}\ell(F)$, *ou bien coïncide avec* $L_i(F)$.

Preuve. — C'est une application immédiate du fait que si F est un polynôme quasiconvexe, sa forme homogène P_d de plus haut degré est aussi quasiconvexe, et du lemme précédent. □

Après ces considérations d'ordre général sur les polynômes quasiconvexes, passons au caractère particulier de notre problème.

2. Élimination des contraintes superflues et réduction à un ensemble borné. — Soient $F_1,\dots,F_s \in \mathbb{Z}[X_1,\dots,X_n]$ des polynômes quasiconvexes de degré majoré par $d \geq 2$, et soit $\ell := \ell(\{F_1,\dots,F_s\})$. Soit M l'ensemble convexe défini par :

$$M := \big\{x \in \mathbb{R}^n : F_1(x) \leq 0,\dots,F_s(x) \leq 0\big\}.$$

Le but de cette section est d'étudier lesquelles des contraintes $F_1,\dots,F_s$ sont de trop, c'est-à-dire de déterminer à partir des contraintes F_i $(1 \leq i \leq s)$ qui définissent M un ensemble convexe M' d'aspect plus uniforme que M et vérifiant principalement la condition :

$$M \cap \mathbb{Z}^n \neq \emptyset \iff M' \cap \mathbb{Z}^n \neq \emptyset.$$

Pour cela, faisons le raisonnement suivant.

Supposons qu'il existe une direction $u \in \mathbb{R}^n - \{0\}$ telle que $F_1(Tu)$ soit strictement décroissant et $F_2(Tu),\dots,F_s(Tu)$ soient décroissants ou constants (dans ce cas on dit que u est une direction de récession de $F_1,\dots,F_s$, non constante pour F_1), et supposons de plus que $u \in \mathbb{Z}^n$.

Soit alors $x_1 \in \mathbb{Z}^n$ tel que $F_2(x_1) \leq 0,\dots,F_s(x_1) \leq 0$; l'hypothèse et la propriété « d'uniformité » de F_1 impliquent que $F_1(x_1+Tu)$ est strictement décroissant et on peut choisir $t \in \mathbb{N}$ de manière que $F_1(x_1+tu) \leq 0$. Posons $x := x_1+tu$. Le même argument que ci-dessus montre que pour $2 \leq i \leq s$,

on a $F_i(x) = F_i(x_1 + tu) \leq F_i(x_1) \leq 0$. Donc, $x \in \mathbb{Z}^n$ est tel que $F_1(x) \leq 0, \ldots, F_s(x) \leq 0$, et dans ce cas nous dirons que F_1 est une contrainte superflue.

Il est clair que le rôle de F_1 peut être joué par n'importe quelle contrainte F_j $(1 \leq j \leq s)$, et pour la considération de l'ensemble M, nous supprimerons la contrainte superflue. Une fois éliminée une contrainte superflue, on peut répéter le procédé jusqu'à la suppression (dans un certain ordre) de toutes les contraintes superflues.

Les questions qui se posent sont alors les suivantes : comment choisir les directions de récession entières u ? Que se passe-t-il quand il n'y a plus de contraintes superflues ?

La réponse est dans la proposition suivante :

PROPOSITION. — *Il existe* $\{i_1, \ldots, i_t\} \subseteq \{1, \ldots, s\}$ *tel que si*

$$M' := \{x \in \mathbb{R}^n : F_{i_1}(x) \leq 0, \ldots, F_{i_t}(x) \leq 0\},$$

alors :

(i) $M \cap \mathbb{Z}^n \neq \emptyset \iff M' \cap \mathbb{Z}^n \neq \emptyset$.

(ii) *A partir de chaque point entier* $x' \in M'$, *on récupère un point entier* $x \in M$ *de manière que* :

$$\ell(x) = d^n \ell(x') + d^{0(n)} \ell.$$

(*Dans le cas où* $t = s$, *on peut choisir* $x' = 0$.)

(iii) $M' = V + (M' \cap V^{\perp})$, *où* V *est un sous-espace linéaire de* $\mathbb{R}^n$, *qui admet une base entière* $\mathcal{B}$ *telle que* $\ell(\mathcal{B}) = d^{0(n)}\ell$, *et* $M' \cap V^{\perp}$ *est un sous-ensemble compact de* $\mathbb{R}^n$.

