Solving Systems of Linear Diophantine Equations: An Algebraic Approach *

Eric Domenjoud
CRIN & INRIA Lorraine
BP 239 F-54506 Vandœuvre-Lès-Nancy Cedex
FRANCE
e-mail domen@loria.crin.fr

Abstract

We describe through an algebraic and geometrical study, a new method for solving systems of linear diophantine equations. This approach yields an algorithm which is intrinsically parallel. In addition to the algorithm, we give a geometrical interpretation of the satisfiability of an homogeneous system, as well as upper bounds on height and length of all minimal solutions of such a system. We also show how our results apply to inhomogeneous systems yielding necessary conditions for satisfiability and upper bounds on the minimal solutions.

Solving linear diophantine equations is a problem which appears in many fields, from linear programming to resolution of equations in semigroups or constrained logic programming. In the framework of semigroups, one needs an efficient test for the satisfiability of equations as well as a way to generate a basis for the set of all solutions. The efficiency of the satisfiability test becomes crucial in constrained equational logic because constraints are accumulated until their conjunction becomes unsatisfiable. The simplex method is quite convenient for checking the satisfiability of a set of homogeneous equations, but does not provide an algorithm for finding all solutions. Such algorithms were proposed by G. Huet [9], A. Fortenbacher [6], A. Herold & T. Guckenbiehl [8], M. Clausen & A. Fortenbacher [4] for one equation. In 1987, J.-L. Lambert [10] gave an upper bound on the components of all minimal solutions of a system, and a finer one on the length of minimal solutions of one equation, improving then greatly Huet's algorithm. In 1989, J.-F. Romeuf [14] described an algorithm for solving two equations, using a finite automaton recognizing the solutions. Definite improvements were then brought in 1989 by E. Contejean and H. Devie [5, 2] who found an extension of Fortenbacher's algorithm to systems of arbitrary size, and L. Pottier who described in [11] a similar algorithm and gave a new upper bound on the length of all minimal solutions of a system. Very recently, L. Pottier gave in [12] another algorithm using Gröbner bases and improved the upper bounds on the minimal solutions.

*This work was partly supported by the GRECO de programmation (CNRS)

Our approach and L. Pottier's one, seem to be the first attempts to find the solutions from algebraic considerations only. These two approaches are however completely different. All other algorithms have in common to implicitly or explicitly increase vectors starting from $\vec{0}$, until a solution or a failure is reached. On the contrary, our algorithm computes directly a finite set of solutions containing all minimal ones. This makes our algorithm very easy to parallelize because no comparison between solutions is needed until the very last step.

The paper is organized as follows. In section 1, we give our main definitions and notations, and two theorems used in all the rest of the paper. In particular, we show that the diophantine system $A^1x_1 + \cdots + A^nx_n = \vec{0}$ is satisfiable if and only if the convex hull of $\{A^1, \ldots, A^n\}$ contains $\vec{0}$. In sections 2 and 3, we describe how we get a basis of the set of solutions of this system by generating first an integer basis of its real positive solutions. In section 4, we give upper bounds on the length and the height of all minimal solutions and we show in section 5 how our results apply to inhomogeneous systems $A^1x_1 + \cdots + A^nx_n = C$. All these results have been first presented at the fourth international workshop on unification held in Leeds (UK) in July 1990.

