Solutions minimales des systemes diophantiens lineaires : bornes et algorithmes

Loïc Pottier

UNITÉ DE RECHERCHE
INRIA-SOPHIA ANTIPOLIS

Institut National
de Recherche
en Informatique
et en Automatique

Domaine de Voluceau
Rocquencourt
B.P.105
78153 Le Chesnay Cedex
France
Tél.:(1) 39 63 55 11

Rapports de Recherche

N° 1292

Programme 8
Communication Homme-Machine

SOLUTIONS MINIMALES DES SYSTEMES DIOPHANTIENS LINEAIRES : BORNES ET ALGORITHMES

Loïc POTTIER

Octobre 1990

RR-1292

Solutions minimales des systèmes diophantiens linéaires : bornes et algorithmes

Loïc Pottier

17 septembre 1990

Institut National de Recherche en Informatique et Automatique
2004 route des Lucioles, Sophia Antipolis, 06565 Valbonne CEDEX
Email : pottier@mirsa.inria.fr

Résumé : On donne de nouvelles bornes et de nouveaux algorithmes concernant les solutions minimales de systèmes diophantiens linéaires. Nos bornes sont simplement exponentielles en la dimension du système, alors que les bornes connues jusqu'il y a peu étaient doublement exponentielles.

Minimal solutions for linear diophantine systems : bounds and algorithms

Abstract : We give new bounds and algorithms for minimal solutions of linear diophantine systems. Our bounds are simply exponential, while previous known bounds were, at least until recently, doubly exponential.

1 Introduction

Un système diophantien linéaire est un ensemble d'inéquations linéaires à coefficients entiers dont on cherche les solutions entières : $Ax \leq b$, où A est une matrice d'entiers à m lignes et n colonnes, b un vecteur de Z^met x un vecteur de n indéterminées. Rappelons que décider si un tel système a au moins une solution entière est un problème NP-complet.
On s'intéresse ici à décrire et calculer l'ensemble des solutions, cela en étudiant un problème équivalent, qui est la résolution en entiers positifs des systèmes $Ax = 0$.
Les solutions entières positives de $Ax = 0$ forment un sous-monoïde M de N^n, engendré par ses éléments non nuls minimaux pour l'ordre partiel $(x_1, \ldots, x_n) \preceq (y_1, \ldots, y_n) \iff \forall i, 1 \leq i \leq n, x_i \leq y_i$, qui forment un ensemble fini. On appellera cet ensemble "la base de Hilbert de M" (après [F.Giles et W.R.Pulleyblank 79]), et on le notera $\mathcal{H}(M)$.
Les deux sections suivantes sont consacrées à borner les éléments de $\mathcal{H}(M)$, et à les calculer. La dernière section applique les résultats précédents au problème initial, i.e. la résolution des systèmes $Ax \leq b$.

2 Bornes de $\mathcal{H}(M)$

On sait depuis [J.Von zur Gathen et M.Sieveking 78] que si $\mathcal{H}(M)$ est non vide, elle contient un élément de norme (par exemple $||x||_\infty$, où $||x||_\infty = sup_i |\ x_i\ |$) au plus simple exponentielle en la taille de A (par exemple $n.m.(log||A||_\infty + 2)$).
Mais on s'intéresse ici à borner uniformément les normes des éléments de $\mathcal{H}(M)$.

Soient

$$||M||_\infty = sup_{x \in \mathcal{H}(M)} ||x||_\infty$$

et

$$||M||_1 = sup_{x \in \mathcal{H}(M)} ||x||_1$$

(avec $||x||_1 = \sum_i | x_i |$).
[I.Borosh et L.B.Treybig 76] ont majoré $||M||_\infty$ par une expression double exponentielle en la taille de A.
A notre connaissance, deux bornes simple exponentielles existent pour majorer $||M||_\infty$ ou $||M||_1$. Nous avons donné la première dans [L.Pottier 90]. La seconde peut être déduite d'un résultat peu connu de [J.L.Lambert 87].
Ces deux bornes sont essentiellement différentes de par leurs expressions et leurs démonstrations.
On donne ici deux nouvelles bornes plus fines, la première inspirée de [L.Pottier 90], la seconde de [J.L.Lambert 87] et [A.Koscielski et L.Pacholski 90].
Rappelons que dans le cas d'une équation ($m = 1$), [G.Huet 78] puis [J.L.Lambert 87] ont donné des bornes ne dépendant que de $||A||_\infty$. Dans le cas de deux équations, [J.F.Romeuf 89] donne une borne quadratique en la taille de A.

