



**HAL**  
open science

# Certificates and relaxations for integer programming and the semi-group membership problem

Jean-Bernard Lasserre, Eduardo S. Zeron

► **To cite this version:**

Jean-Bernard Lasserre, Eduardo S. Zeron. Certificates and relaxations for integer programming and the semi-group membership problem. 2009. hal-00382774

**HAL Id: hal-00382774**

**<https://hal.science/hal-00382774>**

Preprint submitted on 11 May 2009

**HAL** is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

# CERTIFICATES AND RELAXATIONS FOR INTEGER PROGRAMMING AND THE SEMI-GROUP MEMBERSHIP PROBLEM

J. B. LASSERRE AND E. S. ZERON

ABSTRACT. We consider integer programming and the semi-group membership problem. We develop and extend the approach started in [5, 6] so as to provide the following *theorem of the alternative*: the system  $b = Ax$  has no nonnegative integral solution  $x \in \mathbb{N}^n$  if and only if  $p(b) < 0$  for some given polynomial  $p$ . The coefficients of  $p$  form a vector which lies in some convex cone  $\Omega$ , and so we characterize  $\Omega$ . We also provide a hierarchy of linear programming relaxations, where the continuous case  $Ax = b$  describes the first relaxation in the hierarchy for  $x \in \mathbb{R}^n$  and  $x \geq 0$ .

## 1. INTRODUCTION

This paper is concerned with certificates for integer programming (IP) as well as with the semi-group membership problem. That is, given a finitely generated abelian group  $G$  (e.g.  $\mathbb{Z}^n$ ), a semi-group  $G_a \subset G$  generated by a finite family  $(a_k)_{k=1}^n \subset G$ , and an element  $b \in G$ , we provide a certificate of  $b \in G_a$  or  $b \notin G_a$ . We build upon and extend previous work of [5, 6, 9], notably on a discrete Farkas lemma for IP. Among other things, we provide a hierarchy of linear programming relaxations (LP-relaxations) for integer programming. The first relaxation in the hierarchy is just the usual LP relaxation, which then appears as a *first-order* (or linear) approximation to the discrete case, whereas usually IP is viewed as an arithmetic refinement of LP. We also provide a theorem of the alternative (or duality theorem) in the form of a polynomial certificate associated with the IP problem, and we compare with the certificate for LP obtained by the standard Farkas lemma.

A central idea in nonconvex optimization is to replace a non convex (hence hard) problem with a suitable easier convex problem in some lifted space, but at the price of increasing the dimension. For instance in the lift-and-project approach for polynomial optimization (e.g. 0-1 problems) one replaces  $x \in \mathbb{R}^n$  with the vector  $\mathbf{y} = (x^\alpha)$  of all moments and solves some hierarchy of appropriate linear or semidefinite

relaxations. The interested reader is referred for more details to e.g. Serali and Adams [12, 13], Lovász and Schrijver [11], and Lasserre [7, 8]; see also Laurent [10] for a comparison. Of course, any IP problem can also be modeled via polynomial equations. For example, if the entry  $x_i$  is bounded by some integer  $M$ , then one may include the polynomial constraint  $\prod_{k=0}^M (x_i - k)$  which forces  $x_i$  to be an integer, and so the above methodology applies. However, since the degree in the constraint is  $M$  (as opposed to 2 in the Boolean case), the size of the first linear or semidefinite relaxation in the hierarchy (in e.g. [8]) is already very large because it includes moments up to order  $M$ .

Let  $A \in \mathbb{N}^{m \times n}$  be a fixed matrix. In the approach developed in [5, 6] the integral solution  $x \in \mathbb{N}^n$  to  $Ax = b$  is also lifted to some  $\mathbf{y} \in \mathbb{R}^p$  with  $p \leq n \prod_j (1+b_j)$ . But this time the lifting process has a different meaning. Indeed there is some very simple matrix  $E \in \mathbb{R}^{n \times p}$  such that  $x := E\mathbf{y} \in \mathbb{R}^n$  is now a point in the integer hull of feasible solutions. Furthermore, the vector  $\mathbf{y}$  is a point of some polytope and several interpretations can be deduced from the lifting process. For example it was already shown in [5] that the lifting process can be used to prove that  $b = Ax$  for some nonnegative integral vector  $x \in \mathbb{N}^n$  if and only if the polynomial  $z^b - 1$  has a nonnegative representation in the binomial ideal generated by the binomials  $(z^{A_k} - 1)$ . But this interpretation is only one among many other interpretations as shown in the present paper.

