Solving Linear Diophantine Equations Using the Geometric Structure of the Solution Space

Ana Paula Tomás and Miguel Filgueiras

LIACC, Universidade do Porto, Portugal
email: {apt,mig}@ncc.up.pt

Abstract. In the development of algorithms for finding the minimal solutions of systems of linear Diophantine equations, little use has been made (to our knowledge) of the results by Stanley using the geometric properties of the solution space. Building upon these results, we present a new algorithm, and we suggest the use of geometric properties of the solution space in finding bounds for searching solutions and in having a qualitative evaluation of the difficulty in solving a given system.

1 Introduction

The problem of finding the set of the minimal solutions of the monoid of nonnegative integral solutions of (1), also called Hilbert Basis,

$$AX = 0, \quad A \text{ a } m \times n \text{ integral matrix}, \tag{1}$$

has been investigated by Elliott [4] and MacMahon [9] in the beginning of this century, and more recently by several other researchers ([7, 8, 2, 1, 12, 10, 3, 6, 5]) when it was found to be related to areas such as AC-unification, word problems, or combinatorics.

In terms of the development of algorithms for solving this problem, little use has been made (to our knowledge) of the results by Stanley using the geometric properties of the solution space [14, 15], in particular, his characterization of the generating function of the solutions monoid.

Building upon these results, we present a new algorithm, which is a reformulation of the Slopes Algorithm we described previously for solving a single equation [6], and we suggest the use of geometric properties of the solution space in finding bounds for searching solutions and in having a qualitative evaluation of the difficulty in solving a given system. We also note that, as a direct consequence of Stanley's results, the algorithm by Domenjoud [3] can be improved.

2 Triangulating the Cone of Nonnegative Real Solutions

The set of nonnegative real solutions of a system of linear homogeneous Diophantine equations is a pointed convex polyhedral cone, to which we shall refer as *the solution cone*. The main definitions and results about polyhedral convex cones may be found for instance in [13]. We briefly recall those that are needed

in the sequel. In the real Euclidean space $\mathbb{R}^n$, any set $\mathcal{C}$ which is the intersection of finitely many linear half-spaces is called a convex polyhedral cone. A cone $\mathcal{C}$ is said to be pointed if for all nonnull $v \in \mathcal{C}$, $-v \notin \mathcal{C}$. It is known that each pointed convex polyhedral cone is the convex hull of its extremal rays, which are finitely many. Extremal rays are the 1-dimensional faces of $\mathcal{C}$, each *face* being the intersection of $\mathcal{C}$ with some hyperplane $\mathcal{H}$ such that $\mathcal{C}$ lies entirely on one of the half-spaces determined by $\mathcal{H}$. The dimension of a face $\mathcal{F}$, denoted by $\dim \mathcal{F}$, is the dimension of the linear subspace of $\mathbb{R}^n$ spanned by $\mathcal{F}$. If $\mathcal{C}$ is p-dimensional, then any $p-1$ dimensional face of $\mathcal{C}$ is called a facet. The set of faces, including the improper face $\mathcal{C}$, ordered by inclusion is a lattice, so-called the face lattice. Given $x = (x_1, \ldots, x_n) \in \mathbb{R}^n$, the x_i's being the coordinates of x wrt the canonical basis of $\mathbb{R}^n$, the support of x, denoted by $\operatorname{supp} x$, is $\{i \mid x_i \neq 0\}$. If $X \subseteq \mathbb{R}^n$, then by definition $\operatorname{supp} X = \cup_{x \in X} \operatorname{supp} x$. The face lattice and the lattice of the supports of the faces of the cone of real nonnegative solutions of a system of linear homogeneous Diophantine equations are isomorphic, each extremal ray being defined by a minimal nonnegative integral solution of minimal[1] support. Moreover, each minimal solution of minimal support is the minimum positive integral solution of some subsystem of the given system, having at most $m+1$ nonnull components, where m is the rank of the system matrix. Without loss of generality, the matrix may certainly be assumed of full row rank. There are other methods to compute such minimal solutions, for instance by relating them to the vertices of the polytope obtained by intersecting $\mathcal{C}$ with the hyperplane $\sum_{i=1}^{n} x_i = 1$. Some bibliographical references to methods for enumerating the vertices of a polytope, based on the Simplex algorithm, may be found in [13].

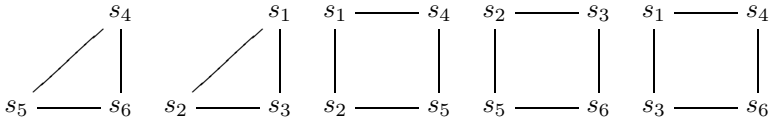
Example 1 The system $AX = 0$ where

$$A = \begin{bmatrix} 3 & -1 & 0 & -2 & 3 & -2 & -1 & -3 \\ 2 & -2 & 0 & 0 & 2 & 1 & -2 & -1 \\ 1 & 1 & 1 & -3 & 3 & 2 & -3 & 0 \\ 0 & 0 & -1 & 0 & 0 & 2 & 3 & 0 \end{bmatrix}$$

has 6 minimal solutions of minimal support, namely

$$\begin{array}{ll} s_1 = (\ 1\ \ 2\ 0\ 2\ 1\ 0\ 0\ 0\ ) & s_4 = (\ 0\ 0\ \ 3\ \ 1\ 1\ 0\ 1\ \ 0\ ) \\ s_2 = (\ 33\ 35\ 8\ 28\ 0\ 4\ 0\ 0\ ) & s_5 = (\ 31\ 0\ 121\ 21\ 0\ 8\ 35\ 0\ ) \\ s_3 = (\ 13\ 11\ 0\ \ 8\ \ 0\ 0\ 0\ 4\ ) & s_6 = (\ 15\ 0\ \ 33\ \ \ 5\ \ 0\ 0\ 11\ 8\ ) \end{array}$$

which determine a 4-dimensional solution cone. The cone has five facets, two of which are 3-dimensional simplicial cones, their cross-sections being represented schematically as follows.



[1] Not taking $\emptyset$ into account.

The faces and their supports are the following.

4-dimensional face (solution cone)
$\{1,2,3,4,5,6,7,8\}$: $cone\{s_1, s_2, s_3, s_4, s_5, s_6\}$
3-dimensional faces (facets)
$\{1,3,4,5,6,7,8\}$: $cone\{s_4, s_5, s_6\}$ $\{1,2,3,4,6,7,8\}$: $cone\{s_2, s_3, s_5, s_6\}$
$\{1,2,3,4,5,6,8\}$: $cone\{s_1, s_2, s_3\}$ $\{1,2,3,4,5,7,8\}$: $cone\{s_1, s_3, s_4, s_6\}$
$\{1,2,3,4,5,6,7\}$: $cone\{s_1, s_2, s_4, s_5\}$
2-dimensional faces
$\{1,3,4,6,7,8\}$: $cone\{s_5, s_6\}$ $\{1,3,4,5,7,8\}$: $cone\{s_4, s_6\}$
$\{1,2,3,4,7,8\}$: $cone\{s_3, s_6\}$ $\{1,3,4,5,6,7\}$: $cone\{s_4, s_5\}$
$\{1,2,3,4,6,7\}$: $cone\{s_2, s_5\}$ $\{1,2,3,4,5,7\}$: $cone\{s_1, s_4\}$
$\{1,2,3,4,6,8\}$: $cone\{s_2, s_3\}$ $\{1,2,4,5,8\}$: $cone\{s_1, s_3\}$
$\{1,2,3,4,5,6\}$: $cone\{s_1, s_2\}$
1-dimensional faces (extremal rays)
$\{1,2,4,5\}$: $cone\{s_1\}$ $\{1,2,3,4,6\}$: $cone\{s_2\}$
$\{1,2,4,8\}$: $cone\{s_3\}$ $\{3,4,5,7\}$: $cone\{s_4\}$
$\{1,3,4,6,7\}$: $cone\{s_5\}$ $\{1,3,4,7,8\}$: $cone\{s_6\}$

A *simplicial* cone is a p-dimensional cone with p extremal rays, that is whose extremal rays are linearly independent. The cone generated by $\mathtt{r}_1, \ldots, \mathtt{r}_k \in \mathbb{R}^n$, say $cone\{\mathtt{r}_1, \ldots, \mathtt{r}_k\}$, is given by $cone\{\mathtt{r}_1, \ldots, \mathtt{r}_k\} = \{\sum_{i=1}^{k} \alpha_i \mathtt{r}_i \mid \alpha_i \geq 0\}$. We call a finite set $\Gamma = \{\sigma_1, \ldots, \sigma_t\}$ of simplicial cones a *triangulation* of $\mathcal{C}$ if $\mathcal{C} = \cup\sigma_i$ and the intersection $\sigma_i \cap \sigma_j$ of σ_i and σ_j, is a common face of σ_i and σ_j. This definition differs from that given by Stanley in [15], which requires in addition that every face of σ_i is also in Γ, for all i.