Preuve. — Selon le raisonnement fait auparavant, le procédé consiste à trouver des directions entières de récession u, non constantes pour une contrainte donnée.

Pour tout $F \in \mathbb{Z}[X_1, \ldots, X_n]$ quasiconvexe, posons :

$$L(F) := \{u \in \mathbb{R}^n : \sup\{F(tu), t \in \mathbb{R}\} < +\infty\},$$

$$K(F) := \{u \in \mathbb{R}^n : \sup\{F(tu), t \geq 0\} < +\infty\}.$$

Il est alors clair que $u \in \mathbb{Z}^n - \{0\}$ est une direction de récession de $F_1, \ldots, F_s$, non constante pour F_j, si et seulement si

$$u \in K(F_1) \cap \ldots \cap K(F_s) \quad \text{et} \quad u \notin L(F_j).$$

Dans [1, chap. 4] ou [2], il est montré que pour tout $F = \sum_{0 \leq i \leq d} P_i$ quasiconvexe, écrit comme somme de formes homogènes de degré i, il existe i_0, $1 \leq i_0 \leq d$, tel que :

$$L(F) = \{u \in \mathbb{R}^n : P_d(u) = 0, \ldots, P_{i_0}(u) = 0\}, \text{ et}$$
$$K(F) = \{u \in \mathbb{R}^n : P_d(u) = 0, \ldots, P_{i_0+1}(u) = 0,\ P_{i_0}(u) \leq 0\}.$$

C'est-à-dire, suivant la notation du COROLLAIRE, $L(F) = L_{i_0}(F)$ et $K(F) = K_{i_0}(F)$; ainsi, une direction $u \in \mathbb{Z}^n\{0\}$ est de récession de $F_1, \ldots, F_s$ non constante pour F_j si et seulement si $u \neq 0$ appartient au cône polyédral (i.e. à l'intersection d'un nombre fini de demi-espaces de $\mathbb{R}^n$) $K(F_1) \cap \ldots \cap K(F_s)$ mais non au sous-espace linéaire $L(F_j)$. La preuve de la proposition s'obtient maintenant à l'aide des résultats suivants :

LEMME 2. — *Dans les conditions de la Proposition, supposons que* $K(F_1) \cap \ldots \cap K(F_s) \not\subseteq L(F_j)$, *et soit* $x_1 \in \mathbb{Z}^n$ *tel que* $F_i(x_1) \leq 0$, *pour tout* $i \neq j$. *Alors il existe* $x \in M \cap \mathbb{Z}^n$ *tel que* $\ell(x) = d(\ell(x_1) + d^{0(n)}\ell)$.

Preuve. — Si le cône polyédral $K(F_1) \cap \ldots \cap K(F_s)$ n'est pas contenu dans $L(F_j)$, il existe un générateur u du cône qui n'appartient pas à $L(F_j)$. D'après la démonstration du théorème de Farkas-Minkowski-Weyl (qui affirme qu'un cône convexe est polyédral si et seulement si il admet un nombre fini de générateurs; voir par exemple [11, cor. 7.1.a] ou [10]) et d'après les bornes énoncées dans le LEMME 1, il existe un système de générateurs entier $\mathcal{G}$ du cône polyédral $K(F_1) \cap \ldots \cap K(F_s)$ tel que $\ell(\mathcal{G}) = d^{0(n)}\ell$. Ceci montre qu'on peut choisir $u \in \mathbb{Z}^n - \{0\}$, tel que $\ell(u) = d^{0(n)}\ell$. Le raisonnement présenté auparavant montre aussi qu'il existe un entier $t \in \mathbb{N}$ tel que $F_j(x_1 + tu) \leq 0$. Un tel t dépend de la taille des coefficients du polynôme $F_j(x_1 + Tu)$, c'est-à-dire des coefficients de F_j, de x_1 et de u (voir par exemple [8] pour cette relation). On pose alors $x := x_1 + tu$, et on obtient $\ell(x) = d(\ell(x_1) + d^{0(n)}\ell)$. □