1 Preliminaries

$\boldsymbol{N}$, $\boldsymbol{Z}$, $\boldsymbol{Q}$ and $\boldsymbol{R}$ denote respectively the set of natural, integer, rational and real numbers. If $X \in \boldsymbol{R}^n$, $\|X\|_1 = \sum_{i=1}^n |x_i|$ is its length, and $\|X\|_\infty = \max |x_i|$ is its height. The carrier of X is the set of indexes of its nonzero components. If V and W are vectors, $V \geq W$ iff $\forall i : v_i \geq w_i$, $V > W$ iff $V \geq W$ and $V \neq W$, $V \gg W$ iff $\forall i : v_i > w_i$. The null vector of $\boldsymbol{R}^n$ will be denoted by $\vec{0}_n$ or simply $\vec{0}$ if no ambiguity arises. For a matrix A, A^j is its j^{th} column and if A is a $n \times n$ matrix, $|A|$ is its determinant and A is unimodular iff $|A| = \pm 1$. A and B are similar, written $A \sim B$, if there exists an integer unimodular matrix U such that $UA = B$. A linear diophantine system is an equation $AX = C, X \in \boldsymbol{N}^n$ where A is an $m \times n$ integer matrix and $C \in \boldsymbol{Z}^m$. If $C = \vec{0}$, the diophantine system is homogeneous, otherwise it is inhomogeneous. A solution S of this system is minimal if $S \neq \vec{0}$ and there does not exist a nonzero solution $S' < S$. If V is a set of vectors, card(V) is its cardinality and Conv(V) its convex hull. If $V = \{V_1, \ldots, V_k\}$, we write Conv$(V_1, \ldots, V_k)$ instead of Conv$(\{V_1, \ldots, V_k\})$.

$$\mathrm{Conv}(V_1, \ldots, V_k) = \{\lambda_1 V_1 + \cdots + \lambda_k V_k \mid \forall i : \lambda_i \geq 0 \text{ and } \sum_{j=1}^{k} \lambda_j = 1\}$$

At last, if A is an $(n-1) \times n$ matrix and e is the canonical basis of $\boldsymbol{R}^n$, $\begin{vmatrix} e \\ A \end{vmatrix}$ is the vector product of A's rows.

In the sequel, we shall use the following two theorems.

Theorem 1 (Carathéodory) *Let V be a subset of $\boldsymbol{R}^m$.*

$$\mathrm{Conv}(V) = \bigcup_{\substack{V' \subset V \\ \mathrm{card}(V') \leq m+1}} \mathrm{Conv}(V')$$

The proof of this theorem may be found in [3]. We shall actually use the following two corollaries of this theorem:

Corollary 1 *Let V be a subset of $\boldsymbol{R}^m$, the convex hull of which contains X. Then there exists $V' \subset V$ such that* $\mathrm{card}(V') \leq m+1$ *and* $X \in \mathrm{Conv}(V')$.

Corollary 2 *If $\vec{0} \in \mathrm{Conv}(V)$ and for all strict subsets V' of V, $\vec{0} \notin \mathrm{Conv}(V')$, then V has rank* $\mathrm{card}(V) - 1$.

Proof: There exists an isomorphism ϕ from the vector space spanned by V to $\boldsymbol{R}^k$, where k is the rank of V. Since $\mathrm{Conv}(\phi(V)) = \phi(\mathrm{Conv}(V))$, $\vec{0}_k \in \mathrm{Conv}(\phi(V))$. Now from corollary 1, there exist $V_1, \ldots, V_{k+1}$ in V such that $\vec{0}_k \in Conv(\phi(V_1), \ldots, \phi(V_{k+1}))$. Hence, $\vec{0}_m \in \mathrm{Conv}(V_1, \ldots, V_{k+1})$ and $k+1 = \mathrm{card}(V)$ otherwise, $\{V_1, \ldots, V_{k+1}\}$ is a strict subset of V, the convex hull of which contains $\vec{0}_m$. □

Theorem 2 *If A is an $m \times n$ integer matrix, the diophantine system $AX = \vec{0}, X \in \boldsymbol{N}^n$ has a nonzero solution iff $\vec{0} \in \mathrm{Conv}(A^1, \ldots, A^n)$.*

Proof:

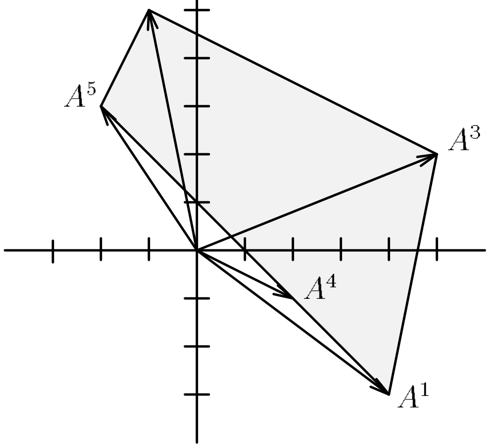
$\boxed{\Rightarrow}$ If $X \in \boldsymbol{N}^n - \{\vec{0}\}$ and $AX = \vec{0}$ then $\frac{x_i}{\|X\|_1} \geq 0$, $\left\| \frac{X}{\|X\|_1} \right\|_1 = 1$ and $A\frac{X}{\|X\|_1} = \vec{0}$. Hence $\vec{0} \in \mathrm{Conv}(A^1, \ldots, A^n)$