A relevant result about triangulations of pointed convex polyhedral cones, which does not hold for general polyhedra, may be found in [15], and asserts that *"a pointed convex polyhedral cone $\mathcal{C}$ possesses a triangulation Γ whose extremal rays (i.e. 1-dimensional cones in Γ) are the extremal rays of $\mathcal{C}$."* Let $\mathcal{C}$ be the solution cone of $AX = 0$. It follows from Stanley's proof that when $\mathcal{C}$ is not already simplicial such a triangulation may be constructed by selecting (non-deterministically) one extremal ray, say $\mathtt{r}_j$, then proceed recursively to triangulate the facets of $\mathcal{C}$ intersecting $\mathtt{r}_j$ only at 0 (i.e., such that $\mathtt{r}_j$ is not one of their extremal rays), and obtaining as a triangulation (in our sense) of $\mathcal{C}$, the set of simplicial cones that are convex hulls of $\mathtt{r}_j$ with each of the simplicial cones in the triangulation of such facets. Thus, if $\Gamma_{\mathtt{facets}} = \{cone\mathcal{G}_i\}_i$ then $\Gamma = \{cone(\mathcal{G}_i \cup \{\mathtt{r}_j\})\}_i$. In the example above, $\{cone\{s_1, s_4, s_5, s_6\},\ cone\{s_1, s_2, s_3, s_6\},\ cone\{s_1, s_2, s_5, s_6\}\}$ is a triangulation of the solution cone. Actually, first we choose s_1, and the facets of $\mathcal{C}$ not containing s_1 are $cone\{s_4, s_5, s_6\}$ and $cone\{s_2, s_3, s_5, s_6\}$. The former is simplicial. The latter is decomposed into $\{cone\{s_2, s_3, s_6\}, cone\{s_2, s_5, s_6\}\}$ by selecting s_2. The facets of $cone\{s_2, s_3, s_5, s_6\}$ not containing s_2 being $cone\{s_3, s_6\}$ and $cone\{s_5, s_6\}$, which are simplicial. When s_1 is the first selection, yet another triangulation is $\{cone\{s_1, s_4, s_5, s_6\},\ cone\{s_1, s_2, s_3, s_5\},\ cone\{s_1, s_3, s_5, s_6\}\}$.

Having found the face lattice of $\mathcal{C}$, it is not difficult to compute triangulations like these ones. The face lattice may be easily obtained from the minimal

solutions of minimal support, say $s_1, \ldots, s_p$. The algorithms we included in our implementation in C are based on the following properties. Each face of $\mathcal{C}$ is a pointed convex polyhedral cone whose extremal rays are extremal rays of $\mathcal{C}$. Since $\phi(\mathcal{F}) = \text{supp } \mathcal{F}$, for all $\mathcal{F}$, is an isomorphism from the face lattice onto the supports' lattice, $\{0\} \neq \mathcal{F} = cone\{s_{i_1}, \ldots, s_{i_k}\}$ is a face if and only if there exists no other $s_{i_{k+1}}$ such that $\text{supp } \mathcal{F} = \text{supp}\{s_{i_1}, \ldots, s_{i_k}\} = \text{supp}\{s_{i_1}, \ldots, s_{i_k}, s_{i_{k+1}}\}$. The set of 1-dimensional faces is $\{cone\{s_i\} \mid 1 \leq i \leq p\}$. If $\mathcal{F}'$ is a d-dimensional face that precedes immediately $\mathcal{F}$ (thus $\mathcal{F}'$ is a facet of $\mathcal{F}$), $\dim \mathcal{F} = d + 1$.

Domenjoud's Algorithm revisited In 1991, Domenjoud remarked that the minimal solutions of (1) whose supports are not minimal are linear rational nonnegative combinations with coefficients < 1 of linearly independent minimal solutions of minimal support. Based on this, Domenjoud proposed an algorithm [3] for finding the minimal solutions which computes the solutions generated by *each* maximal independent set of minimal solutions of minimal support. In other words, the algorithm is seeking for solutions in all possible maximal dimensional simplicial subcones whose extremal rays are extremal rays of the solution cone $\mathcal{C}$. The algorithm is significantly improved if instead of that only those subcones making a triangulation of $\mathcal{C}$ are taken into account, thus avoiding much redundancy. This is a straightforward corollary of Stanley's results. For instance, if $\mathcal{C}$ is 3-dimensional with p extremal rays only $p-2$ subcones have to be considered, instead of $p!/(3!\ (p-3)!)$. Work in this direction is also described in [11].

3 The Slopes Algorithm – Solving a Single Equation

A few years ago, we proposed algorithms for solving a single homogeneous Diophantine equation – Slopes Algorithm [16] and Rectangles Algorithm [5]. A complete description of Slopes is given in [6]. We showed that the (nonnull) solutions of (2) that are minimal in a component-wise ordering may be computed directly.

$$ax = by + cz + v, \quad a, b, c > 0,\ v \in \mathbb{Z},\ \ x, y, z \in \mathbb{N} \tag{2}$$

The Basic Slopes Algorithm, which applies to (2), yields the minimal solutions in z-increasing order by computing the *starting solution* and a set of spacings from which the remaining solutions may be derived. We shall refer to this set of spacings as the *basic spacings*. Given a solution s, the next solution is obtained by adding a suitable spacing to s. The basic spacings $\{(-\delta_y^{\mathtt{k}}, \delta_z^{\mathtt{k}})\}_k$ in δ_z increasing order, correspond to the minimal solutions of an homogeneous linear equation in three unknowns, which we present as a congruence (3), in the variables δ_y and u

$$\begin{cases} \delta_y^1 u + (y_{\max} - 1)\delta_y \equiv 0 \pmod{y_{\max}} \\ \delta_z = \delta_z^1 u \end{cases} \tag{3}$$

where u is some new auxiliary unknown, and $(-\delta_y^1, \delta_z^1)$, the so-called *minimum spacing* is given by

$$\delta_y^1 = \frac{c}{\gcd(a, b, c)} m_b \bmod y_{\max} \qquad \delta_z^1 = \frac{\gcd(a, b)}{\gcd(a, b, c)},$$

being m_b the inverse of $b/\gcd(a,b)$ modulo $y_{\max}$, with $y_{\max} = a/\gcd(a,b)$. The two trivial solutions of (2) when $v = 0$ are $(y_{\max}, 0)$ and $(0, z_{\max})$, where $z_{\max} = a/\gcd(a,c)$. In the case $v = 0$, we deduced expressions that give the minimal solutions and the suitable spacings, based on a geometric view of the solution space. If $s = (y, z)$ is a minimal solution and $(-\delta_y^{\mathtt{k}}, \delta_z^{\mathtt{k}})$ is the current spacing, then the next minimal solution is $s' = s + (-\delta_y^{\mathtt{k}}, \delta_z^{\mathtt{k}})$, provided that $y \geq \delta_y^{\mathtt{k}}$. Otherwise, $s' = \lceil \delta_y^{\mathtt{k}}/y \rceil s + (-\delta_y^{\mathtt{k}}, \delta_z^{\mathtt{k}})$ and the spacing is replaced by $s' - s$. Initially, the starting solution is $(y_{\max}, 0)$ and the first spacing is $(-\delta_y^{\mathtt{1}}, \delta_z^{\mathtt{1}})$. Recently, we noticed that MacMahon [9] had already given a method to compute the minimal solutions of $ax = by + cz$, when $c = 1$, by relating them to the continued fraction convergents to a/b. The algorithm we designed has strong similarities to the method proposed by MacMahon, although he seems not to have been aware that his method could still be applied when $c \neq 1$. Nevertheless, our method is more general.

Provided that $\gcd(a,b,c)$ divides v, (2) is satisfiable, *the starting solution* being $(y_0 + k_0 y_{\max}, z_0)$, where $k_0 = max\{0, \lceil (-by_0 - cz_0 - v)/(by_{\max}) \rceil\}$ and

$$z_0 = \frac{-vM_c}{\gcd(a,b,c)} \bmod \delta_z^{\mathtt{1}} \qquad y_0 = \frac{(-v - z_0 c)m_b}{\gcd(a,b)} \bmod y_{\max}. \tag{4}$$

Here, M_c is any integer satisfying $bM_b + cM_c + aM_a = \gcd(a,b,c)$, for some integers M_a, and M_b, and $y_{\max}$, $\delta_z^{\mathtt{1}}$, and m_b are as defined above. The output of mod is the nonnegative remainder of the division. All gcd's are positive.