Interestingly, one can also use the lifting process to provide a hierarchy of LP relaxations for the IP problem, so that the continuous case  $\{Ax = b : x \in \mathbb{R}^n, x \geq 0\}$  appears as a first-order (or linear) approximation of the discrete case with  $x \in \mathbb{N}^n$ . This hierarchy also provides us with a *theorem of the alternative* (or duality theorem) which uses a non linear polynomial, a discrete analogue of the celebrated Farkas Lemma in linear algebra and convex optimization. Recall that the Farkas Lemma provides a membership certificate for the convex cone  $\Theta := \{Ax : x \in \mathbb{R}^n, x \geq 0\}$ , in the form  $b \notin \Theta$  if and only if  $\omega'b < 0$  for some  $\omega$  with  $\omega'A \geq 0$ . In other words  $b \notin \Theta$  if and only if the *linear* polynomial  $z \mapsto p_\omega(z) := \omega'z$  is negative when evaluated at  $z = b$ .

**Contribution.** Every finitely generated abelian group  $G$  can be identified with a subset of  $\mathbb{Z}^m$  and so:

- We firstly show that the semi-group membership problem reduces to the existence of a nonnegative integral vector  $x \in \mathbb{N}^n$ , solution of

some related linear system  $Ax = b$  for some nonnegative integral matrix  $A \in \mathbb{N}^{m \times n}$ . Shevshenko [15, p. 11] developed a similar result in the framework of additive semigroups with unity, contained in a finite generated abelian group.

• Set  $p := \sum_{k=1}^n \prod_{j=1}^m (1+b_j - A_{j;k})$ . We next show that existence of a nonnegative integral solution  $x \in \mathbb{N}^n$  to the linear system  $Ax = b$  reduces to the existence of a nonnegative real solution  $\mathbf{y} \in \mathbb{R}^p$  for a system of linear equations of the form :

$$(1.1) \quad b_j = \mathbf{y}' A^{(e_j)}, \quad \forall 1 \leq j \leq m;$$

$$(1.2) \quad b_i b_j = \mathbf{y}' A^{(e_i + e_j)}, \quad \forall 1 \leq i \leq j \leq m;$$

$$\dots = \dots$$

$$(1.3) \quad b_1^{z_1} \dots b_m^{z_m} = \mathbf{y}' A^{(z)}, \quad \left( \begin{array}{l} \forall 0 \leq z_j \leq b_j, \\ z_1 + \dots + z_m = \delta; \end{array} \right)$$

$$\dots = \dots$$

$$(1.4) \quad b_1^{b_1} \dots b_m^{b_m} = \mathbf{y}' A^{(b)};$$

for some appropriate nonnegative integer vectors  $A^{(e_j)}, A^{(e_i + e_j)}, A^{(z)} \in \mathbb{N}^p$  with  $z \in \mathbb{N}^m$  and  $z \leq b$ . The parameter  $\delta \geq 1$  in (1.3) is the degree of the monomial  $b \mapsto b_1^{z_1} \dots b_m^{z_m}$  in (1.3). Therefore a certificate of  $b \neq Ax$  for every  $x \in \mathbb{N}^n$  is obtained as soon as any subsystem of (1.1)-(1.4) has no solution  $\mathbf{y} \in \mathbb{R}^p$ ; that is, one does not need to consider the entire system (1.1)-(1.4).