$\boxed{\Leftarrow}$ From corollaries of theorem 1, there exists $\{A^{i_1}, \ldots, A^{i_k}\} \subset \{A^1, \ldots, A^n\}$, the convex hull of which contains $\vec{0}$ and rank is $k-1 \leq m$. There exists then an $m \times m$ integer unimodular matrix U such that $U[A^{i_1} \cdots A^{i_k}] = \begin{bmatrix} M \\ 0 \end{bmatrix}$ where M has $k-1$ rows and rank $k-1$. The kernel of M is thus spanned by one vector. Since $\vec{0} \in \mathrm{Conv}(A^{i_1}, \ldots, A^{i_k})$, there exists a nonzero positive solution of $MY = \vec{0}$ and thus all components of any solution of $MY = \vec{0}$ have the same sign. Now, $S = (|M^{i_2} \cdots M^{i_k}|, \ldots, (-1)^{k-1}|M^{i_1} \cdots M^{i_{k-1}}|)$ is an integer solution of $MY = \vec{0}$ which is not zero because the rank of M is $k-1$. Thus, S or $-S$ is a nonzero solution of $MY = \vec{0}, Y \in \boldsymbol{N}^k$ and $S' = s_1 e^{i_1} + \cdots + s_k e^{i_k}$ or $-S'$, where $e = (e^1, \ldots, e^m)$ is the canonical basis of $\boldsymbol{R}^m$, is a nonzero solution of $AX = \vec{0}, X \in \boldsymbol{N}^m$. □

Example 1 *The homogeneous diophantine system, the matrix of which is*

$$A = \begin{bmatrix} 4 & -1 & 5 & 2 & -2 \\ -3 & 5 & 2 & -1 & 3 \end{bmatrix}$$

has no nonzero solution because $\vec{0} \notin \mathrm{Conv}(A^1, \ldots, A^5)$.



2 Basis of the set of positive solutions of $AX = \vec{0}$

From now on, A is an $m \times n$ integer matrix with rank m and $n \geq m+1$, and $\mathcal{A}$ denotes the set $\{A^1, \ldots, A^n\}$. Let $P_0(A)$ be the set of subsets of $\mathcal{A}$, the convex hull of which contains $\vec{0}$ and which are minimal with respect to the inclusion. For each $E = \{A^{i_1}, \ldots, A^{i_k}\} \in P_0(A)$, from the proof of theorem 2, $[A^{i_1} \cdots A^{i_k}]X = \vec{0}, X \in \boldsymbol{N}^k$ has a unique minimal solution $(x_1, \ldots, x_k)$. Let then $S^{(E)}$ be the vector $x_1 e^{i_1} + \cdots + x_k e^{i_k}$ where e is the canonical basis of $\boldsymbol{R}^n$, and $S_0(A)$ be $\{S^{(E)} \mid E \in P_0(A)\}$. The elements of $S_0(A)$ are known as the minimal solutions with minimal carrier. The following theorem is a refinement of a classical result which may be found in [10]:

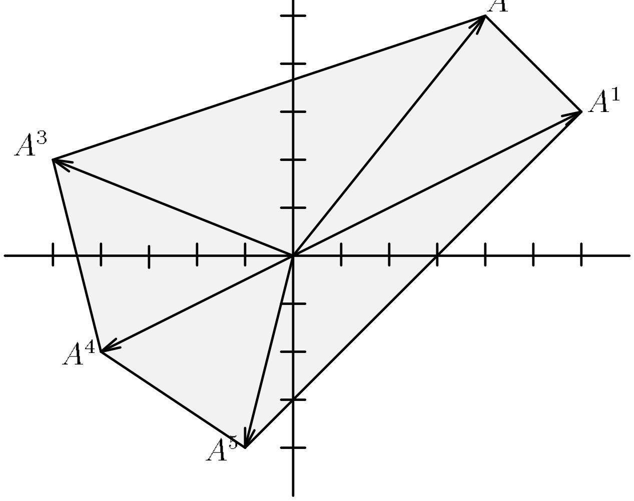
Theorem 3 *Every positive solution of $AX = \vec{0}$ is a linear combination with positive coefficients of linearly independent vectors in $S_0(A)$.*

Proof: By induction on the carrier of a solution. The theorem obviously holds for every positive solution, the carrier of which is minimal. Now, let X be a positive solution of $AX = \vec{0}$, the carrier of which is not minimal, and let us assume that the theorem holds for any vector, the carrier of which is strictly contained in X's one. $S_0(A)$ contains a vector S, the carrier of which is contained in X's one, and $X' = X - \lambda S$ where $\lambda = \min\{\frac{x_i}{s_i} \mid s_i \neq 0\}$, is again a positive solution of $AX = \vec{0}$. Since the carrier of X' is strictly contained in X's one, by the induction hypothesis, $X' = \sum \lambda_i S_i$ where λ_i's are positive and S_i's are linearly independent vectors of $S_0(A)$. X is then equal to $\lambda S + \sum \lambda_i S_i$. S and S_i's are linearly independent because at least one component of S is zero in all S_i's. □

One may note that if X is rational, so is the coefficient λ constructed in the proof. Thus every positive solution of $AX = \vec{0}, X \in \boldsymbol{Q}^n$ is a linear combination with positive rational coefficients of linearly independent vectors in $S_0(A)$.

Example 2 *Consider the matrix*

$$A = \begin{bmatrix} 6 & 4 & -5 & -4 & -1 \\ 3 & 5 & 2 & -2 & -4 \end{bmatrix}$$



Since Conv$(\mathcal{A})$ *contains* $\vec{0}$*, the system* $AX = \vec{0}, X \in \boldsymbol{N}^n$ *has a nonzero solution. In this case,*

$$P_0(A) = \{\{A^1, A^4\}, \{A^1, A^3, A^5\}, \{A^2, A^3, A^5\}, \{A^2, A^4, A^5\}\}$$

and

$$S_0(A) = \{(2,0,0,3,0), (22,0,21,0,27), (0,2,1,0,3), (0,14,0,11,12)\}$$

There is actually no need for looking for $P_0(A)$. The simplex algorithm gives a way to compute $S_0(A)$. We give here another way:

Theorem 4 *If* $S^{(E)} \in S_0(A)$*, there exists* $\{A^{i_1}, \ldots, A^{i_{m+1}}\} \subset \mathcal{A}$ *such that*

$$\begin{vmatrix} e^{i_1} \cdots e^{i_{m+1}} \\ A^{i_1} \cdots A^{i_{m+1}} \end{vmatrix} = K \cdot S^{(E)}$$

where K *is a nonzero integer.*

Proof: $E = \{A^{i_1}, \ldots, A^{i_k}\}$ and from corollary 2 of theorem 1, E has rank $k-1$. we get then

$$[A^{i_1} \cdots A^{i_k}] \sim \begin{bmatrix} B^{i_1} \cdots B^{i_k} \\ 0 \ \cdots \ 0 \end{bmatrix} \}k-1 \qquad \text{and} \quad \begin{vmatrix} e^{i_1} \cdots e^{i_k} \\ B^{i_1} \cdots B^{i_k} \end{vmatrix} = K_1 \cdot S^{(E)}$$