To solve a problem in more than three unknowns $\sum_{i=1}^{n} a_i x_i = \sum_{j=1}^{m} b_j y_j$ $a_i, b_j > 0$, we proposed Slopes Algorithm, which computes the set of minimal solutions by solving a family of subproblems in *positive* integers. Each subproblem is obtained by setting some of the unknowns to zero and requiring that the remaining are positive. In geometric terms each subproblem consists in finding solutions in the interior of a given face of the solution cone. The faces are explored in increasing order of dimension. In this way, whenever a solution is found its minimality is decided by comparing it with the minimal solutions previously computed. For each subproblem in more than three unknowns, the values of all but three of them (say all but x_1, y_1, y_2) are enumerated under known bounds, and for each fixed tuple, a problem as (2) is solved by the Basic Slopes Algorithm.

4 Extending the Slopes Algorithm to Solve Systems

The Basic Slopes Algorithm still applies to systems $AX = 0$ whose solution space is on a plane. That is the case, for instance, of systems whose number of unknowns exceeds in two the rank of A. By Property 1 below, we see that when the solution cone is 2-dimensional, solving the system is equivalent to solving a $k \times (k+2)$ subsystem, the k equations being independent. By considering the geometric structure of the faces of the solution cone, Slopes Algorithm has been almost straightforwardly adapted to solve systems of equations. Basically,

we remarked that any system with more than one minimal solution may be rewritten into a form that is rather appropriate to apply Slopes Algorithm.

Example 2 Consider the system of the previous example. By rewriting it *relatively to cone*$\{s_4, s_5, s_6\}$ whose support is $\{1,3,4,5,6,7,8\}$, and leaving x_6, x_8, x_5 free, as well as x_2, we conclude that the given system is equivalent to

$$\begin{cases} 8x_1 = 31x_6 + 15x_8 + 4x_2 \\ 8x_3 = 121x_6 + 33x_8 + 24x_5 - 12x_2 \\ 8x_4 = 21x_6 + 5x_8 + 8x_5 + 4x_2 \\ 8x_7 = 35x_6 + 11x_8 + 8x_5 - 4x_2 \end{cases}$$

We see that all the components of the first three right-hand side columns are nonnegative. The fact that the system is rewritten with respect to a face which is a 3-dimensional simplicial cone, together with the choice of the three first free unknowns, implies the nonnegativity of those three columns. The criterion for selecting x_6, x_8, and x_5 is the following, its correctness resulting from the proof of Proposition 1, below. Given a face $\mathcal{F}$ that is a p-dimensional simplicial cone, let $\mathcal{F}$ be spanned by $\{s_{i_1}, \ldots, s_{i_p}\}$. Then, p unknowns are selected, say x_{k_j}, $1 \leq j \leq p$, such that $k_j \in \text{supp } s_{i_j} \backslash \text{supp } (\{s_{i_1}, \ldots, s_{i_p}\} \backslash \{s_{i_j}\})$. The subsystem whose solutions are on $\mathcal{F}$, may be rewritten in a solved form where the p columns associated to x_{k_j}'s, the right-hand side columns, are nonnegative.

4.1 Giving the system an appropriate form

Given a system of linear Diophantine equations $A^1x_1 + \ldots + A^nx_n = 0$, which we shall write as $AX = 0$, each A^i denoting the ith column of A, we suppose, without loss of generality, that A is a *full row* rank $m \times n$ integral matrix. Let $S_0(A)$ denote the set of minimal solutions of minimal support, and $\mathcal{L}(S_0(A))$ denote the linear space spanned by them, that is, the real space generated by the nonnegative solutions of the system. The following property gives the relationship between the dimension of the solution cone and supp $S_0(A)$.

Property 1 *If $S_0(A) \neq \emptyset$, and λ denotes the number of components that are null in all the solutions in $S_0(A)$, then dim $\mathcal{L}(S_0(A)) = n - \lambda - \text{rank}(A^{i_1}, \ldots, A^{i_{n-\lambda}})$, where $[\ A^{i_1}\ \ldots\ A^{i_{n-\lambda}}]$ is the submatrix obtained from A by removing the λ columns corresponding to the components that are null. In other words, if* supp $S_0(A) = \{i_1, \ldots, i_{n-\lambda}\}$, *then dim $\mathcal{L}(S_0(A)) = n - \lambda - \text{rank}(A^{i_1}, \ldots, A^{i_{n-\lambda}})$.*

Thus, when dim $\mathcal{L}(S_0(A)) < n - m$, the solutions may be found by solving a subsystem of the one given, namely the one whose matrix is $[A^{i_1}\ \ldots\ A^{i_{n-\lambda}}]$. For this reason, in the sequel we assume that supp $S_0(A) = \{1, \ldots, n\}$. Property 2 follows immediately from Property 1 and the definition of simplicial cone.

Property 2 *If A is a full row rank $m \times n$ matrix, and such that* supp $S_0(A) = \{1, \ldots, n\}$, *the number of minimal solutions of minimal support is $n - m$ if and only if the solution cone is simplicial.*

Using the fact that each i-dimensional face of a simplicial cone is also a simplicial cone, we shall prove the following result, which will be useful when extending Slopes Algorithm to solve systems.

Proposition 1 *If A is a full row rank $m \times n$ matrix, such that* supp $S_0(A) = \{1, \ldots, n\}$ *and the number of minimal solutions of minimal support is $n - m$, the system $AX = 0$ may be written in solved form as*

$$d\, x_{i_k} = \alpha_{i_k 1} x_{i_{m+1}} + \ldots + \alpha_{i_k n-m} x_{i_n}, \;\; 1 \leq k \leq m$$

all coefficients being nonnegative integers, $d > 0$.

Since the minimal positive solutions of minimal support are in this case linearly independent, the equivalent system may be seen as a parametric representation of the solution space based on such minimal solutions. In matricial terms, Proposition 1 asserts that when the solution cone is simplicial, the system is equivalent to $dX_0 = \mathcal{A}_{11} X_1$ with $d > 0$ and $\mathcal{A}_{11} \in \mathbb{N}^{m \times (n-m)}$, the set of variables being partitioned into $\{X_0, X_1\}$, $X_0 \in \mathbb{N}^m$, $X_1 \in \mathbb{N}^{n-m}$.

Corollary 1.1 *Let A be a full row rank $m \times n$ matrix, such that* supp $S_0(A) = \{1, \ldots, n\}$. *Let $\mathcal{C}$ denote the solution cone of $AX = 0$, and $\mathcal{F}$ be a face of $\mathcal{C}$. If $\mathcal{F}$ is a p-dimensional simplicial cone, then the system may be given the form*

$$\begin{cases} dX_0 = \mathcal{A}_{11} X_1 + \mathcal{A}_{12} X_2 \\ dX_3 = \qquad\quad \mathcal{A}_{22} X_2 \end{cases}$$

all coefficients being integral, $\mathcal{A}_{11} \in \mathbb{N}^{r \times p}$ where $r = \text{rank}\{A^i \mid i \in \text{supp}\mathcal{F}\}$, $d > 0$, the set of variables being decomposed into $\{X_0, X_1, X_2, X_3\}$ (with possibly X_2 or X_3 empty), and supp $\mathcal{F} = \{i \mid x_i$ *in* X_0 *or* $X_1\}$.

Noting that, when *dim* $\mathcal{L}(S_0(A)) \geq 2$ there exists a 2-dimensional face, and that any 2-dimensional face is necessarily simplicial, Corollary 1.1 justifies that any system having at least two minimal solutions can be written as

$$a x_{i_k} = b_{k1} x_{i_{m+1}} + b_{k2} x_{i_{m+2}} + \sum_{j=3}^{n-m} b_{kj} x_{i_{m+j}}, \;\; 1 \leq k \leq m \tag{5}$$

with all coefficients integral, $a > 0$, and $b_{kj} \geq 0$ for $j = 1, 2$. As we will see, the fact that a system can be given this particular form makes the generalization of Slopes Algorithm to solve systems quite straightforward.

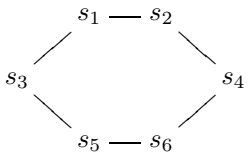
Before going on, we shall present an example that illustrates the results stated above, while motivating the following ones.