We can index the entries of  $A^{(e_j)} = (A^{(e_j)}[k, u]) \in \mathbb{N}^p$  in (1.1) in such a way that  $A^{(e_j)}[k, u] = A_{j;k}$  for all  $u, 1 \leq j \leq m$ , and  $1 \leq k \leq n$ . If we also index the entries of  $\mathbf{y} = (y[k, u]) \in \mathbb{R}^p$  in the same way, the new vector  $\hat{x} = (\hat{x}_k) \in \mathbb{R}^n$  with  $\hat{x}_k := \sum_u y[k, u]$  satisfies  $A\hat{x} = b$  and belongs to the integer hull of  $\{x \in \mathbb{R}^n : Ax = b, x \geq 0\}$ , whenever  $\mathbf{y}$  is a solution to (1.1)-(1.4). In this approach, LP (or the continuous case) appears as a particular "first order" (or "linear") approximation of IP (the discrete case). Indeed, if one considers (1.1) alone (i.e. ignoring (1.2)-(1.4) which have nonlinear right-hand-sides terms  $b^z$  for  $\|z\| > 1$ ) then from any nonnegative solution  $\mathbf{y}$  of (1.1) one obtains a real nonnegative solution  $\hat{x} \in \mathbb{R}^n$  of  $A\hat{x} = b$ , and conversely.

To construct a natural hierarchy of LP-relaxations for the IP feasibility problem  $Ax = b, x \in \mathbb{N}^n$ , just consider an increasing number of equations among the system (1.1)-(1.4), so that the last (and largest size) LP-relaxation is the whole system (1.1)-(1.4) that describes the integer hull of the set  $\{x \in \mathbb{N}^n : Ax = b\}$ . Thus, if on the one hand the discrete case is an arithmetic refinement of the continuous one, on the other hand the discrete case can be approximated via LP-relaxations of

increasing sizes, and these relaxations are different from the lift-and-project ones described in e.g. ([10]). To the best of our knowledge such a hierarchy has not been investigated before. Even if it is not clear at the moment whether this hierarchy of linear relaxations is useful from a computational viewpoint, it provides new insights for integer programming.

On the other hand it was already proved in [5, 6] that existence of a nonnegative integral solution  $x \in \mathbb{N}^n$  to the linear system  $Ax = b$ , reduces to the existence of a nonnegative real solution  $\mathbf{y} \in \mathbb{R}^p$  for a system of the form

$$(1.5) \quad (-1, 0, \dots, 0, 1)' = \Theta \mathbf{y},$$

where  $\Theta$  is some appropriated *network* matrix (hence totally unimodular). We show that the system (1.1)-(1.4) can be deduced from (1.5) by multiplying it from the left times a square invertible matrix  $\Delta \in \mathbb{R}^{s \times s}$ . In particular  $\Delta$  is a Kronecker product of Vandermonde matrices. Hence any real vector  $\mathbf{y} \geq 0$  is solution of (1.5) if and only the same  $\mathbf{y}$  is solution of (1.1)-(1.4).

- We provide a polyhedral convex cone  $\Omega \subset \mathbb{R}^s$  associated with (1.1)-(1.4) for some  $s \in \mathbb{N}$ , such that a direct application of Farkas lemma to the continuous system (1.1)-(1.4) implies that either  $b = Ax$  for some integral vector  $x \in \mathbb{N}^n$  or there exists  $\xi = (\xi_w) \in \Omega$  such that  $p_\xi(b) < 0$  for a polynomial  $p_\xi \in \mathbb{R}[u_1, \dots, u_m]$  of the form

$$(1.6) \quad u \mapsto p_\xi(u) = \sum_{w \in \mathbb{N}^m, w \neq 0} \xi_w u^w.$$

Thus (1.6) provides an explicit nonlinear *polynomial* certificate for IP, in contrast with the *linear* polynomial certificate fro LP obtained from the classical Farkas lemma.

In the discrete Farkas lemma presented in [5, 6] the author defines a polyhedral cone  $\Omega_2 \subset \mathbb{R}^s$  associated with (1.5), and proves that either  $b = Ax$  for some nonnegative integral vector  $x \in \mathbb{N}^n$  or there exists  $\pi \in \Omega_2$  such that  $(-1, 0, \dots, 0, 1) \cdot \pi < 0$ . It turns out that the vector  $\xi = (\xi_w)$  in (1.6) indeed satisfies  $\pi = \Delta' \xi$  for a square invertible matrix  $\Delta$  defined as the Kronecker product of Vandermonde matrices.