2.1 Première borne

Cette borne est inspirée de [L.Pottier 90].
Soit $||A||_l = sup_i\{\sum_j | a_{ij} |\}$.

Théorème 1

$$||M||_1 \leq (1 + ||A||_l)^r = B_0$$

Preuve :

On peut sans restriction choisir r équations indépendantes de $Ax = 0$. Soient $x = (x_1, \ldots, x_n)$ un élément de M non nul, $p = ||x||_1$, et $\{e_1, \ldots, e_n\}$ la base canonique de R^n. Pour tout y dans R^n, on note C_y le cube de volume 1 défini par

$$z \in C_y \Leftrightarrow z = y + \sum_{i=1}^{n} \lambda_i e_i, \ avec \ \forall i \in [1,n], \ \lambda_i \in [0,1]$$

On va construire par récurrence une suite de N^n $y^0, \ldots, y^p$ et une suite de R^n $z^0, \ldots, z^p$ vérifiant :

$y^0 = 0 \prec y^1 \prec \ldots \prec y^p = x$.
$\forall k \in [0, p-1], \ \exists j, y^{k+1} = y^k + e_j$
$\forall k \in [0,p], z^k \in C_{y^k} \cap [0,x]$.

$y^0 = z^0 = 0$ convient clairement.

Supposons y^k construit, $0 \leq k \leq p-1$. $[0,x] \cap C_{y^k}$ est l'ensemble des z qui s'écrivent $\lambda \sum_i x_i e_i$ avec $0 \leq \lambda \leq 1$ et

$$\forall i \in [1,n], \ y_i^k \leq \lambda x_i \leq y_i^k + 1$$

Il est par hypothèse non vide, c'est un segment. Prenons $z_{k+1} = \lambda_k \sum_i x_i e_i$ sa borne où λ_k est maximum. x est non nul, donc il existe un j tel que

$$\lambda_k = \frac{y_j^k + 1}{x_j} = inf_{i | x_i \neq 0}\{\frac{y_i^k + 1}{x_i}\}$$

Soit maintenant $y^{k+1} = y^k + ej$. On a alors

$$\forall i \in [1,n], \ y_i^{k+1} \leq \lambda_k x_i \leq y_i^{k+1} + 1$$

et z^{k+1} appartient donc au cube $C_{y^{k+1}}$.

Les points z^{k+1} et y^{k+1} sont donc correctement construits. Enfin, si $k = p-1$, $y^p = x$, car $y^p \preceq x$ et $||y^p||_1 = p = ||x||_1$, et on prend $z^p = 0$.

Soit maintenant $y'^k = z^k - y^k$. On a alors :

$$\forall i, 0 \leq y_i'^k \leq 1$$

donc, si $(Ay^k)_i$ désigne la i^{eme} coordonnée de Ay^k :

$$|\,(Ay^k)_i\,| = |\,(Az^k)_i - (Ay'^k)_i\,| = |\,(Ay'^k)_i\,|$$

Comme $0 \leq y_i'^k \leq 1$, il y donc au plus $\sum_j |\,a_{ij}\,| + 1$ valeurs possibles pour $(Ay^k)_i$ et donc au plus B_0 vecteurs Ay^k distincts.

Supposons maintenant $p > B_0$. Il existe alors (lemme des tiroirs) i et j, $i > j > 0$ avec $Ay^i = Ay^j$. Soit $z = y^i - y^j$. On a alors $Az = 0$. De plus on a $0 \prec z \prec x$, et $z \in M$. Donc $x \notin \mathcal{H}(M)$.