Example 3 Let us consider the system $AX = 0$ where A is given by

$$A = \begin{bmatrix} 2 & 0 & -1 & 0 & -2 & 0 & 2 & 0 \\ 0 & 1 & -2 & 0 & 1 & -2 & -2 & 2 \\ 1 & 2 & -2 & 0 & -1 & 1 & 0 & 0 \\ 2 & 1 & -2 & -1 & -2 & 2 & 0 & 2 \\ 2 & -1 & 2 & -2 & 1 & 0 & 1 & 0 \end{bmatrix}$$

which can be found to have six minimal support solutions, namely

$$
\begin{array}{l}
s_1 = (\ 15\ 22\ 30\ 34\ 0\ \ 1\ \ 0\ 20\ ) \\
s_2 = (\ 27\ \ 0\ \ 10\ 48\ 22\ 15\ \ 0\ 14\ ) \\
s_3 = (\ \ 4\ \ 10\ 12\ 12\ \ 0\ \ 0\ \ 2\ \ 9\ \ ) \\
s_4 = (\ \ 8\ \ \ 0\ \ \ 0\ \ 22\ 18\ 10\ 10\ 11\ ) \\
s_5 = (\ \ 0\ \ 30\ 28\ 24\ \ 4\ \ \ 0\ \ 18\ 29\ ) \\
s_6 = (\ \ 0\ \ \ 8\ \ \ 0\ \ 26\ 30\ 14\ 30\ 25\ )
\end{array}
$$



A cross-section of the 3-dimensional solution cone is drawn schematically on the right. The 2-dimensional facet $cone\{s_1, s_2\}$ has support $\{1, 2, 3, 4, 5, 6, 8\}$. To give the system the form described in Corollary 1.1, we note that $2 \notin \text{supp } s_2$, and $5 \notin \text{supp } s_1$, so that we solve the system with respect to the components in $\{1, 3, 4, 6, 8\}$, leaving the 2nd and 5th free, as well as the 7th, obtaining

$$
\begin{cases}
22x_1 & & & & & & & = 15x_2 + 27x_5 - 31x_7 \\
& 22x_3 & & & & & & = 30x_2 + 10x_5 - 18x_7 \\
& & 22x_4 & & & & & = 34x_2 + 48x_5 - 38x_7 \\
& & & & 22x_6 & & & = \ \ x_2 + 15x_5 - \ 5x_7 \\
& & & & & & 22x_8 & = 20x_2 + 14x_5 - \ \ x_7
\end{cases}
$$

Hence, apart from non-redundant positivity constraints, which reduce to $x_2, x_5, x_7 \geq 0$, $15x_2 + 27x_5 - 31x_7 \geq 0$, $30x_2 + 10x_5 - 18x_7 \geq 0$, and $x_2 + 15x_5 - 5x_7 \geq 0$, solutions satisfy the system of congruences (6).

$$
\begin{cases}
15x_2 + \ \ 5x_5 + 13x_7 \equiv 0 \pmod{22} \\
\ \ 8x_2 + 10x_5 + \ \ 4x_7 \equiv 0 \pmod{22} \\
12x_2 + \ \ 4x_5 + \ \ 6x_7 \equiv 0 \pmod{22} \\
\ \ \ x_2 + 15x_5 + 17x_7 \equiv 0 \pmod{22} \\
20x_2 + 14x_5 + 21x_7 \equiv 0 \pmod{22}
\end{cases}
\tag{6}
$$

Furthermore, we remark that in order to compute the solutions in the 2-dimensional $cone\{s_1, s_2\}$ only need we to find minimal (x_2, x_5) solving (6) for $x_7 = 0$. In this case, (6) is equivalent to $x_2 + 15x_5 \equiv 0 \pmod{22}$, as deduced from Property 3 below, and so the Basic Slopes Algorithm can be used to solve the problem. Indeed, even in the general case, solving a two column system as this one, may be reduced to solving a single congruence, and henceforth Basic Slopes applies. In this example, the basic spacings for the subsystem are

δ_{x_1}	δ_{x_3}	δ_{x_4}	δ_{x_6}	δ_{x_8}	$-\delta_{x_2}$	δ_{x_5}
-15	-30	-34	-1	-20	-22	0
-9	-20	-21	0	-13	-15	1
-3	-10	-8	1	-6	-8	2
3	0	5	2	1	-1	3
27	10	48	15	14	0	22

which are determined by the basic spacings $(-\delta_{x_2}, \delta_{x_5})$ obtained to the single equation. Consequently, the minimal solutions with $x_7 = 0$ are

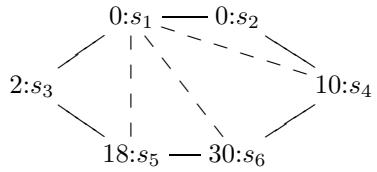
x_1	x_3	x_4	x_6	x_8	x_2	x_5
15	30	34	1	20	22	0
6	10	13	1	7	7	1
9	10	18	3	8	6	4
12	10	23	5	9	5	7
15	10	28	7	10	4	10

x_1	x_3	x_4	x_6	x_8	x_2	x_5
18	10	33	9	11	3	13
21	10	38	11	12	2	16
24	10	43	13	13	1	19
27	10	48	15	14	0	22

Although we have also given the values of x_1, x_3, x_4, x_6 and x_8, Slopes is actually driven only by those of x_2 and x_5, for no additional constraints are imposed by nonnegativity, in this case. The values of those unknowns become important when we want to find the solutions with $x_7 \neq 0$ by using Slopes techniques. Firstly, we can simplify the system of congruences, rewriting it equivalently as

$$x_2 + 15x_5 + 6x_7 \equiv 0 \pmod{22} \quad \wedge \quad 11x_7 \equiv 0 \pmod{22}$$

so that, by setting x_7 as $2x'_7$, we find that $x_2 + 15x_5 \equiv 10x'_7 \pmod{22}$. Upper bounds on the values of x_7 can be deduced from triangulations of the solution cone. Being each simplicial subcone a pointed convex polyhedral cone, the minimal solutions in each subcone are rational nonnegative combination (being the coefficients < 1) of the minimal solutions of minimal support that define the extremal rays of the subcone. Thus, by considering the triangulation illustrated by the following diagram, each label containing the value of x_7 in the corresponding minimal solution we conclude that $x_7 < 48$ in any minimal solution, and thus $x'_7 < 24$.



By enumerating on the values of x'_7, we find the candidates to minimal solutions. For instance, when $x_7 = 2x'_7 = 2$, the following candidate solutions are found, which, in this case, are actually minimal.

x_1	x_3	x_4	x_6	x_8	x_2	x_5	x_7	
4	12	12	0	9	10	0	2	(the starting solution)
1	2	4	1	3	2	2	2	
4	2	9	3	4	1	5	2	
7	2	14	5	5	0	8	2	

When $x_7 = 4$, the starting solution is $(8, 24, 24, 0, 18, 20, 0, 4)$. Because $x_1 = 8$, the spacing that first applies is $(-3, -10, -8, 1, -6, -8, 2, 0)$, the components being in the same order as on the table above. None of the candidate solutions obtained in this case is minimal.

4.2 When dim $\mathcal{C} \leq 2$

Being planar the solution space of (7)

$$a\ x_i = b_i\ y + c_i\ z,\ 1 \leq i \leq m,\ \ a > 0,\ \ b_i \geq 0,\ \ c_i \geq 0 \tag{7}$$

the Basic Slopes algorithm may be used to compute its minimal solutions. All we need is to obtain the *minimum spacing* for the system, and the bounds $y_{\max}$ and $z_{\max}$. As for the case of a single equation, (X_0, y_0, z_0) solves (7) for some $X_0 \in \mathbb{N}^m$ if and only if (y_0, z_0) solves the system of congruences

$$b_i\ y + c_i\ z \equiv 0 \pmod{a}, 1 \leq i \leq m \tag{8}$$

We shall denote (7) also by $aX = By + Cz$. In order to compute the minimum spacing between solutions of (7), we reduce the system matrix of (8) to a Hermite normal form[2] by performing elementary transformations on rows. If M is a matrix, M_i denotes the ith row of M.

Property 3 *(Hermite Normal Form) Let M be a $m \times n$ integral matrix of full column rank. There exist a unique unimodular $m \times m$ matrix U, and a unique upper triangular $n \times n$ matrix $T = (t_{ij})$, with $0 \leq t_{ij} < t_{jj}$, and such that $(UM)_i = T_i$, for $1 \leq i \leq n$, and $(UM)_i = 0$, for $n < i \leq m$. Moreover, provided $U_iV \equiv 0$ for $n < i \leq m$, the system $MX \equiv V \pmod{a}$ is equivalent to $TX \equiv [U_1V\ \ldots\ U_nV]^t \pmod{a}$. Otherwise, the system is unsatisfiable.*

Consequently, the set of minimal solutions of system (7) corresponds to the set of minimal solutions of a single equation, as stated in Proposition 2.

Proposition 2 *(y_0, z_0) is a minimal solution of (7) if and only if (y_0, w_0) is a minimal solution of $ax = t_{11}y + t_{12}\ a/\gcd(t_{22}, a)w$, being $z_0 = a/\gcd(t_{22}, a)\ w_0$, and $T = (t_{ij})$ is obtained from $M = (B\ C)$ as defined in Property 3.*

Each basic spacing between solutions of the given system determines, and is determined by, a basic spacing between solutions of the associated equation $ax = t_{11}y + t_{12}\ a/\gcd(t_{22}, a)w$. The Basic Slopes algorithm can be used to compute these latter spacings, say $\{(-\delta_y^{\mathtt{k}}, \delta_w^{\mathtt{k}})\}_{0 \leq k \leq L}$, in δ_w-increasing order, as mentioned in section 3. Let $\delta_z^{\mathtt{k}} = a/\gcd(a, t_{22})\delta_w^{\mathtt{k}}$, and $\delta_{x_i}^{\mathtt{k}} = (-b_i\delta_y^{\mathtt{k}} + c_i\delta_z^{\mathtt{k}})/a$.