- Inspired by the relationships between the systems (1.1)-(1.4) and (1.5), we finally show that existence of a nonnegative integral solution  $x \in \mathbb{N}^n$  for the linear system  $Ax = b$  reduces to the existence of a nonnegative real solution  $\mathbf{y} \in \mathbb{R}^p$  for a system of linear equations of the

form:

$$M(-1, 0, \dots, 0, 1)' = M \Theta \mathbf{y},$$

where  $M \in \mathbb{R}^{s \times s}$  is any square invertible matrix. We can apply the standard Farkas lemma to any one of the linear systems presented above, and deduce a specific (Farkas) certificate for each choice the invertible matrix  $M$ . Each certificate can be seen as a *theorem of the alternative* of the form: the system  $b = Ax$  has no nonnegative integral solution  $x \in \mathbb{N}^n$  if and only if  $f(b) < 0$  for some given function  $f$ . For the particular choice  $M := \Delta'$ , existence of a nonnegative integral solution  $x \in \mathbb{N}^n$  for the linear system  $Ax = b$  reduces to existence of a nonnegative real solution  $\mathbf{y} \in \mathbb{R}^p$  for a system of linear equations of the form:

$$u^b - 1 = \mathbf{y}' D^{[u]}, \quad \forall u \in \mathbb{N}^m \quad \text{with} \quad u \leq b,$$

for some appropriate nonnegative integer vectors  $D^{[u]} \in \mathbb{N}^p$ . In this case, the function  $f$  involved in the Farkas certificate  $f(b) < 0$  has the exponential-like expansion

$$(1.7) \quad u \mapsto f(u) := \sum_{z \in \mathbb{N}^m} \xi_z \cdot (z^u - 1).$$

Both certificates (1.6) and (1.7) are different from the certificate obtained from the superadditive dual approach of Gomory and Johnson [2], Johnson [4], and Wolsey [16]. In particular, in [16] the linear system associated with such a certificate has dimension  $s^2 \times s$ , which is larger than the size  $ns \times s$  of the system (1.5) of this paper.

**The method.** A theorem of the alternative is obtained in three steps:

**{1}** One first shows that a linear system  $Ax = b$  (with  $A \in \mathbb{N}^{m \times n}$  and  $b \in \mathbb{N}^m$ ) has a nonnegative integral solution  $x \in \mathbb{N}^n$  if and only if the function  $f : \mathbb{Z}^m \rightarrow \mathbb{R}$  given by  $z \mapsto f(z) := b^z$  can be written as a linear combination of functions  $z \mapsto f_u(z) := (u + A_k)^z - u^z$  weighted by some nonnegative coefficients (for the indexes  $u \in \mathbb{N}^m$  with  $u \leq b$ ).

**{2}** One then shows that computing the nonnegative coefficients in the above linear decomposition of  $f$  is equivalent to finding a nonnegative real solution to a finite system of linear equations whose dimension is bounded from above by  $ns \times s$  with  $s := \prod_j (1 + b_j)$ .

**{3}** Finally one applies the standard continuous Farkas lemma to the linear system described in **{2}** and obtains the certificate (1.6).

This approach is similar in flavor but different from the one in [5, 6]. However, they are strictly equivalent and can be deduced one from each other under some appropriate linear transformation whose associated matrix  $\Delta \in \mathbb{N}^{s \times s}$  has a simple explicit form.

## 2. NOTATION AND DEFINITIONS

The notation  $\mathbb{R}$ ,  $\mathbb{Z}$  and  $\mathbb{N} = \{0, 1, 2, \dots\}$  stand for the usual sets of real, integer and natural numbers, respectively. Moreover, the set of positive integer numbers is denoted by  $\mathbb{N}^* = \mathbb{N} \setminus \{0\}$ . Given any vector  $b \in \mathbb{Z}^m$  and matrix  $A \in \mathbb{Z}^{m \times n}$ , the  $[k]$ -entry of  $b$  (resp.  $[j; k]$ -element of  $A$ ) is denoted by either  $b_k$  or  $b[k]$  (resp.  $A_{j;k}$  or  $A[j; k]$ ). The notation  $A'$  stands for the transpose of any matrix (or vector)  $A \in \mathbb{R}^{m \times n}$ ; and the  $k$ th column of the matrix  $A$  is denoted by  $A_k := (A_{1;k}, \dots, A_{m;k})'$ .