□

2.2 Seconde borne

Soient r le rang de A, a_{ij} son terme de ligne i et de colonne j, et $||A||_1 = \sum_{i,j} |\,a_{ij}\,|$.
Soit D la plus grande valeur absolue des mineurs de A. [J.L.Lambert 87] donne le résultat suivant :

Théorème 2 (Lambert)

$$||M||_\infty \leq nD$$

Reprenant ce résultat, ainsi que celui de [A.Koscielski et L.Pacholski 90], aussi inspiré de [J.L.Lambert 87], nous obtenons les améliorations suivantes :

Théorème 3 *Soit D_r la plus grande valeur absolue des mineurs d'ordre r de A .*

$$||M||_\infty \leq (n-r)D_r = B_1$$

d'où

$$||M||_\infty \leq (n-r)\left(\frac{||A||_1}{r}\right)^r = B_2$$

Preuve :

Soit $\mathcal{C}$ le cône de R^n des solutions réelles positives de $Ax = 0$. Soient $\mathcal{C}_j$ ses intersections avec les hyperplans d'équations $x_j = 0$. Il est clair que $\mathcal{C}$ est l'enveloppe convexe de la réunion des cônes $\mathcal{C}_j$. On peut récursivement appliquer cette décomposition de $\mathcal{C}$ aux $\mathcal{C}_j$, tant que la dimension des cônes construits est plus grande que 1. $\mathcal{C}$ est alors l'enveloppe convexe de la réunion de ces cônes de dimension 1, dits "arêtes" de $\mathcal{C}$.

Chacune de ces arêtes est alors l'ensemble des solutions positives d'un système d'équations obtenues en choisissant r équations indépendantes de $Ax = 0$, et en leur ajoutant $n - r - 1$ équations du type $x_j = 0$ de manière à garder le système de rang maximum, i.e. $n - 1$.

On peut alors obtenir des vecteurs directeurs (à coefficients entiers naturels) des arêtes en calculant les n mineurs d'ordre $n - 1$ pour chacun systèmes précédents, ce qui revient à calculer des mineurs d'ordre r de A.

Soient $g_1, \ldots, g_k$ ces vecteurs, qui ont donc leurs coordonnées majorées en valeur absolue par D_r.

M est alors inclus dans le cône positif qu'ils engendrent (leurs combinaisons linéaires à coefficients réels positifs), qui n'est autre que $\mathcal{C}$, de dimension au plus $n - r$. On a donç grâce au théorème de Carathéodory :

$$Ax = 0, x \geq 0 \implies \exists j_1, \ldots, j_{n-r}, \exists \alpha_1, \ldots, \alpha_{n-r} \geq 0, x = \sum_{l=1}^{n-r} \alpha_i g_{j_i}$$

Si maintenant x est minimal, il est clair que les α_i sont strictement plus petits que 1. On obtient donc la première partie du théorème.

La seconde partie est une majoration simple du déterminant d'une sous-matrice carrée A' d'ordre r de A :

$$| det(A') | \leq \prod_j \sum_i | a'_{ij} | \leq \left(\frac{\sum_{i,j} | a'_{ij} |}{r} \right)^r \leq \left(\frac{\|A\|_1}{r} \right)^r$$

□

La borne B_1 peut être optimale , comme on le verra sur des exemples, mais elle n'est pas raisonnablement calculable en pratique: vaut-il mieux calculer *tous* les mineurs principaux de A que de directement calculer $\mathcal{H}(M)$, par exemple avec l'algorithme de [E.Contejean et H.Devie 89] qui n'utilise pas de borne de $\mathcal{H}(M)$?

2.3 Comparaison de B_0, B_1 et B_2

Il est clair que ces trois bornes sont simple exponentielles en la taille de A. Les exemples suivants montrent qu'on ne peut comparer en général les la première et la derniére, la seconde pouvant être optimale, mais étant incalculable en pratique.
On étudiera les comportements des rapports $\frac{B_2}{B_0}$ (bornes de $\|x\|_\infty$) et $\frac{nB_2}{B_0}$ (bornes de $\|x\|_1$), lorsque n ou $\|A\|_\infty$ tendent vers l'infini.