Definition 1 *The set of basic spacings to (7), in δ_z-increasing order, is denoted by $\{\Delta_{\mathtt{k}}\}_{0 \leq k \leq L}$ and defined as $\{\ (\delta_{x_1}^{\mathtt{k}}, \ldots, \delta_{x_m}^{\mathtt{k}}, -\delta_y^{\mathtt{k}}, \delta_z^{\mathtt{k}})\ \}_{0 \leq k \leq L}$.*

In all cases, $\Delta_{\mathtt{0}}$ is defined by $(-y_{\max}, 0)$ with $y_{\max} = \mathrm{lcm}_i\{a/\gcd(a, b_i)\} = a/\gcd(a, t_{11})$, and $\Delta_{\mathtt{L}}$ is given by $(0, z_{\max})$, where $z_{\max} = a/\gcd(a, t_{12}, t_{22}) = \mathrm{lcm}_i\{a/\gcd(a, c_i)\}$. As before, we denote the spacing in y by $-\delta_y$ instead of δ_y to emphasize solutions being computed in y-decreasing order.

[2] In the common usage of the term (e.g., in [13]), the reduced matrix is actually the Hermite normal form of the transpose of the system matrix.

4.3 Solving a system by Slopes Algorithm

To find the minimal solutions of $AX = 0$, the Slopes algorithm first computes the set of minimal solutions of minimal support and the face lattice of the solution cone $\mathcal{C}$. Then, the idea is to find all the candidate solutions in the interior of each face $\mathcal{F}$ of dimension p, for all $2 \leq p \leq \dim \mathcal{C}$, faces being explored in increasing order of dimension. As before, the solutions in distinct faces of the same dimension are not comparable. To decide whether a solution in $\mathcal{F}$ is minimal it is sufficient to compare it with the minimal solutions found previously in $\mathcal{F}$ and in subfaces of $\mathcal{F}$.

When $p = \dim \mathcal{F} = 2$, the subsystem associated to $\mathcal{F}$ is given the form of (7) and the Basic Slopes Algorithm is used to directly find all its minimal solutions as discussed in the previous subsection. When $p > 2$, the subsystem is given the form (9), as described before (cf. (5)), with $r = \text{rank}\{A^i \mid i \in \text{supp } \mathcal{F}\}$, all coefficients being integral, $a > 0$, and $b_{i1} \geq 0$, $b_{i2} \geq 0$.

$$a x_i = b_{i1} x_{r+1} + b_{i2} x_{r+2} + \sum_{j=3}^{p} b_{ij} x_{r+j}, \;\; 1 \leq i \leq r \tag{9}$$

Upper bounds on the values of the unknowns, as for instance, bounds deduced from the minimal solutions of minimal support generating $\mathcal{F}$ may, up to some extent, be taken into account to choose the free unknowns $x_{r+3}, \ldots, x_{r+p}$, whose values are enumerated under those bounds. It must also be guaranteed that the system may be rewritten in form (9), in which all the coefficients of the two other free unknowns are nonnegative. The latter condition, is required by Slopes and holds if and only if supp $\mathcal{F}$ except the indices of the $p-2$ selected unknowns, includes the support of a 2-dimensional face of $\mathcal{F}$ (or equivalently, of $\mathcal{C}$).

To simplify the notation, let us rename x_{r+1} and x_{r+2} as y and z, respectively. After we have fixed a tuple $(x_{r+3}, \ldots, x_{r+p})$, to obtain the values of the remaining unknowns only have we to find $(x_1, \ldots, x_r, y, z)$ that satisfy a system of the type of (10) below, with $v_i = \sum_{j=3}^{p} b_{ij} x_{r+j}$.

$$a\; x_i = b_{i1}\; y + b_{i2}\; z + v_i, \;\; 1 \leq i \leq r, \;\; a > 0, \;\; b_{ij} \geq 0, \;\; v_i \text{ integer}, \tag{10}$$

Since our goal is to compute minimal solutions, we only search for solutions of (10) that are minimal in component-wise order. In the following subsection, we show how the Basic Slopes algorithm is adapted to compute these solutions.

4.4 Solving $aX = By + Cz + V$ by the Basic Slopes Algorithm

Apart from positivity restrictions, solutions of (11), i.e., of $aX = By + Cz + V$,

$$a\; x_i = b_i\; y + c_i\; z + v_i, \;\; 1 \leq i \leq m, \;\; a > 0, \;\; b_i \geq 0, \;\; c_i \geq 0, \;\; v_i \in \mathbb{Z} \tag{11}$$

have naturally to satisfy $b_i\; y + c_i\; z \equiv -v_i \pmod{a}$, $1 \leq i \leq m$, which, by Property 3 above, may be rewritten as

$$\begin{cases} t_{11}\; y + t_{12}\; z \equiv -U_1 V \pmod{a} \\ \qquad\quad t_{22}\; z \equiv -U_2 V \pmod{a} \end{cases} \tag{12}$$

provided that $U_iV \equiv 0 \pmod{a}$ holds[3], for all $3 \leq i \leq m$, where U_i stands for the ith row of the unimodular matrix of transformations, and $V = [v_1 \dots v_m]^t$. We may suppose that all the coefficients have been reduced modulo a, although that does not really make any change, other than possibly that of decreasing the coefficients magnitude. Conventioning that $\gcd(0, \alpha) = \alpha$, whatever α is, and provided that $\gcd(t_{22}, a)$ divides U_2V, otherwise (12) is inconsistent, we compute the least nonnegative z_μ satisfying the 2nd equation, which is given by

$$z_\mu = -U_2V/\gcd(t_{22}, a)\ (t_{22}/\gcd(t_{22}, a))^{-1} \bmod a/\gcd(t_{22}, a),$$

where the inverse is modulo $a/\gcd(t_{22}, a)$. Since $z \equiv z_\mu \pmod{a/\gcd(a, t_{22})}$ and $z \geq z_{\min} = max(0, \{\lceil -v_i/c_i \rceil \mid b_i = 0 \wedge c_i \neq 0\})$, we set $z = z'_\mu + a/\gcd(a, t_{22})\ w$, with $z'_\mu = z_\mu + a/\gcd(a, t_{22})\ max(0, \lceil (z_{\min} - z_\mu)\gcd(a, t_{22})/a \rceil)$, and further simplify (12) deriving the congruence

$$t_{11}\ y + t_{12}a/\gcd(a, t_{22})\ w \equiv -U_1V - t_{12}z'_\mu \pmod{a}, \tag{13}$$

that is satisfiable if and only if $\gcd(a, t_{11}, t_{12}a/\gcd(a, t_{22}))$ divides $-U_1V - t_{12}z'_\mu$. Clearly, if (11) is satisfiable, $y \geq y_{\min} = max(0, \{\lceil -v_i/b_i \rceil \mid c_i = 0 \wedge b_i \neq 0\})$.

Now, to solve (11) using Slopes Algorithm techniques, we shall compute the starting solution (the one with the least z) and the set of basic spacings. Similarly to the case of a single equation, when $v_i < 0$, for some i, nonnegative solutions of (13) may lead to a negative x_i. When finding the appropriate spacing to move from a minimal solution to the following one, not only the values of $-\delta_y$ and δ_z are relevant, but those of δ_{x_i}. The starting solution $(y_0 + k_0 y_{\max}, z_0)$ of (11) is obtained from the nonnegative solution (y_0, w_0) of (13) having the least w, defined as in (4). Here $k_0 = max(0, \{\lceil (-b_i y_0 - c_i z_0 - v_i)/(b_i y_{\max}) \rceil \mid b_i \neq 0\})$.

The interesting aspect is that the results stated in [6] for the case of a single equation can be trivially generalized, all the proofs being adapted trivially. Due to the fact that $b_i \geq 0$, $c_i \geq 0$, the sequence of basic spacings with respect to x_i is either strictly increasing, as previously, or null (being $b_i = c_i = 0$). This was the key of the previous proofs. The spacing that must be added to the current minimal solution of (11) to move to the following one is either the basic spacing with the least δ_z and such that when added to the current solution yields a nonnegative minimal solution, or when there exists none that can be applied, some composite spacing is obtained. In a more formal way, we deduce Lemma 1, Proposition 3, and Corollaries 3.1 and 3.2, which are the extensions of results proved in [6]. Due to linearity, the possible spacings are the same as for the homogeneous case. The basic spacings are as in Definition 1.