Since A has rank m, we may find $A^{i_{k+1}}, \ldots, A^{i_{m+1}}$ such that $\{A^{i_1} \cdots A^{i_{m+1}}\}$ has rank m. We get then

$$\begin{vmatrix} e^{i_1} \cdots e^{i_{m+1}} \\ A^{i_1} \cdots A^{i_{m+1}} \end{vmatrix} = \begin{vmatrix} e^{i_1} \cdots e^{i_k} & e^{i_{k+1}} \cdots e^{i_{m+1}} \\ B^{i_1} \cdots B^{i_k} & R \\ 0 \ \cdots \ 0 & U \end{vmatrix} = |U| \cdot \begin{vmatrix} e^{i_1} \cdots e^{i_k} \\ B^{i_1} \cdots B^{i_k} \end{vmatrix} = |U| \cdot K_1 \cdot S^{(E)}$$

□

We compute then $S_0(A)$ as follows: for each subset $\{A^{i_1}, \ldots, A^{i_{m+1}}\}$ of $\mathcal{A}$, we compute the determinant $\begin{vmatrix} e^{i_1} \cdots e^{i_{m+1}} \\ A^{i_1} \cdots A^{i_{m+1}} \end{vmatrix}$. If it is a nonzero vector, all components of which have the same sign, we divide it by the greatest common divisor of its components and we get a vector in $S_0(A)$. Furthermore, from theorem 4, we get all vectors in $S_0(A)$ in this way.

3 Minimal solutions of $AX = \vec{0}, X \in N^n$

Theorem 5 *Vectors in $S_0(A)$ are minimal solutions of $AX = \vec{0}, X \in \boldsymbol{N}^n$.*

Proof: follows immediately from minimality of subsets in $P_0(A)$ and corollary 2. □

We saw in section 2 that every solution of $AX = \vec{0}, X \in \boldsymbol{N}^n$ is a combination with positive rational coefficients of linearly independent vectors in $S_0(A)$. Let M be a matrix the columns of which are k linearly independent vectors in $S_0(A)$. The problem is now to find all $\alpha \in (\boldsymbol{Q}^+)^k$ such that $M\alpha$ is an integer vector. There exists an integer unimodular matrix U such that $UM = \begin{bmatrix} T \\ 0 \end{bmatrix}$ where T is an upper triangular matrix with positive entries on the diagonal. Now, $M\alpha$ is integer iff $T\alpha$ is, that is to say, iff $\alpha = T^{-1}X$ where X is an integer vector. Since we are only interested in minimal solutions, we may consider only the case $0 \leq \alpha_i < 1$ for all i. Indeed we are only interested in the case $0 \leq \alpha_i$ for all i, and if $\alpha_i \geq 1$ for some i then $M\alpha \geq M^i$ which is a minimal solution we already have. For this purpose, we take $\alpha = T^{-1}X - \lfloor T^{-1}X \rfloor = \frac{1}{d}[dT^{-1}X]_d$ where d is the determinant of T, $\lfloor x \rfloor$ denotes the floor value of x and $[n]_d$ denotes the smallest positive integer congruent with n modulo d. The following theorem allows us to cut down the search space for convenient X.

Theorem 6 *If $D = (d_1, \ldots, d_k)$ is the diagonal of T and $d = d_1 \cdots d_k$ is its determinant, then:*

$$\forall X \in \boldsymbol{Z}^k : \exists X' \in \boldsymbol{Z}^k : \vec{0} \leq X' \ll D \text{ and } [dT^{-1}X']_d = [dT^{-1}X]_d$$

Proof: For all i, and all X,

$$\begin{aligned} dT^{-1}X &= dT^{-1}(X - Te^i + Te^i) \\ &= dT^{-1}(X - Te^i) + de^i \\ &\equiv dT^{-1}(X - Te^i) \pmod{d} \end{aligned}$$

$X - Te^i$ is an integer vector such that $\forall j > i : (X - Te^i)_j = X_j$ and $(X - Te^i)_i = X_i - d_i$. This proves the result. □