2.3.1 Exemple 1

Soient a un entier supérieur ou égal à 3 et A la matrice

$$\begin{pmatrix} a & 1-a & & \\ & \ddots & \ddots & \\ & & a & 1-a \end{pmatrix}$$

où les coefficients non écrits sont nuls.
On a $r = m = n - 1$ et $\mathcal{H}(M)$ n'a qu'un élement : $((a-1)^{n-1}, a(a-1)^{n-2}, \ldots, a^{n-1})$.
Ainsi :

$$\|M\|_\infty = B_1 = a^{n-1}, \|M\|_1 = a^n - (a-1)^n, B_2 = (2a-1)^{n-1}, B_0 = (2a)^{n-1}$$

B_1 est donc optimale, B_2 et B_0 étant très proches.
Asymptotiquement, on a enfin :

$$\lim_{n\to\infty} \frac{B_2}{B_0} = 0, \lim_{n\to\infty} \frac{nB_2}{B_0} = 0, \lim_{a\to\infty} \frac{B_2}{B_0} = 1, \lim_{a\to\infty} \frac{nB_2}{B_0} = \infty$$

2.3.2 Exemple 2 : matrices carrées magiques

Une matrice carrée est dite magique si les sommes de ses coefficients d'une ligne ou d'une colonne sont toutes égales. Les matrices carrées magiques d'ordre k à coefficients positifs sont donc les solutions positives du système $Ax = 0$, où $n = k^2 + 1, m = 2k$ et :

$$A = \begin{pmatrix} 1 & \ldots & 1 & & & & -1 \\ & & & 1 & \ldots & 1 & -1 \\ & & & & & \ddots & \vdots \\ 1 & & & 1 & & & -1 \\ & \ddots & & & \ddots & \ldots & \vdots \\ & & 1 & & & 1 & -1 \end{pmatrix}$$

où les coefficients non écrits sont nuls.
On a $r = 2k - 1$. La base de Hilbert de M est l'ensemble des matrices de permutations d'ordre k (cf [R.P.Stanley 83]). Ainsi :

$$||M||_\infty = 1, ||M||_1 = k + 1, B_1 \geq k^2 - 2k + 2$$

$$B_2 = (k^2 - 2k + 2)\left(\frac{2k(k+1)}{2k-1}\right)^{2k-1}, B_0 = (k+2)^{2k-1}$$

et :

$$\lim_{n\to\infty} \frac{B_2}{B_0} = \infty, \lim_{n\to\infty} \frac{nB_2}{B_0} = \infty$$

ce qui donne un comportement inverse de l'exemple précédent.

3 Algorithmes

Le sujet de cette section est le calcul de tous les éléments de $\mathcal{H}(M)$.
Les premiers algorithmes ont été basés sur la borne de [G.Huet 78] puis celle de [J.L.Lambert 87] valables pour une équation, extensibles au cas d'un système, mais donnant des bornes double exponentielles. Ces bornes sont les suivantes :

Propriété 1 *Soit $x = (x_1, \ldots, x_p, y_1, \ldots, y_q)$ un élément de la base de Hilbert de l'équation*

$$a_1x_1 + \ldots + a_px_p + b_1y_1 + \ldots + b_qy_q = 0.$$

où les a_i sont positifs et les b_j sont négatifs. Alors :

$$\forall i, |\, x_i \,| \leq sup_j |\, b_j \,|$$

(Huet)

$$\sum_i x_i \leq sup_j |\, b_j \,|$$

(Lambert).
(la partie concernant les y_j est symétrique).

$\mathcal{H}(M)$ est alors obtenue par énumération sous la borne, et dans le cas de plusieurs équations, on itère la méthode en injectant les solutions des équations précédentes dans la suivantes (après avoir éventuellement triangularisé la matrice A).
Dans le cas de deux équations [J.F.Romeuf 89] donne une méthode originale pour construire un automate fini énumérant $\mathcal{H}(M)$, et une borne quadratique dans ce cas.