Lemma 1 *Let $s = (x_1^{\mathtt{s}}, \dots, x_m^{\mathtt{s}}, y^{\mathtt{s}}, z^{\mathtt{s}})$ be a minimal solution of (11) such that $y^{\mathtt{s}} - y_{min} \geq \delta_y^{\mathtt{L-1}} = min\{\delta_y^{\mathtt{i}} \mid \delta_y^{\mathtt{i}} \neq 0\}$, with $\delta_y^{\mathtt{i}}$ as defined previously. Then, the minimum t such that some spacing $\Delta_{\mathtt{k}}$, with $k < L$, can be added to $s + t\Delta_{\mathtt{L}}$ is*

$$t_0 = max\left(0, max_i\left\{\left\lceil -(x_i^{\mathtt{s}} + \delta_{x_i}^{\mathtt{L-1}})/\delta_{x_i}^{\mathtt{L}}\right\rceil \mid \delta_{x_i}^{\mathtt{L}} \neq 0\right\}\right).$$

Moreover, $\Delta_{\mathtt{q}} = (\delta_{x_1}^{\mathtt{q}}, \dots, \delta_{x_m}^{\mathtt{q}}, -\delta_y^{\mathtt{q}}, \delta_z^{\mathtt{q}})$ is the first spacing that can be added, where $q = min\{k \mid \delta_y^{\mathtt{k}} \leq y^{\mathtt{s}} - y_{min},$ and $x_i^{\mathtt{s}} + t_0\delta_{x_i}^{\mathtt{L}} + \delta_{x_i}^{\mathtt{k}} \geq 0$ for all $i\}$.

[3] This condition may be used while generating the values of the enumerated unknowns.

Proposition 3 *The spacings required to solve the family of problems*

$$\{aX = By + Cz + V\}_{V \in \mathbb{Z}^m},\ a > 0,\ \ B, C \in \mathbb{N}^m \tag{14}$$

result from the spacings $\{\Delta_{\mathtt{k}}\}_{0 \le k \le L}$ *as follows. Let* $s = (x_1^{\mathtt{s}}, \ldots, x_m^{\mathtt{s}}, y^{\mathtt{s}}, z^{\mathtt{s}})$ *be a minimal solution of (14) for fixed* $V \in \mathbb{Z}^m$*. If* $y^{\mathtt{s}} - y_{min} \ge \delta_y^{\mathtt{L}-1}$ *then the spacing that must be added to* s *to obtain the next minimal solution is*

$$t_0 \Delta_{\mathtt{L}} + \Delta_{\mathtt{q}} + r_0 \Delta_{\mathtt{0}}$$

with $r_0 = min\{\lfloor (y^{\mathtt{s}} - y_{min} - \delta_y^{\mathtt{q}})/y_{max} \rfloor, min_i\{\lfloor -(x_i^{\mathtt{s}} + t_0 \delta_{x_i}^{\mathtt{L}} + \delta_{x_i}^{\mathtt{q}})/\delta_{x_i}^{\mathtt{0}} \rfloor \mid \delta_{x_i}^{\mathtt{0}} \neq 0\}\}$*, and* q *and* t_0 *as defined in Lemma 1. If* $y^{\mathtt{s}} - y_{min} < \delta_y^{\mathtt{L}-1}$*, there are no more minimal solutions.*

Corollary 3.1 *The spacings required to solve the family of problems*

$$\{aX = By + Cz + V\}_{V \ge 0},\ a > 0,\ \ B, C \in \mathbb{N}^m \tag{15}$$

are the basic spacings $\{\Delta_{\mathtt{k}}\}_{0 \le k \le L}$*. Given* $s = (x_1^{\mathtt{s}}, \ldots, x_m^{\mathtt{s}}, y^{\mathtt{s}}, z^{\mathtt{s}})$*, a minimal solution of (15) for fixed* $V \in \mathbb{N}^m$*, let* $q = min\{k \mid \delta_y^{\mathtt{k}} \le y^{\mathtt{s}}\}$*. The next minimal solution is obtained by adding* $\Delta_{\mathtt{q}} = (\delta_{x_1}^{\mathtt{q}}, \ldots, \delta_{x_m}^{\mathtt{q}}, -\delta_y^{\mathtt{q}}, \delta_z^{\mathtt{q}})$ *to* s*, provided* $\delta_y^{\mathtt{q}} \neq 0$*. Otherwise, there are no more minimal solutions.*

Corollary 3.2 *Under the conditions of Proposition 3, and provided* $L \ge 2$*,*

- *if for some* $k < L$*, we have* $\delta_{x_i}^{\mathtt{k}} \ge 0$ *for all* i*, then* $\Delta_{\mathtt{L}}$ *is never added, that is* $t_0 = 0$ *for all* s*;*
- *if* $\delta_{x_i}^{\mathtt{1}} \le 0$ *for all* i*, then* $\Delta_{\mathtt{0}}$ *is never added, i.e.* $q \neq 0$ *and* $r_0 = 0$ *for all* s*.*

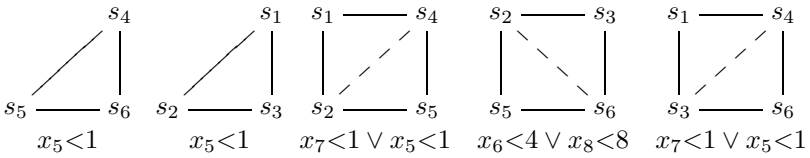
5 About the Difficulty in Solving a Given Problem

Theoretical bounds on the minimal solutions have been given for instance by Domenjoud [3] and Pottier [12]. Being expressed in terms of the entries or the minors of the system matrix, the estimated bounds may be distinct for equivalent systems. Furthermore, their use in controlling and pruning the search may be much less effective than the minimal solutions of minimal support. In particular, we are investigating bounds determined by different triangulations of the solution cone for a given problem. A simple heuristic to obtain a *fairly good* triangulation is to select first the extremal ray having the least value for the sum of components. A somewhat more elaborate criterion, not so easy to implement, is to minimize the bounds that are derived in the end for some selected components.

On the other hand, we consider the structure of the solution cone in conjunction with bounds on the minimal solutions to decide how to solve a given problem. We have a non-optimized implementation in C of our algorithm. Although no extensive comparison to other algorithms has yet been made, there are obvious speed-ups in some cases, confirming our belief that it would perform quite efficiently when the solution cone is either simplicial or has simplicial faces

of high dimensions, as it was the case with the version for single equations [6]. In fact, when the solution cone is simplicial, to check whether a solution is minimal only the values of the free unknowns need to be inspected, which speeds up the test. Moreover, bounds on the components may be dynamically obtained from the minimal solutions to effectively prune the search, without much overhead.

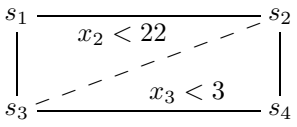
Example 4 (Example 1 continued.) By inspecting the minimal solutions of minimal support generating each facet, we conclude that there is no minimal solution in the interior of the facets but for $cone\{s_2, s_3, s_5, s_6\}$, for which there are also the bounds $x_6 < 12 \wedge x_8 < 12$.



For any minimal solution in the interior of the solution cone, $1 \leq x_3 < 3$ due to $s_4 = (0, 0, 3, 1, 1, 0, 1, 0)$. Also, $1 \leq x_5 < 2$, and $1 \leq x_2 < 48$. By contrast, the theoretical bound [3, 12] on $||s||_\infty$ for minimal solutions $s \in cone\{s_4, s_5, s_6\}$ is at least $3 \times 121 = 363$. And, in the interior of the solution cone it is at least $4 \times 121 = 484$.

Example 5 Let us consider for instance $537x_1 + 3x_2 = 22x_3 + 235x_4$.

$$
\begin{array}{ll}
s_1 = (& 22 \quad 0 \; 537 \quad 0 \;) \\
s_2 = (& 235 \quad 0 \quad 0 \; 537 \;) \\
s_3 = (& 0 \quad 22 \quad 3 \quad 0 \;) \\
s_4 = (& 0 \; 235 \quad 0 \quad 3 \;)
\end{array}
$$



The theoretical upper bounds on x_2 and x_3 are 235 and 537 respectively. To find the minimal solutions in the interior of the cone by Slopes Algorithm, instead of solving $537x_1 = 22x_3 + 235x_4 - 3x_2,\ x_2 < 235$, we would rather solve $235x_4 = 537x_1 + 3x_2 - 22x_3,\ x_3 < 3$ (wrt face $\{s_2, s_4\}$) and $537x_1 = 22x_3 + 235x_4 - 3x_2,\ x_2 < 22 \wedge x_3 \geq 3$ (wrt face $\{s_1, s_2\}$). Similar ideas apply when solving any system, whose solution cone is 3-dimensional with 4 extremal rays.