Example 3 (Example 2 continued)
$S_0(A) = \{(2,0,0,3,0), (22,0,21,0,27), (0,2,1,0,3), (0,14,0,11,12)\}$

$$M = \begin{bmatrix} 2 & 0 & 22 \\ 0 & 2 & 0 \\ 0 & 1 & 21 \\ 3 & 0 & 0 \\ 0 & 3 & 27 \end{bmatrix} \sim \begin{bmatrix} 1 & 0 & -4 \\ 0 & 1 & -3 \\ 0 & 0 & 6 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} \quad \text{and} \quad 6 \begin{bmatrix} 1 & 0 & -4 \\ 0 & 1 & -3 \\ 0 & 0 & 6 \end{bmatrix}^{-1} = \begin{bmatrix} 6 & 0 & 4 \\ 0 & 6 & 3 \\ 0 & 0 & 1 \end{bmatrix}$$

and we get $\alpha = \frac{1}{6}([6x_1 + 4x_3]_6, [6x_2 + 3k_3]_6, [x_3]_6) = \frac{1}{6}([4x_3]_6, [3k_3]_6, [x_3]_6)$ with $1 \leq x_3 \leq 6$. The table below contains for each value of k_3, the value of α and the corresponding solution *of* $AX = \vec{0}$.

k_3	6α	solution
1	$(4,3,1)$	$(5,1,4,2,6)$
2	$(2,0,2)$	$(8,0,7,1,9)$
3	$(0,3,3)$	$(11,1,11,0,15)$
4	$(4,0,4)$	$(16,0,14,2,18)$
5	$(2,3,5)$	$(19,1,18,1,24)$

4 Bounds on minimal solutions of $AX = \vec{0}, X \in N^n$

We prove now two bounds on minimal solutions of an homogeneous diophantine system. The former one bounds each component of a minimal solution while the latter one bounds its length.

Theorem 7 *Let $\mathcal{M}$, and $\mathcal{M}'$ be upper bounds on absolute values of $m \times m$ subdeterminants of A, and $(m+1) \times (m+1)$ subdeterminants of $\begin{bmatrix} 1 \cdots 1 \\ A^1 \cdots A^n \end{bmatrix}$ respectively. Then for any minimal solution S of $AX = \vec{0}, X \in \mathbf{N}^n$:*

1. $\|S\|_\infty \leq (n-m)\mathcal{M}$
2. $\|S\|_1 \leq (n-m)\mathcal{M}'$

Proof: We saw that every minimal solution is a combination with coefficients between 0 and 1 of vectors in $S_0(A)$. But $S_0(A)$ contains at most $n-m$ linearly independent vectors because it is the dimension of the kernel of A. Thus, each component of a minimal solution is bounded by $n-m$ times the maximum of a component of a vector in $S_0(A)$ and analogously, the length of a minimal solution is bounded by $n-m$ times the maximal length of a vector in $S_0(A)$. Now, we saw in section 2 that for any vector $S \in S_0(A)$, $S = \frac{1}{K}\begin{vmatrix} e^{i_1} \cdots e^{i_{m+1}} \\ A^{i_1} \cdots A^{i_{m+1}} \end{vmatrix}$ for some $A^{i_1}, \ldots, A^{i_{m+1}}$ and some nonzero integer K. Thus any component of S is bounded by a determinant $|A^{j_1} \cdots A^{j_m}|$ and the length of S is bounded by the absolute value of $\begin{vmatrix} 1 \cdots 1 \\ A^{i_1} \cdots A^{i_{m+1}} \end{vmatrix}$.
□

Bounds similar to 1 were already proved by I. Borosch & L.B. Treybig [1] and J. von zur Gathen and M. Sieveking [7] for the components of the smallest solution, and by J.-L. Lambert [10] for the components of all minimal solutions. Our bound is a slight improvement of Lambert's one, and was also discovered independently by L. Pottier [12]. On the other hand, our bound on the length of minimal solutions compares favorably with previous ones. L. Pottier gave in [11] a bound which is, in any case, much larger than ours and in [12] he proved that the length of minimal solutions is bounded by $(1+\max\|A_i\|_1)^m$ which is also in general greater than our bound. At last, J.-F. Romeuf [13] gave $(2a)^{2^m-1}$ as an upper bound, which is interesting since it does not depend on the number of variables but is doubly exponential and thus grows very fast. We conjecture that our bounds hold without the factor $n-m$, but we have no proof for this. I. Borosch & L.B. Treybig gave one, but only for the minimal solutions of an inhomogeneous system when the associated homogeneous system has no nonzero solution. From the proof of theorem 7, we see that these bounds would be sharp. Furthermore, the very sharp bound Lambert gave on the length of minimal solutions of one equation would become an instance of this one.