**The semi-group membership problem.** A classical result in group theory states that every abelian group  $G$  with  $m \in \mathbb{N}^*$  generators is isomorphic to some Cartesian product

$$G \cong [\mathbb{Z}/p_1\mathbb{Z}] \times [\mathbb{Z}/p_2\mathbb{Z}] \times \cdots \times [\mathbb{Z}/p_q\mathbb{Z}] \times [\mathbb{Z}^{m-q}],$$

for some set of numbers  $\{p_j\} \subset \mathbb{N}^*$  and  $q \leq m$ ; see e.g. [1]. One may even suppose that every  $p_j$  divides  $p_k$  whenever  $j < k$ . Therefore, if one introduces the *extended*  $m$ -dimensional vector:

$$(2.1) \quad P := (p_1, p_2, \dots, p_q, \infty, \dots, \infty)'$$

the abelian group  $G$  is isomorphic to the group  $\tilde{G}$  of vectors  $x \in \mathbb{Z}^m$  such that  $0 \leq x_j < p_j$  for every  $1 \leq j \leq q$ ; notice that  $q \leq m$ . The group sum  $x \oplus y$  of two elements  $x$  and  $y$  in  $\tilde{G} \subset \mathbb{Z}^m$  is then defined by

$$(2.2) \quad x \oplus y := (x + y) \bmod P \quad \text{in } \tilde{G},$$

where the sum  $x + y$  is the standard addition on  $\mathbb{Z}^m$  and the modulus of the sum  $(x + y) \bmod P$  is calculated entry by entry, so that for every index  $1 \leq k \leq m$ ,

$$(2.3) \quad [(x + y) \bmod P]_k = \begin{cases} (x_k + y_k) \bmod P_k & \text{if } P_k < \infty, \\ (x_k + y_k) & \text{if } P_k = \infty. \end{cases}$$

Hence from now on we suppose that  $G = \tilde{G} \subset \mathbb{Z}^m$ . Next let  $\{a_k\} \subset G$  be a collection of  $n$  elements of  $G$ . Each element  $a_k$  can be seen as a vector of  $\mathbb{Z}^m$ , for  $1 \leq k \leq n$ , so that the semi-group generated by  $\{a_k\}$  is the same as the set

$$\begin{aligned} G_a &:= \{Ax \bmod P \mid x \in \mathbb{N}^m\}, \quad \text{with} \\ A &:= [a_1 | a_2 | \cdots | a_n] \in \mathbb{Z}^{m \times n}. \end{aligned}$$

Thus, given  $b \in G$ , the semi-group membership problem of deciding whether  $b \in G_a$  is equivalent to deciding whether the system of linear

equations  $b = Ax \bmod P$  has a solution  $x \in \mathbb{N}^n$ . This in turn is equivalent to deciding whether the following system of linear equations

$$(2.4) \quad b = Ax + \begin{pmatrix} -B & B \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} u \\ w \end{pmatrix},$$

has a solution  $(x, u, w)$  in  $\mathbb{N}^n \times \mathbb{N}^q \times \mathbb{N}^q$ , where

$$(2.5) \quad B := \begin{pmatrix} p_1 & 0 & \cdots & 0 \\ 0 & p_2 & \cdots & 0 \\ \vdots & \vdots & \cdot & \vdots \\ 0 & 0 & \cdots & p_q \end{pmatrix} \in \mathbb{N}^{q \times q}.$$

Hence, with no loss of generality, the membership problem is equivalent to deciding whether some related system of linear equations  $\mathcal{A}x = b$  (with  $\mathcal{A} \in \mathbb{Z}^{m \times \ell}$  and  $b \in \mathbb{Z}^m$ ) has a solution  $x \in \mathbb{N}^\ell$ , which is the problem we will consider in the sequel.