Pour compléter la preuve de (i) et (ii) de la PROPOSITION, on procède par récurrence en travaillant maintenant avec les contraintes F_i, $1 \leq i \leq s$, $i \neq j$, et en supprimant une à une, dans un certain ordre, toutes les contraintes superflues. On obtient ainsi un ensemble :

$$M' := \{x \in \mathbb{R}^n : F_{i_1}(x) \leq 0, \ldots, F_{i_t}(x) \leq 0\}$$

de manière que pour tout j, $1 \leq j \leq t$, $K(F_{i_1}) \cap \ldots \cap K(F_{i_t}) \subseteq L(F_{i_j})$. Cet ensemble vérifie la condition (i) de la PROPOSITION :

$$M \cap \mathbb{Z}^n \neq \emptyset \iff M' \cap \mathbb{Z}^n \neq \emptyset.$$

Pour (ii), on a le lemme suivant :

LEMME 3. — *Soit M' défini comme précédemment et soit $x' \in M' \cap \mathbb{Z}^n$. Alors, il existe $x \in M \cap \mathbb{Z}^n$ tel que :*

$$\ell(x) = d^n \ell(x') + d^{0(n)}\ell.$$

(*Dans le cas où M' n'est défini par aucune contrainte, on pose $x' := 0$.*)

Preuve. — Supposons sans perte de généralité que pour définir M', on ait supprimé, dans cet ordre, F_s, $F_{s-1}, \ldots, F_{r+1}$ et qu'ainsi :

$$M' := \{x \in \mathbb{R}^n : F_1(x) \leq 0, \ldots, F_r(x) \leq 0\}.$$

Si on appliquait récursivement le résultat du lemme précédent, on obtiendrait l'estimation suivante :

$$\ell(x) \leq d^s\big(\ell(x') + sd^{0(n)}\ell\big)$$

puisque a priori la seule borne sur le nombre de contraintes qu'on supprime est le nombre total s de contraintes. Ceci n'est pas l'estimation désirée étant donné que s apparaît dans l'exposant. Le raisonnement suivant permet de borner le nombre de répétitions de la procédure du lemme par la dimension n de l'espace ambiant.

Rappelons que si $K \subseteq \mathbb{R}^n$ est un ensemble convexe,

$$\dim_{\mathbb{R}} K := \min\{\dim_{\mathbb{R}} L, L \text{ sous-espace linéaire de } \mathbb{R}^n \text{ qui contient } K\}.$$

Et par simplicité, définissons :

$$K_{r+1} := K(F_1) \cap \ldots \cap K(F_r) \cap K(F_{r+1}),$$

$$K_{r+i} := K_{r+i-1} \cap K(F_{r+i}), \quad \text{pour tout } i > 1.$$

Clairement $K_s \subseteq K_{s-1} \subseteq \ldots \subseteq K_{r+1}$.

On considérera en une seule étape tous les ensembles convexes K_{r+i} de même dimension. Par exemple, soit :

$$\dim_{\mathbb{R}} K_{r+1} = \cdots = \dim_{\mathbb{R}} K_{r+j} > \dim_{\mathbb{R}} K_{r+j+1} = \cdots$$

Alors, pour tout $1 \leq i \leq j$, le fait qu'on ait supprimé la contrainte F_{r+i} de l'ensemble $\{F_1, \ldots, F_{r+i}\}$ implique :

$$\dim_{\mathbb{R}}\big(K_{r+1} \cap L(F_{r+i})\big) < \dim_{\mathbb{R}} K_{r+1} = \cdots = \dim_{\mathbb{R}} K_{r+j}.$$

On affirme que dans ce cas on peut choisir $u \neq 0$, $u \in K_{r+j}$, tel que $u \notin L(F_{r+i})$ $(1 \leq i \leq j)$, c'est-à-dire que la direction u va servir pour supprimer en une fois toutes les contraintes $F_{r+j}, \ldots, F_{r+1}$ de l'ensemble $\{F_1, \ldots, F_{r+j}\}$. Pour cela, on considère un système de générateurs $\mathcal{G}$ du cône polyédral K_{r+j}, tel que $\ell(\mathcal{G}) = d^{0(n)}\ell$, et on pose $u := v_1 + \cdots + v_e$, où $\{v_1, \ldots, v_e\} \subseteq \mathcal{G}$ est un système linéairement indépendant maximal de $\mathcal{G}$. La propriété «d'uniformité» des polynômes quasiconvexes permet de montrer l'affirmation; d'autre part il est clair que $\ell(u) = d^{0(n)}\ell$.