3.1 Algorithme de Contejean-Devie

[E.Contejean et H.Devie 89] ont trouvé un algorithme élégant ne nécessitant pas de borne de $\mathcal{H}(M)$. Le principe est le suivant. Ordonnons N^n par l'ordre $\preceq$ précédemment défini, ce qui nous donne un DAG (graphe acyclique) de racine 0. L'algorithme parcourt une partie de ce DAG en profondeur de la manière suivante :
on commence par 0, et si on se trouve sur un vecteur x non nul tel que pour aucun de ses ancêtres y on ait $A(x - y) = 0$, on ne visite que ses fils $x + e_j$ (e_j est le j^{ieme} élement de la base canonique de Z^n) vérifiant $Ax.Ae_j \leq 0$ (le . désignant le produit scalaire de R^n).
Cet algorithme a la surprenante propriété de terminer et d'être complet. En s'arrangeant pour ne pas visiter deux fois un noeud du DAG, et en ne retenant que les solutions minimales pour $\preceq$, on obtient $\mathcal{H}(M)$.
Le seul résultat de complexité sur cet algorithme est, à notre connaissance, une conséquence de [L.Baratchart et L.Pottier 89], qui donne une borne double exponentielle sur le nombre de noeuds visités.
Cet algorithme se comporte bien en pratique, mais est coûteux si les éléments de $\mathcal{H}(M)$ sont de grande norme.

3.2 Un algorithme inspiré du théorème 3

L'examen de la preuve du théorème 1 permet de modifier la méthode de l'algorithme de [E.Contejean et H.Devie 89] en se limitant à n'incrémenter un x que par les e_l tels que pour tout i, la i-ème coordonnée de $A(x+e_l)$ soit comprise entre $-\sum_j a_{ij}^-$ et $\sum_j a_{ij}^+$.
Les générateurs sont alors tous obtenus comme points des suites strictement croissantes construites similairement à l'algorithme précédent.

3.3 Utilisation des bases standard

On donne ici un algorithme nouveau utilisant les bornes précédentes sur $\|M\|_\infty$ et $\|M\|_1$, basé sur la théorie des bases standard (ou de Gröbner).
L'idée est de voir les colonnes de A comme les exposants de monômes à m variables, et les solutions de $Ax = 0$ dans Z^ncommes des sisygies relatives à ces monômes. Un calcul de base standard approprié (par un algorithme de complétion semblable à celui de [B.Buchberger 83]) donne un système de réécriture canonique dont l'inverse énumère M par norme croissante . Il suffit alors de ne retenir que les solutions minimales pour $\preceq$ et de norme inférieure à $inf\{nB_2, B_0\}$.
Soient $X_1, \ldots, X_m, Y_1, \ldots, Y_n$, $n+m$ variables, et k un corps quelconque.
On note a_j la j^{eme} colonne de A.
Pour tous $\alpha \in Z^m$ et $\beta \in Z^n$, on note X^α et Y^β les monômes $X_1^{\alpha_1} \ldots X_m^{\alpha_m}$ et $Y_1^{\beta_1} \ldots Y_n^{\beta_n}$.
α^+ est le sup de α et de zéro (pour l'ordre partiel $\preceq$), et α^- est le sup de $-\alpha$ et zéro. Ainsi $\alpha = \alpha^+ - \alpha^-$.
Pour tout $j \in [1, n]$, on définit un polynôme P_j de l'anneau $R = k[X_1, \ldots, X_m, Y_1, \ldots, Y_n]$:

$$P_j = X^{a_j^+} - Y_j X^{a_j^-}$$

Soit $\mathcal{I}$ l'idéal de R engendré par les P_j et $\mathcal{J}$sa trace sur l'anneau $R' = k[Y_1, \ldots, Y_n]$.
Soit maintenant $\mathcal{B}_\mathcal{I}$ la base standard réduite de $\mathcal{I}$ pour l'ordre suivant sur les monômes de R :
on compare d'abord lexicographiquement sur les X_i, puis en cas d'égalité on utilise l'ordre du degré, et enfin l'ordre lexicographique.
Soit $\mathcal{B}_\mathcal{J}$ l'ensemble des polynômes de $\mathcal{B}_\mathcal{I}$ où les X_i n'apparaissent pas.
$\mathcal{B}_\mathcal{J}$ est alors une base standard de l'idéal $\mathcal{J}$pour l'ordre du degré. De plus ses éléments sont des différences de monômes (car ceux de $\mathcal{B}_\mathcal{I}$ le sont).
Ainsi soient $Y^{\alpha_k} - Y^{\beta_k}$ les éléments de $\mathcal{B}_\mathcal{J}$, $k \in [1, p]$ et Y^{α_k} étant monôme dominant.
Maintenant, notons $\longrightarrow$ la relation de réécriture corespondant à la division des polynômnes par la base standard $\mathcal{B}_\mathcal{J}$, et $\xrightarrow{*}$ sa fermeture réflexive transitive.
On écrit $m1 \downarrow m2$ lorsque deux monômes $m1$ et $m2$ se réécrivent en un même monôme, ou de manière équivalente quand $m1 - m2 \xrightarrow{*} 0$.
Alors :

Propriété 2

$$\forall x \in Z^n \ , \ Ax = 0 \iff Y^{x^+} - Y^{x^-} \in \mathcal{I} \iff Y^{x^+} \downarrow Y^{x^-}$$

Preuve :

Facile par raisonnement équationnel sur les équations $Y_j = X^{a_j^+} X^{-a_j^-}$ dérivée des polynômes P_j, et en utilisant la proriété fondamentale des bases de Gröbner. □

En conséquence :

Propriété 3

$$\forall x \in N^n \ , \ x \in M \iff Y^x \xrightarrow{*} 1$$

Cette derniére propriété permet de tester si M est non réduit à $\{0\}$:

Théorème 4 *Le système $Ax = 0$ a une solution positive non nulle si et seulement si il existe dans $\mathcal{B}_\mathcal{I}$ un polynôme de la forme $Y^\alpha - 1$.*

On a de plus une représentation effective de M avec des règles de réécriture :
Soit SR_M le système de règles de réécriture de monômes obtenues en inversant les polynômes de $\mathcal{B}_{\mathcal{J}}$:

$$SR_M = \{Y^{\beta_1} \longrightarrow Y^{\alpha_1}, \ldots, Y^{\beta_p} \longrightarrow Y^{\alpha_p}\}$$

Notons $\longrightarrow_i$ sa relation de réécriture (c'est la symétrique de $\longrightarrow$, et elle n'est pas noethérienne).
Alors

$$x \in M \iff 1 \xrightarrow{*}_i Y^x$$

On peut donc engendrer tous les éléments de M en explorant l'arbre des réécritures de 1 par $\longrightarrow_i$, et obtenir $\mathcal{H}(M)$ en ne gardant que les éléments minimaux, et de degré inférieur aux bornes nB_2 et B_0 (cette méthode est complète car $\longrightarrow_i$ fait croître les degrés des monômes, donc les normes $\|.\|_1$ des solutions).
Plus précisément :

Théorème 5 *L'algorithme suivant s'arrête et retourne $\mathcal{H}(M)$:*

1. $E := \{1\}$
2. **Tant que** $\exists x \in E, y \notin E, avec\ x \longrightarrow_i y,\ et\ deg(y) \leq inf\{nB_2, B_0\}$

   Faire $E := E \cup \{y\}$
3. **Rendre** $\mathcal{H}(M)$:= *éléments minimaux pour $\preceq$ des vecteurs d'exposants des monômes de $E - \{1\}$.*

3.4 Comparaisons

4 Application à $Ax \leq b$

Revenons maintenant au problème initial, i.e. la résolution d'un système $Ax \leq b$. Soit C l'ensemble de ses solutions dans Z^n. Alors :

Corollaire 1 *Il existe deux parties finies C_1 et C_2 de Z^n telles que :*

$$x \in C \Leftrightarrow x = x_1 + x_2 + \ldots + x_k,\ avec\ x_1 \in C_1,\ et\ x_2, \ldots, x_k \in C_2$$

et

$$\forall x \in C_1 \cup C_2,\ \|x\|_1 \leq (2 + \|A\|_{1,\infty} + \|b\|_\infty)^r$$

Preuve :

On va se ramener à des systèmes d'équations homogènes à résoudre dans N.