### 3. EXISTENCE OF INTEGER SOLUTIONS TO $\{Ax = b, x \geq 0\}$

Let  $\mathbb{R}[z] = \mathbb{R}[z_1, \dots, z_m]$  be the ring of real polynomials in the variables  $z = (z_1, \dots, z_m)$  of  $\mathbb{R}^m$ . With  $\mathcal{A} \in \mathbb{Z}^{m \times \ell}$  we analyze existence of a nonnegative integer solution  $x \in \mathbb{N}^\ell$  to the system of linear equations  $\mathcal{A}x = b$ .

According to the computational complexity terminology in [14], let  $\varphi$  be the facet complexity of the rational convex polyhedron  $\mathbf{P} := \{x \in \mathbb{R}^\ell : x \geq 0, \mathcal{A}x = b\}$ . That is, each inequality in  $\mathcal{A}x \leq b$ ,  $\mathcal{A}x \geq b$ , and  $x \geq 0$  has size at most  $\varphi$ . Corollary 17.1b in [14, p. 239] states that  $\mathbf{P}$  contains an integral vector of size at most  $6\ell^3\varphi$ , if  $\mathbf{P}$  contains an integral vector  $x \in \mathbb{N}^\ell$ . Hence existence of an integral vector in  $\mathbf{P}$  is equivalent to analyze existence of an integral vector of the convex (compact) polytope

$$\widehat{\mathbf{P}} := \{x \in \mathbb{R}^\ell : x \geq 0, \mathcal{A}x = b, \sum_{i=1}^{\ell} x_i \leq M_{\mathcal{A},b}\},$$

where  $M_{\mathcal{A},b}$  is obtained explicitly from the facet complexity of  $\mathbf{P}$ .

**3.1. Reduction to  $A \in \mathbb{N}^{m \times n}$ .** In view of the above one may restrict our analysis to the existence of a nonnegative integral solution  $x \in \mathbb{N}^n$  for a system of linear equations  $Ax = b$  associated with a rational convex *polytope*  $\mathbf{P} := \{x \in \mathbb{R}^n : Ax = b, x \geq 0\}$ , where  $A \in \mathbb{Z}^{m \times n}$  and  $b \in \mathbb{Z}^m$ . But this in turn implies that one may restrict our analysis to existence of a nonnegative integral solution  $y \in \mathbb{N}^{n+1}$  to a system of linear equations  $A^*y = b^*$  where  $A^* \in \mathbb{N}^{[m+1] \times [n+1]}$  and  $b^* \in \mathbb{N}^{m+1}$ .



Indeed, if  $A \in \mathbb{Z}^{m \times n}$  and  $A \notin \mathbb{N}^{m \times n}$ , let  $\alpha \in \mathbb{N}^n$  be such that

$$(3.1) \quad \widehat{A}_{j;k} := A_{j;k} + \alpha_k \geq 0; \quad \forall 1 \leq j \leq m, 1 \leq k \leq n.$$

Since  $\mathbf{P}$  is a (compact) polytope,

$$(3.2) \quad \rho := \max_{x \in \mathbb{N}^n, Ax=b} \left\{ \sum_{k=1}^n \alpha_k x_k \right\} < \infty.$$

In particular  $\rho \in \mathbb{N}$ . Now define  $\widehat{b} \in \mathbb{N}^m$  by

$$(3.3) \quad \widehat{b} := b + \rho e_m \geq 0 \quad \text{with} \quad e_m := (1, \dots, 1)' \in \mathbb{N}^m.$$

Let  $\widehat{A} \in \mathbb{N}^{m \times n}$  be defined as in (3.1). The solutions  $x \in \mathbb{N}^n$  to the original system  $Ax = b$  are in one-to-one correspondence with the solutions  $(x, u) \in \mathbb{N}^n \times \mathbb{N}$  to the extended system

$$(3.4) \quad \begin{aligned} \widehat{A}x + e_m u &= \widehat{b}, \\ \alpha'x + u &= \rho. \end{aligned}$$