Ce procédé permet de contrôler le nombre de répétitions du lemme par la dimension n de l'espace ambiant, ce qui fournit la borne :

$$\ell(x) = d^n\big(\ell(x') + nd^{0(n)}\ell\big) = d^n\ell(x') + d^{0(n)}\ell. \quad \square$$

Finalement, étant donné que le fait que l'ensemble

$$M' = \big\{x \in \mathbb{R}^n : F_{i_1}(x) \leq 0, \ldots, F_{i_t}(x) \leq 0\big\}$$

ne contienne plus aucune contrainte superflue est équivalent à la condition $K(F_{i_1}) \cap \ldots \cap K(F_{i_t}) = L(F_{i_1}) \cap \ldots \cap L(F_{i_t})$, on achève la preuve de la proposition à l'aide du lemme suivant :

LEMME 4. — *Soient* $F_{i_1}, \ldots, F_{i_t} \in \mathbb{Z}[X_1, \ldots, X_n]$ *quasiconvexes tels que* $K(F_{i_1}) \cap \ldots \cap K(F_{i_t}) = L(F_{i_1}) \cap \ldots \cap L(F_{i_t})$.

Soit

$$M' = \big\{x \in \mathbb{R}^n : F_{i_1}(x) \leq 0, \ldots, F_{i_t}(x) \leq 0\big\}$$

et soit $\ell := \ell(\{F_{i_1}, \ldots, F_{i_t}\})$.

Alors

$$M' = V + \big(M' \cap V^{\perp}\big)$$

où V *est un sous-espace linéaire de* $\mathbb{R}^n$ *qui admet une base* $\mathcal{B}$ *telle que* $\ell(\mathcal{B}) = d^{0(n)}\ell$ *et* $M' \cap V^{\perp}$ *est un sous-ensemble compact de* $\mathbb{R}^n$.

Preuve. — On définit $V := L(F_{i_1}) \cap \ldots \cap L(F_{i_t})$. Il est clair que V est un sous-espace linéaire de $\mathbb{R}^n$ et on peut facilement en construire une base $\mathcal{B}$ telle que $\ell(\mathcal{B}) = d^{0(n)}\ell$ (en utilisant le fait que chaque $L(F_{i_j})$ admet une base de longueur binaire majorée par $d^{0(n)}\ell$). Soit maintenant $x \in M'$; il existe une représentation de x de la forme $x = y + u$, où $y \in V^{\perp}$ et $u \in V$. Alors, $y = x - u \in M'$ (puisque $-u \in V$ et que par la définition de V,

$$F_{i_k}\big(x + (-u)\big) \leq F_{i_k}(x) \leq 0,$$

pour $1 \leq k \leq t$) c'est-à-dire $x \in (M' \cap V^{\perp}) + V$.

L'inclusion réciproque se montre similairement.

Il suffit de montrer maintenant que l'ensemble $(M' \cap V^{\perp})$ est compact : si l'ensemble fermé et convexe $M' \cap V^{\perp}$ ne l'était pas, il contiendrait une demi-droite $\{x + tu\,;\ t \geq 0\}$, où $x \in M' \cap V^{\perp}$ et $u \in \mathbb{R}^n - \{0\}$ (voir par exemple [10]). Ceci entraînerait que la direction u est une direction de récession de $F_{i_1}, \ldots, F_{i_t}$, et ainsi, $u \in V$. D'un autre côté, on obtient que $u \in V^{\perp}$; par conséquent, $u = 0$, contradiction. □

3. La borne semi-algébrique. — En vertu de la PROPOSITION de la section précédente, il suffit, pour conclure la démonstration du THÉORÈME 1, de montrer que si l'ensemble $M' \cap V^{\perp}$ est non vide, alors il contient un point entier x' de longueur binaire $\ell(x') = (sd)^{0(n)}\ell$.

Étant donné que M' se décompose comme somme d'un sous-espace linéaire de $\mathbb{R}^n$ et d'un ensemble compact, nous nous réduirons à la considération d'un ensemble borné, de rayon dépendant de celui du compact, et nous appliquerons ensuite les résultats précis de géométrie semi-algébrique de par exemple [12] ou [5] pour borner le rayon du compact.