6 Conclusions

We presented a new algorithm for solving a system of linear Diophantine equations which is a generalization of algorithms we described previously for a single equation. It explores the geometric structure of the solution space. We also showed how to use this structure in deriving bounds on the components of minimal solutions, these bounds being independent from the particular form in which the system is given and in general being better than the theoretical ones known to date. In conclusion, we are convinced that it is worth while to consider the geometric structure of the solution space when dealing with problems as such.

Acknowledgements We are grateful to the anonymous referees for their constructive comments.

References

1. Boudet, A., Contejean E., and Devie, H.: A new *AC* Unification algorithm with an algorithm for solving systems of Diophantine equations. In Proceedings of the 5th Conference on Logic and Computer Science, IEEE, 289–299, 1990.
2. Clausen, M., and Fortenbacher, A.: Efficient solution of linear Diophantine equations. *J. Symbolic Computation*, 8, 201–216, 1989.
3. Domenjoud, E.: *Outils pour la Déduction Automatique dans les Théories Associatives-Commutatives*. Thése de doctorat, Université de Nancy I, 1991.
4. Elliott, E. B.: On linear homogenous Diophantine equations. *Quart. J. Pure Appl. Math.*, 34, 348–377, 1903.
5. Filgueiras, M., and Tomás, A. P.: Fast Methods for Solving Linear Diophantine Equations. In M. Filgueiras, L. Damas (eds.) *Progress in Artificial Intelligence — 6th Portuguese Conference on Artificial Intelligence*, Lecture Notes in Artificial Intelligence 727, Springer-Verlag, 297–306, 1993.
6. Filgueiras, M., and Tomás, A. P.: A Fast Method for Finding the Basis of Nonnegative Solutions to a Linear Diophantine Equation. *J. Symbolic Computation*, 19, 507–526, 1995.
7. Huet, G.: An algorithm to generate the basis of solutions to homogeneous linear Diophantine equations. *Information Processing Letters*, 7(3), 1978.
8. Lambert, J.-L.: 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, 39–40, 1987.
9. MacMahon, P.: *Combinatory Analysis*, 2. Chelsea Publishing Co., 1918.
10. Moulinet-Ossola, C.: *Algorithmique des Réseaux et des Systèmes Diophantiens Linéaires*. Thése de doctorat, Université de Nice Sophia-Antipolis, 1995.
11. Petitjean, E.: *Résolution Parallèle de Contraintes Linéaires sur les Entiers Naturels*. Mémoire de DEA, Université de Nancy I, 9/1996.
12. Pottier, L.: Minimal solutions of linear diophantine systems: bounds and algorithms. In R. V. Book (ed.), *Proceedings of the 4th International Conference on Rewriting Techniques and Applications*, Lecture Notes in Computer Science 488, Springer-Verlag, 162–173, 1991.
13. A. Schrijver, *Theory of Linear and Integer Programming*, Wiley-Interscience, 1986.
14. Stanley, R.P.: Linear homogeneous Diophantine equations and magic labelings of graphs. *Duke Math. J.*, 40, 607–632, 1973.
15. Stanley, R.P.: *Enumerative Combinatorics*, Vol I, The Wadsworth & Brooks/Cole Mathematics Series, 1986.
16. Tomás, A. P. and Filgueiras, M.: A new method for solving linear constraints on the natural numbers. In P. Barahona, L. Moniz Pereira, A. Porto (eds.), *Proceedings of the 5th Portuguese Conference on Artificial Intelligence*, Lecture Notes in Artificial Intelligence 541, Springer-Verlag, 30–44, 1991.
17. Tomás, A. P.: *On Solving Linear Diophantine Constraints*. Tese de Doutoramento, submitted to Faculdade de Ciências da Universidade do Porto, 1997.

Proof. (Proposition 1)

Let $S_0(A) = \{s_1, \ldots, s_{n-m}\}$. Let $\mathcal{C}$ be the solution cone. Since $\mathcal{C}$ is simplicial, each facet of $\mathcal{C}$ is obtained by removing one extremal ray. Let then, $\mathcal{F}_j$ be the facet whose extremal rays are $S_0(A)\backslash\{s_j\}$. Thus, supp $\mathcal{F}_j \subset$ supp $\mathcal{C}$ = supp $S_0(A)$, there existing $q_j \in$ supp s_j such that $q_j \notin$ supp $\mathcal{F}_j$. This means that $q_j \notin$ supp s_p, for all $p \neq j$. Let $\{i_1, \ldots, i_m\} = \{1, \ldots, n\}\backslash\{q_1, \ldots, q_{n-m}\}$. Necessarily $|A^{i_1} \ldots A^{i_m}| \neq 0$, otherwise rank$(A) < m$. Furthermore, if we rename q_j as i_{m+j}, it follows that

$$(x_{i_1}, \ldots, x_{i_m}, x_{i_{m+1}}, \ldots, x_{i_n}) = x_{i_{m+1}}/s_{i_{m+1}1}(s_{i_1 1}, \ldots, s_{i_m 1}, s_{i_{m+1}1}, 0, \ldots, 0) + \\ \ldots + \ x_{i_n}/s_{i_n n-m}(s_{i_1 n-m}, \ldots, s_{i_m n-m}, 0, 0, \ldots, s_{i_n n-m})$$

and so, $x_{i_k} = s_{i_k 1}/s_{i_{m+1}1}x_{i_{m+1}} + \ldots + s_{i_k n-m}/s_{i_n n-m}x_{i_n}$, $1 \leq k \leq m$. Thus,

$$0 \leq s_{i_k j}/s_{i_{m+j} j} = |A^{i_1} \ldots A^{i_{k-1}} \ -A^{i_{m+j}} A^{i_{k+1}} \ldots A^{i_m}|/|A^{i_1} \ldots A^{i_m}| = \alpha_{i_k j}/d,$$

which completes the proof.

Proof. (Corollary 1.1)

$\mathcal{F}$ is the cone of real nonnegative solutions of the subsystem

$$A^{i_1}x_{i_1} + \ldots + A^{i_r}x_{i_r} + A^{i_{m+1}}x_{i_{m+1}} + \ldots + A^{i_{m+p}}x_{i_{m+p}} = 0.$$

From Property 1, $p = dim\ \mathcal{F} = (r + p) - rank(A^{i_1} \ldots A^{i_r}\ A^{i_{m+1}} \ldots A^{i_{m+p}})$. Hence $r = rank(A^{i_1} \ldots A^{i_r}\ A^{i_{m+1}} \ldots A^{i_{m+p}})$, and the indices may be rearranged if necessary, so that $A^{i_1}, \ldots, A^{i_r}$ are linearly independent. If $r < m$, we may find $\{i_{r+1}, \ldots, i_m\} \subseteq \{1, \ldots, n\}\backslash$supp $\mathcal{F}$, such that $A^{i_1}, \ldots, A^{i_r}, A^{i_{r+1}}, \ldots, A^{i_m}$ are linearly independent. Consequently, $AX = 0$ may be given the form

$$|A^{i_1} \ldots A^{i_m}|x_{i_k} = \sum_{j=1}^{n-m} |A^{i_1} \ldots A^{i_{k-1}} \ -A^{i_{m+j}} A^{i_{k+1}} \ldots A^{i_m}|x_{i_{m+j}},\ 1 \leq k \leq m.$$

For all $1 \leq j \leq p$ and $1 \leq k \leq r$, we may write $|A^{i_1} \ldots A^{i_{k-1}} \ -A^{i_{m+j}} A^{i_{k+1}} \ldots A^{i_m}|$ as

$$\frac{|A^{i_1} \ldots A^{i_{k-1}} \ -A^{i_{m+j}} A^{i_{k+1}} \ldots A^{i_r}|}{|A^{i_1} \ldots A^{i_r}|}\ |A^{i_1} \ldots A^{i_m}|$$

and being $\mathcal{F}$ simplicial, $|A^{i_1} \ldots A^{i_{k-1}} \ -A^{i_{m+j}} A^{i_{k+1}} \ldots A^{i_r}|/|A^{i_1} \ldots A^{i_r}| \geq 0$ by Proposition 1. Finally, if $k \geq r+1$, then $|A^{i_1} \ldots A^{i_{k-1}} \ -A^{i_{m+j}} A^{i_{k+1}} \ldots A^{i_m}| = 0$, for all $1 \leq j \leq p$, since $A^{i_{m+j}}$ is a linear combination of $A^{i_1}, \ldots, A^{i_r}$. This leads to the conclusion that the system may be given the form described in the corollary.

Proof. (Proposition 2) Almost immediate from Property 3. Just a brief note: when $rank(B) = 1$, $b_{i2} = \alpha b_{i1}$ for some rational α, thus $t_{12} = \alpha t_{11}$ and $t_{22} = 0$. By convention, $\gcd(\alpha, 0) = \alpha$.