5 Inhomogeneous diophantine systems

The inhomogeneous case is a bit more complicated than the homogeneous one. Indeed, we are unable to find necessary and sufficient conditions for the satisfiability of such a system over natural numbers. However, we give here necessary conditions which are not sufficient and sufficient conditions which are not necessary.

Theorem 8 *The inhomogeneous diophantine system $AX = C, X \in \boldsymbol{N}^n$ has a solution only if $AX = C, X \in \boldsymbol{Z}^n$ has a solution and there exists a natural l such that $\frac{1}{l}C \in \mathrm{Conv}(A^1, \ldots, A^n)$.*

If $AX = C, X \in \boldsymbol{Z}^n$ has a solution and for all i, $AX = \vec{0}, X \in \boldsymbol{N}^n$ has a solution such that $x_i \neq 0$, then $AX = C, X \in \boldsymbol{N}^n$ has a solution.

Proof: It is obvious that $AX = C, X \in \boldsymbol{Z}^n$ has a solution if $AX = C, X \in \boldsymbol{N}^n$ has one. Now let S be a solution of $AX = C, X \in \boldsymbol{N}^n$. Then $A\frac{S}{\|S\|_1} = \frac{1}{\|S\|_1}C$ and $\frac{1}{\|S\|_1}C \in \mathrm{Conv}(A^1, \ldots, A^n)$ because $\left\|\frac{S}{\|S\|_1}\right\|_1 = 1$. This proves the first part of the theorem.

For the second part, let S be a solution of $AX = C, X \in \boldsymbol{Z}^n$. For each component s_i which is negative, we add to S a solution S' of $AX = 0, X \in \boldsymbol{N}^n$ such that $s'_i \neq 0$, until the component becomes positive. We get then a solution of $AX = C, X \in \boldsymbol{N}^n$. □

One may note that the satisfiability over integers is very easy to check. Let k be the rank of A. There exist then two unimodular integer matrices L and R such that $LAR = \begin{bmatrix} D & 0 \\ 0 & 0 \end{bmatrix}$ where D is an $k \times k$ diagonal matrix and 0's stand for null matrices of suitable size (maybe 0). Any solution X is then of the form RY where Y is a solution of $\begin{bmatrix} D & 0 \\ 0 & 0 \end{bmatrix} Y = LC$. Checking the satisfiability of this last system is then straightforward.

To solve an inhomogeneous system, we add a variable x_{n+1}, solve the homogeneous system $[A\ -C]\begin{bmatrix} X \\ x_{n+1} \end{bmatrix} = \vec{0}$, and keep only solutions which satisfy $x_{n+1} \leq 1$. If $x_{n+1} = 0$ then X is a solution of the homogeneous system $AX = \vec{0}$, otherwise, X is a solution of the inhomogeneous system $AX = C$. Any solution of the inhomogeneous system is then of the form $X_0 + X_1$ where X_0 is a basic solution of $AX = C$ and X_1 is any linear combination with natural coefficients of solutions of $AX = \vec{0}$. We get then bounds on the solutions by applying theorem 7 to the homogeneous system $[A\ -C]\begin{bmatrix} X \\ x_{n+1} \end{bmatrix}$.

6 Conclusion

Our approach of linear diophantine equations is interesting for various reasons. First of all, it provides a geometrical interpretation of the satisfiability of a system and yields upper bounds on minimal solutions that are sharper than previous ones. From a more practical point of view, let us first notice that our algorithm may compare favorably with E. Contejean & H. Devie's one. The table below displays for some homogeneous systems, the matrix of the system, the number of minimal solutions, the computation time in seconds for our algorithm and for theirs. These comparisons are performed by a program written in the C programming language, running on a SUN 4/390 workstation.