On peut, sans perte de généralité, supposer dans cette section que $M = \{x \in \mathbb{R}^n : F_1(x) \leq 0, \ldots, F_s(x) \leq 0\}$ ne contient aucune contrainte superflue (dans le sens donné dans la section précédente), ce qui entraîne que $M = V + (M \cap V^{\perp})$, où $M \cap V^{\perp}$ est compact et V linéaire admet une base entière $\mathcal{B}$ telle que $\ell(\mathcal{B}) = d^{0(n)}\ell$.

OBSERVATION . — *Si $M \cap \mathbb{Z}^n$ est non vide, alors M contient un point entier dans l'ensemble $M \cap V^{\perp} + B$, où $B := \left\{\sum_{v \in \mathcal{B}} \beta_v \cdot v,\ 0 \leq \beta_v < 1\right\}$.*

Preuve. — Soit $x \in M \cap \mathbb{Z}^n$. On a la décomposition $x = y + u$, $y \in M \cap V^{\perp}$ et $u \in V$. Soit $\mathcal{B} := \{v_1, \ldots, v_m\}$ la base entière de V et soit $u = \alpha_1 v_1 + \cdots + \alpha_m v_m$ $(\alpha_1, \ldots, \alpha_m \in \mathbb{R})$ la représentation de u dans la base $\mathcal{B}$. Pour tout $1 \leq i \leq m$, posons :

$$\alpha_i = [\alpha_i] + \beta_i \quad \text{où} \quad [\alpha_i] \in \mathbb{Z} \quad \text{et} \quad 0 \leq \beta_i < 1$$

et soit $\bar{x} := y + \beta_1 v_1 + \cdots + \beta_m v_m$. Alors $\bar{x} = x - ([\alpha_1]v_1 + \cdots + [\alpha_m]v_m) \in \mathbb{Z}^n$. De plus, $\bar{x} \in M + V \subseteq M$; par conséquent, $\bar{x} \in M \cap \mathbb{Z}^n$ et $\bar{x}$ appartient à $M \cap V^{\perp} + B$. □

Ceci signifie que si l'ensemble $M \cap \mathbb{Z}^n$ est non vide, il contient un point « près » de l'ensemble borné $M \cap V^{\perp}$. Étant donné que la base $\mathcal{B}$ de V est telle que $\ell(\mathcal{B}) = d^{0(n)}\ell$, il suffit, pour conclure la démonstration du théorème, de montrer l'existence d'un rayon $R \in \mathbb{N}$ tel que $M \cap V^{\perp} \subseteq B(0, R)$ et $\ell(R) = (sd)^{0(n)}\ell$.

LEMME 5. — *$M \cap V^{\perp} \subseteq B(0, R)$, où $R \in \mathbb{N}$ est tel que $\ell(R) = (sd)^{0(n)}\ell$.*

Preuve. — L'ensemble semi-algébrique $M \cap V^{\perp}$ peut être défini à l'aide d'une formule sans quantificateurs du langage de premier ordre de $\mathbb{R}$ à constantes dans $\mathbb{Z}$, dans laquelle apparaissent les coefficients des polynômes $F_1, \ldots, F_s$ et les équations de $V^{\perp}$. On peut alors décrire l'ensemble semi-algébrique $S := \{\rho \in \mathbb{R} : M \cap V^{\perp} \subseteq B(0,\rho)\}$ par la formule Φ suivante (qui a un seul bloc de quantificateurs) :

$$\Phi : (\forall X) \quad \big(X \in M \cap V^{\perp} \Rightarrow \|X\|^2 \leq \rho^2\big)$$

où $X := (X_1, \ldots, X_n)$ sont les variables liées de Φ et ρ est la seule variable libre. Si on applique à Φ l'algorithme rapide d'élimination des quantificateurs pour le cas particulier d'une formule à une variable libre et un bloc de quantificateurs (voir par exemple [12]), on obtient une formule Ψ sans quantificateurs, en la variable ρ, qui décrit exactement l'ensemble S.