Proof. (Lemma 1)

When $b_{i1} = b_{i2} = 0$, the value of $x_i^{\mathtt{s}}$ does not matter, since $\delta_{x_i}^{\mathtt{k}} = 0$, for all k. When $b_{i1} \neq 0 \ \vee \ b_{i2} \neq 0$, the sequence $\{\delta_{x_i}^{\mathtt{k}}\}_k$ is strictly increasing. Indeed, from $\delta_y^{\mathtt{k+1}} < \delta_y^{\mathtt{k}}$ and $\delta_z^{\mathtt{k+1}} > \delta_z^{\mathtt{k}}$, it follows $a\delta_{x_i}^{\mathtt{k+1}} = b_{i1}(-\delta_y^{\mathtt{k+1}}) + b_{i2}\delta_z^{\mathtt{k+1}} > b_{i1}(-\delta_y^{\mathtt{k}}) + b_{i2}\delta_z^{\mathtt{k}} = a\delta_{x_i}^{\mathtt{k}}$. Hence, $\delta_{x_i}^{\mathtt{L}-1} \geq \delta_{x_i}^{\mathtt{k}}$ for all $k < L$. If $\delta_{x_i}^{\mathtt{L}} = 0$ then $b_{i2} = 0$, since $\delta_y^{\mathtt{L}} = 0 \ \wedge \ \delta_z^{\mathtt{L}} = z_{\max}$. But, then $x_i^{\mathtt{s}} + \delta_{x_i}^{\mathtt{L}-1} \geq 0$, otherwise $y^{\mathtt{s}} + \delta_y^{\mathtt{L}-1} < y_{\min}$, which contradicts the hypothesis on s. As a result, $\Delta_{\mathtt{k}}$ can be added to $s + t_0\Delta_{\mathtt{L}}$ only if $\Delta_{\mathtt{L}-1}$ can be. Thus, t_0 is given as in the Lemma.

Proof. (Proposition 3)

If $y^{\mathtt{s}} - y_{\min} < \delta_y^{\mathtt{L}-1}$, there is no minimal solution following s because $\delta_y^{\mathtt{L}-1}$ is the minimum positive spacing in y between integral solutions.

If $y^{\mathtt{s}} - y_{\min} \geq \delta_y^{\mathtt{L}-1}$ then there exists $k \geq 0$ such that $s + \Delta_{\mathtt{L}-1} + k\Delta_{\mathtt{L}}$ is a positive solution, that is not comparable with s. Thus, s is not the last minimal solution. Then, let $s' = (x_1', \ldots, x_m', y', z')$ be the minimal solution following immediately s, and let $(\delta_{x_1}, \ldots, \delta_{x_m}, -\delta_y, \delta_z)$ be the spacing applied, that is $(\delta_{x_1}, \ldots, \delta_{x_m}, -\delta_y, \delta_z) = (x_1', \ldots, x_m', y', z') - (x_1^{\mathtt{s}}, \ldots, x_m^{\mathtt{s}}, y^{\mathtt{s}}, z^{\mathtt{s}})$. Clearly, we may write $(\delta_{x_1}, \ldots, \delta_{x_m}, -\delta_y, \delta_z)$ in terms of $\Delta_{\mathtt{L}} = (\delta_{x_1}^{\mathtt{L}}, \ldots, \delta_{x_m}^{\mathtt{L}}, 0, z_{\max})$ as follows

$$(\delta_{x_1}, \ldots, \delta_{x_m}, -\delta_y, \delta_z) = \left\lfloor \frac{\delta_z}{z_{\max}} \right\rfloor \Delta_{\mathtt{L}} + (\delta'_{x_1}, \ldots, \delta'_{x_m}, -\delta_y, \delta_z \bmod z_{\max})$$

where $\delta'_{x_i} = \delta_{x_i} - \lfloor \delta_z / z_{\max} \rfloor \delta_{x_i}^{\mathtt{L}}$. We are going to show that

$$\lfloor \delta_z / z_{\max} \rfloor = t_0 \tag{16}$$

and that

$$(\delta'_{x_1}, \ldots, \delta'_{x_m}, -\delta_y, \delta_z \bmod z_{\max}) = \Delta_{\mathtt{q}} + r_0\Delta_{\mathtt{0}}. \tag{17}$$

Because $(\delta_y, \delta_z \bmod z_{\max})$ is a solution of the equation defining the basic spacings, whose minimal solutions are defined by $\{(\delta_y^{\mathtt{k}}, \delta_z^{\mathtt{k}})\}_k$, there are integers $\alpha_k \geq 0$ such that

$$(\delta'_{x_1}, \ldots, \delta'_{x_m}, -\delta_y, \delta_z \bmod z_{\max}) = \sum_{k=0}^{L-1} \alpha_k \Delta_{\mathtt{k}} \tag{18}$$

By definition of t_0, we have $t_0 \neq 0$ only if for some p such that $b_{p2} \neq 0$, $\delta_{x_p}^{\mathtt{k}} < 0$ holds for all $k < L$. Hence, from (18) if $t_0 \neq 0$ then $\delta'_{x_p} \leq \delta_{x_p}^{\mathtt{L}-1} < 0$. Moreover $\delta_y \geq \delta_y^{\mathtt{L}-1}$. Then, as $(\delta'_{x_1}, \ldots, \delta'_{x_m}, -\delta_y, \delta_z \bmod z_{\max})$ can be added to $s + \lfloor \delta_z / z_{\max} \rfloor \Delta_{\mathtt{L}}$, so does $\Delta_{\mathtt{L}-1}$. This implies that $\lfloor \delta_z / z_{\max} \rfloor \geq t_0$, and thus $\lfloor \delta_z / z_{\max} \rfloor = t_0$. Otherwise, $s + t_0\Delta_{\mathtt{L}} + \Delta_{\mathtt{L}-1}$ is a solution that contradicts the assumption that s' immediately follows s.

On the other hand, $t_0 = 0$ implies that at least $\Delta_{\mathtt{L}-1}$ can be added to s. If $\lfloor \delta_z / z_{\max} \rfloor \neq 0 = t_0$ then $s + \Delta_{\mathtt{L}-1}$ is a solution that contradicts s' immediately following s for $\delta_z^{\mathtt{L}-1} < z_{\max}$. Therefore (16) holds.

Now we prove (17) using the fact that (16) holds. From (16) and the definition of q given by Lemma 1 it follows that $\delta_z \bmod z_{\max} = \delta_z^{\mathtt{q}}$. If not, there

would be a positive solution whose z component, say z'', verifies $z^{\mathtt{s}} < z'' = z^{\mathtt{s}} + t_0 z_{\max} + \delta_z^{\mathtt{q}} < z'$, contradicting the fact that s' immediately follows s. As a result, we may write

$$(\delta'_{x_1}, \ldots, \delta'_{x_m}, -\delta_y, \delta_z \bmod z_{\max}) = \Delta_{\mathtt{q}} + (\delta'_{x_1} - \delta^{\mathtt{q}}_{x_1}, \ldots, \delta'_{x_m} - \delta^{\mathtt{q}}_{x_m}, -\delta_y + \delta^{\mathtt{q}}_y, 0).$$

Replacing δ'_{x_i} by their definition, and as $(-\delta_y + \delta^{\mathtt{q}}_y, 0)$ must be of the form $r(-y_{\max}, 0)$, it is not difficult now to conclude that (17) holds. In fact, it follows that $\delta_{x_i} = \lfloor \delta_z / z_{\max} \rfloor \delta^{\mathtt{L}}_{x_i} + \delta^{\mathtt{q}}_{x_i} + r\delta^{\mathtt{0}}_{x_i} = t_0 \delta^{\mathtt{L}}_{x_i} + \delta^{\mathtt{q}}_{x_i} + r\delta^{\mathtt{0}}_{x_i}$, and r_0 was defined so that the solution $s + t_0 \Delta_{\mathtt{L}} + \Delta_{\mathtt{q}} + r_0 \Delta_{\mathtt{0}}$ is nonnegative and as smaller as possible.

Proof. (Corollary 3.1)

When $v_i \geq 0$, the definition of q can be simplified, since in this case, $ax_i = b_{i1}(y^{\mathtt{s}} - \delta^{\mathtt{k}}_y) + b_{i2}(z^{\mathtt{s}} + \delta^{\mathtt{k}}_z) + v_i \geq 0$, if $y^{\mathtt{s}} \geq \delta^{\mathtt{k}}_y$.

Proof. (Corollary 3.2)

The first statement follows trivially from the definition of t_0. As to the second, note that if the solutions were computed in y-increasing order the spacings would just be the symmetrics of the ones we are using now. In that case $-\Delta_{\mathtt{0}}$ would have the same role as $\Delta_{\mathtt{L}}$ is having now, and therefore the second statement is just a reformulation of the first.