Soit une ψ un endomorphisme de R^n qui ne fait que changer le signe de certaines coordonnées de son argument, et $\psi(A)$ la matrice obtenue en changeant de signe les colonnes correspondantes de A.

Soient $y = (y_1, \ldots, y_m)$ un vecteur de m nouvelles variables, z une dernière variable, t le vecteur obtenu en concaténant x, y,et z, et ϕ la projection envoyant t sur x.

Soit A' la matrice obtenue en concaténant $\psi(A)$, l'identité d'ordre m et l'opposé de b.

On a alors clairement l'équivalence :

$$Ax \leq b\ \ \psi(x) \in N^n \iff \exists t \in N^{n+m+1}, A't = 0, z = 1, x = \psi(\phi(t))$$

De plus $rang(A') = rang(A)$, et $\|A'\|_{1,\infty} \leq \|A\|_{1,\infty} + 1 + \|b\|_\infty$.

Soient $\mathcal{H}$ la base de Hilbert de $A't = 0$, et C_1^ψ (resp. C_2^ψ) l'image par ϕ des éléments de $\mathcal{H}$ tels que $z = 1$ (resp. $z = 0$).

On prend alors C_1 (resp. C_2) égal à la réunion des C_1^ψ (resp. C_2^ψ) pour les 2^n choix possibles de ψ.

Comme $\|\psi(x)\|_1 = \|x\|_1$ et $\|\phi(t)\|_1 \leq \|t\|_1$, la deuxième partie du résultat s'en suit. □

Références

[L.Baratchart et L.Pottier 89] "Un résultat sur les systèmes d'addition de vecteurs", manuscrit, INRIA Sophia Antipolis, France, fév. 1989.

[I.Borosh et L.B.Treybig 76] "Bounds of non-negative integral solutions of linear diophantine equations", Proc. AMS v.55, n.2, mars 1976.

[B.Buchberger 83] "Gröbner basis: an algorithmic method in polynomial ideal theory" Camp. Publ. Nr. 83-29. 0, nov. 1983.

[E.Contejean et H.Devie 89] "Solving systems of linear diophantine equations", UNIF'89, proc. of the third international Workshop on unification, Lambrecht, RFA 89.

[F.Giles et W.R.Pulleyblank 79] "Total dual integrality and integer polyedra" Linear algebra and its applications, 25, pp191-196, 1979.

[G.Huet 78] "An algorithm to generate the basis of solutions to homogeneous linear diophantine equations", Information Processing Letters, vol.3, No.7, 1978.

[A.Koscielski et L.Pacholski 90] "Exponent of periodicity of minimal solutions of word equations", manuscrit, Université de Wroclaw, Pologne, juin 90.

[J.L.Lambert 87] "Une borne pour les générateurs des solutions entières positives d'une équation diophantienne linéaire." Comptes Rendus de l'Académie des Sciences de Paris, t.305, Série I, pp39-40, 1987.

[J.L.Lambert 87] "Un problème d'accessibilité dans les réseaux de Petri" Thèse de doctorat, théorème I.5., p 18, Université de Paris-Sud, Orsay, 1987.

[L.Pottier 90] "Bornes et algorithmes de calcul des générateurs des solution de systèmes diophantiens linéaires", note aux Comptes Rendus de l'Académie des Sciences de Paris, septembre 1990.

[J.F.Romeuf 89] "Solutions of a linear diophantine system", UNIF'89, proc. of the third international Workshop on unification, Lambrecht, RFA 89.

[R.P.Stanley 83] "Combinatorics and commutative algebra", Progress in Mathematics, Birkäuser ed., 1983.

[L.B.Treybig 75] "Bounds in piecewise linear topology", Trans.AMS, v.201, 1975.

[J.Von zur Gathen et M.Sieveking 78] "A bound on solutions of linear integer equalities and inequalities" Proc. AMS 72, pp155-158, 1978.

Imprimé en France
par
l'Institut National de Recherche en Informatique et en Automatique

ISSN 0249-6399