Ψ est une disjonction de conjonctions de conditions de signes sur certains polynômes $G_1, \ldots, G_m \in \mathbb{Z}[\rho]$. Étant donné que dans la formule originale Φ tous les paramètres sont de longueur binaire majorée par $d^{0(n)}\ell$ et le nombre et les degrés des polynômes peuvent l'être par s et d respectivement, l'algorithme d'élimination des quantificateurs garantit que ces polynômes $G_1, \ldots, G_m$ vérifient :

$$\deg(G_i) = (sd)^{0(n)} \quad \text{pour} \quad 1 \leq i \leq m \quad \text{et}$$
$$\ell\big(\{G_1, \ldots, G_m\}\big) = (sd)^{0(n)}\ell.$$

De plus, si $\alpha \in \mathbb{R}$ est la plus grande racine réelle qui apparaît dans les polynômes $G_1, \ldots, G_m$, on observe que la formule Ψ est toujours vraie ou toujours fausse dans l'intervalle $]\alpha, +\infty[$ (puisqu'à la droite de α, il n'y a changement de signe d'aucun des polynômes $G_1, \ldots, G_m$).

Comme Ψ est vraie pour $+\infty$, Ψ doit être vraie dans l'intervalle $]\alpha, +\infty[$, et par conséquent il suffit de majorer la plus grande racine réelle des polynômes $G_1, \ldots, G_m$ pour obtenir le rayon R cherché.

La borne sur les degrés et la longueur binaire des coefficients des polynômes $G_1, \ldots, G_m$ produit directement une borne $R \in \mathbb{N}$ pour leurs racines réelles, telle que $\ell(R) = (sd)^{0(n)}\ell$ (on applique par exemple l'inégalité de Cauchy, [8]).

Ainsi s'achève la preuve du THÉORÈME 1. □

Preuve du corollaire. — Celle-ci est immédiate puisque, sachant que si l'ensemble $\{x \in \mathbb{Z}^n : F_1(x) \leq 0, \ldots, F_s(x) \leq 0\}$ est non vide, il contient un point dans la boule $B(0,R)$, où R est tel que $\ell(R) = (sd)^{0(n)}\ell$, il suffit

de vérifier si un point entier $x \in \mathbb{Z}^n$, de longueur binaire majorée par cette borne vérifie les conditions $F_1(x) \leq 0, \ldots, F_s(x) \leq 0$. Cela peut bien sûr s'effectuer en temps $(sd)^{0(n)}\ell$, en tenant compte du degré de $F_1, \ldots, F_s$ et de $\ell(\{F_1, \ldots, F_s\})$. (Observons qu'une borne déterministe est de l'ordre de $2^{(sd)^{0(n)}\ell}$ puisqu'il faut évaluer les polynômes $F_1, \ldots, F_s$ en tous les points entiers de la boule $B(0, R)$.) □

Preuve du théorème 2. — On applique ici à nouveau les méthodes utilisées pour montrer le THÉORÈME 1 : suppression des contraintes superflues et réduction à un ensemble compact. Nous ne fournirons pas ici une preuve complète mais simplement une esquisse de la démonstration, nous remettant à [7] pour les détails.

(i) Étant donné que $M \cap \mathbb{Z}^n \neq \emptyset$, il existe $x_0 \in M \cap \mathbb{Z}^n \cap B(0, R)$ où $\ell(R) = (sd)^{0(n)}\ell$ (THÉORÈME 1), et $\ell(F(x_0)) = (sd)^{0(n)}\ell$.

(ii) Étant donné que $m := \inf\{F(x) : x \in M \cap \mathbb{Z}^n\} > -\infty$, on a $F(x_0) \geq m$, et, par conséquent, si

$$N := \{x \in \mathbb{R}^n : F_1(x) \leq 0, \ldots, F_s(x) \leq 0,\ F(x) \leq F(x_0)\},$$

alors $N \cap \mathbb{Z}^n$ est non vide et $m = \inf\{F(x) : x \in N \cap \mathbb{Z}^n\}$.

On procède maintenant à la suppression des contraintes superflues de la succession $F_1, \ldots, F_s,\ F - F(x_0)$, de manière à obtenir un ensemble N', défini par éventuellement moins de contraintes, comme dans la PROPOSITION de la preuve du THÉORÈME 1. (ii) implique que dans cette procédure, on n'élimine jamais la contrainte $F - F(x_0)$, et par conséquent :

$$\inf\{F(x) : x \in N \cap \mathbb{Z}^n\} = \inf\{F(x) : x \in N' \cap \mathbb{Z}^n\}.$$

Comme auparavant, on a la décomposition :

$$N' = W + (N' \cap W^{\perp})$$

où W est un sous-espace linéaire de $\mathbb{R}^n$, qui admet une base entière $\mathcal{B}$ telle que $\ell(\mathcal{B}) = (sd)^{0(n)}\ell$, et $N' \cap W^{\perp}$ est un sous-ensemble compact de $\mathbb{R}^n$ qui vérifie $N' \cap W^{\perp} \subseteq B(0, R)$, avec $\ell(R) = (sd)^{0(n)}\ell$.