1	$\begin{bmatrix} 1 & 2 & -3 & -2 & -4 \\ 2 & -1 & -3 & 2 & 5 \end{bmatrix}$	10	0.0035	0.0248
2	$\begin{bmatrix} 10 & -7 & -8 & 3 & -11 \\ 12 & -9 & -7 & 3 & 13 \end{bmatrix}$	240	0.7850	9.925
3	$\begin{bmatrix} 1 & 2 & -1 & 0 & -2 & -1 \\ 0 & -1 & -2 & 2 & 0 & 1 \\ 2 & 0 & 1 & -1 & -2 & 0 \end{bmatrix}$	13	0.0278	0.0740
4	$\begin{bmatrix} -10 & 0 & 20 & -1 & -21 \\ 9 & 1 & -17 & 2 & 19 \end{bmatrix}$	0	0.0013	15.94

The most interesting features of our algorithm are:

1. It is intrinsically parallel at various levels and could thus run much more quickly on a parallel machine. This did not hold for E. Contejean and H. Devie's algorithm. Indeed, the computation of $S_0(A)$ may be easily parallelized as well as the computation of all minimal solutions from $S_0(A)$ because our algorithm does not perform any comparison between the solutions until all have been computed.

2. Large solutions are found as easily as small ones. This fact is very interesting because algorithms which find solutions by increasing a vector one coordinate at a time are practically unable to find very large solutions.

3. It fails quickly when a system has no solution. This is demonstrated by example 4 above.

References

[1] I. Borosh and L. B. Treybig. Bounds on positive integral solutions of linear diophantine equations. *Proceedings of the American Mathematical Society*, 55:299–304, 1976.

[2] A. Boudet, E. Contejean, and H. Devie. A new AC unification algorithm with a new algorithm for solving diophantine equations. In *Proceedings 5th IEEE Symposium on Logic in Computer Science, Philadelphia (Pennsylvania, USA)*, pages 289–299, 1990.

[3] A. Brøndsted. *An Introduction to Convex Polytopes*, volume 90 of *Graduate Texts in Mathematics*. Springer-Verlag, 1983.

[4] M. Clausen and A. Fortenbacher. Efficient solution of linear diophantine equations. *Journal of Symbolic Computation*, 8:201–216, 1989. Special issue on unification. Part two.

[5] E. Contejean and H. Devie. Solving systems of linear diophantine equations. In H.-J. Bürckert and W. Nutt, editors, *Proceedings 3rd International Workshop on Unification, Lambrecht (Germany)*, 1989.

[6] A Fortenbacher. Algebraische unifikation. Diplomarbeit, Institut für Informatik, Universität Karlsruhe, 1983.

[7] J. von zur Gathen and M. Sieveking. A bound on solutions of linear integer equalities and inequalities. *Proceedings of the American Mathematical Society*, 72:155–158, 1978.

[8] T. Guckenbiehl and A. Herold. Solving linear diophantine equations. Technical Report SEKI-85-IV-KL, Universität Kaiserslautern, 1985.

[9] G. Huet. An algorithm to generate the basis of solutions to homogenous linear diophantine equations. *Information Processing Letters*, 7:144–147, 1978.

[10] J.-L. Lambert. *Le problème de l'accessibilité dans les réseaux de Petri.* PhD thesis, Université de Paris-sud, Centre d'Orsay, 1987.

[11] L. Pottier. Bornes et algorithme de calcul des générateurs des solutions de systèmes diophantiens linéaires. Technical report, INRIA Sophia Antipolis, 1990.

[12] L. Pottier. Minimal solutions of linear diophantine systems: Bounds and algorithms. In R.V. Book, editor, *Proceedings 4th Conference on Rewriting Techniques and Applications, Como, (Italy)*, volume 488 of *Lecture Notes in Computer Science*, pages 162–173. Springer-Verlag, 1991.

[13] J.-F. Romeuf. Solutions of a linear diophantine system, 1988. LIR & Université de Rouen.

[14] J.-F. Romeuf. A polynomial algorithm for solving systems of two linear diophantine equations. Technical report, Laboratoire d'Informatique de Rouen (France) and LITP, 1989.