On montre ensuite que :

$$\inf\{F(x) : x \in N' \cap \mathbb{Z}^n\} = \inf\{F(x) : x \in (N' \cap W^{\perp} + B) \cap N' \cap \mathbb{Z}^n\}$$

où $B := \{\sum_{v \in \beta} \beta_v \cdot v, 0 \leq \beta_v < 1\}$ et on achève la démonstration en récupérant à partir du point entier x' de $N' \cap \mathbb{Z}^n$ qui se trouve dans

l'ensemble $N' \cap W^{\perp} + B$ et tel que $F(x') = m$, un point entier $x \in M \cap \mathbb{Z}^n$ qui vérifie $\ell(x) = (sd)^{0(n)}\ell$ et $F(x) = m$.

Observons, avant de conclure, que l'hypothèse du théorème

$$\inf\{F(x) : x \in M \cap \mathbb{Z}^n\} = m > \infty$$

entraîne que le résultat ne fournit pas une procédure de recherche de m, mais il est facile de montrer que dans nos conditions particulières, si $M \cap \mathbb{Z}^n$ est non vide, alors

$$\inf\{F(x) : x \in M \cap \mathbb{Z}^n\} > -\infty \iff \inf\{F(x) : x \in M\} > -\infty$$

et par conséquent, étant donné qu'on peut vérifier rapidement à l'aide de l'élimination des quantificateurs (voir [5]) si $\inf\{F(x) : x \in M\} > -\infty$, on obtient une procédure de recherche de m. □

BIBLIOGRAPHIE

[1] Bank (B.) and Mandel (R.). — *Parametric integer optimization.* — Akademie-Verlag, Berlin, 1988.

[2] Bank (B.) and Mandel (R.). — *(Mixed-)Integer solutions of quasiconvex polynomial inequalities*, Math. Res., t. **45**, 1988, p. 20–34.

[3] Heintz (J.), Roy (M.-F.) and Solernó (P.). — *On the complexity of semialgebraic sets (Extended abstract)*, Proc. IFIP Congress'89, IX World Computer Congress, North-Holland, 1989, p. 293–298.

[4] Heintz (J.), Roy (M.-F.) et Solernó (P.). — *Complexité du principe de Tarski-Seidenberg*, C. R. Acad. Sci. Paris Sér. I Math., t. **309**, 1989, p. 825–830.

[5] Heintz (J.), Roy (M.-F.) et Solernó (P.). — *Sur la complexité du principe de Tarski-Seidenberg*, Bull. Soc. Math. France, t. **118**, 1990, p. 101–126.

[6] Khachiyan (L.G.). — *Convexity and complexity in polynomial programming.* — Proc. Int. Congress Math., Varsovie, 1983, p. 1569–1577.

[7] Krick (T.). — Complejidad para problemas de geometría elemental, *Thèse*, Université de Buenos Aires, 1990.

[8] Mignotte (M.). — *Mathématiques pour le calcul formel.* — P.U.F, 1989.

[9] RENEGAR (J.). — On the computational complexity and geometry of the first order theory of the reals, Part III, Quantifier elimination, I. Symbolic Computation, t. **13**, 1992, p. 329–352.

[10] ROCKAFELLAR (R.T.). — *Convex Analysis.* — Princeton Mathematical Series 28, 1970.

[11] SCHRIJVER (A.). — *Theory of linear and integer programming.* — Wiley Interscience Series in Discrete Mathematics, 1989.

[12] SOLERNÓ (P.). — Complejidad de conjuntos semialgebraicos, *Thèse*, Université de Buenos Aires, 1989.

[13] TARASOV (S.P.) and KHACHIYAN (L.G.). — *Bounds of solutions and algorithmic complexity of systems of convex diophantine inequalities*, Soviet. Math. Dokl., t. **22, 3**, 1980, p. 700–704.