Indeed, if  $Ax = b$  with  $x \in \mathbb{N}^n$ , then

$$Ax + e_m \left[ \sum_{k=1}^n \alpha_k x_k \right] - e_m(\alpha'x) + \rho e_m = b + \rho e_m.$$

The following identity follows from the definitions for  $\widehat{A} \in \mathbb{N}^{m \times n}$  and  $\widehat{b} \in \mathbb{N}^m$  given in (3.1)-(3.3) :

$$\widehat{A}x + e_m u = \widehat{b} \quad \text{with} \quad u := \rho - \alpha'x \in \mathbb{Z}.$$

Notice that  $u \geq 0$  because  $\rho \geq \alpha'x$  according to (3.2), so that  $(x, u)$  is the integer nonnegative solution of (3.4) that we are looking for. Conversely let  $(x, u) \in \mathbb{Z}^{n+1}$  be a solution to (3.4). The definitions for  $\widehat{A} \in \mathbb{N}^{m \times n}$  and  $\widehat{b} \in \mathbb{N}^m$  given in (3.1)-(3.3) imply that

$$Ax + e_m \left[ \sum_{k=1}^n \alpha_k x_k \right] + e_m u = b + \rho e_m,$$

so that  $Ax = b$  with  $x \in \mathbb{N}^n$  because  $u = \rho - \alpha'x$ . Hence the existence any solution  $x \in \mathbb{N}^n$  to  $Ax = b$  is completely equivalent to the existence any solution  $(x, u) \in \mathbb{N}^{n+1}$  to

$$\begin{pmatrix} \widehat{b} \\ \rho \end{pmatrix} = A^* \cdot \begin{pmatrix} x \\ u \end{pmatrix} \quad \text{with} \quad A^* := \begin{pmatrix} \widehat{A} & e_m \\ \alpha' & 1 \end{pmatrix},$$

and the new matrix  $A^* \in \mathbb{N}^{[m+1] \times [n+1]}$  has only nonnegative integer entries.

**3.2. The main result.** Given vectors  $b \in \mathbb{N}^m$  and  $z \in \mathbb{R}^m$ , the notation  $z^b$  stands for the monomial  $z_1^{b_1} z_2^{b_2} \cdots z_m^{b_m} \in \mathbb{R}[z]$ . We also need to define a pair of matrices  $\Delta$  and  $\Theta$  that we will use in the sequel.

**Definition 1.** Let  $A \in \mathbb{N}^{m \times n}$  and  $\beta \in \mathbb{N}^m$  be such that  $A_k \leq \beta$  for each index  $1 \leq k \leq n$ . Set the integers

$$(3.5) \quad s := \prod_{j=1}^m (1 + \beta_j) \quad \text{and} \quad p := \sum_{k=1}^n \prod_{j=1}^m (1 + \beta_j - A_{j;k}) \leq ns.$$

Let  $\Delta \in \mathbb{N}^{s \times s}$  be a square Vandermonde matrix whose rows and columns are indexed with the nonnegative vectors  $z, w \in \mathbb{N}^m$  (according to e.g. the lexicographic ordering) so that the  $[z; w]$ -entry is given by

$$(3.6) \quad \Delta[z; w] = w^z = w_1^{z_1} w_2^{z_2} \cdots w_m^{z_m} \quad \forall z, w \leq \beta;$$

and where we use the convention that  $0^0 = 1$ .

Let  $\Theta \in \mathbb{Z}^{s \times p}$  be a network matrix whose rows and columns are respectively indexed with the nonnegative vectors  $w \in \mathbb{N}^m$  and  $(k, u) \in \mathbb{N} \times \mathbb{N}^m$ , so that the  $(w; (k, u))$ -entry is given by

$$(3.7) \quad \Theta[w; (k, u)] = \begin{cases} -1 & \text{if } w = u \leq \beta - A_k, \\ 1 & \text{if } w = u + A_k \leq \beta, \\ 0 & \text{otherwise,} \end{cases}$$

for all indexes  $w \leq \beta$ ,  $u \leq \beta - A_k$ , and  $1 \leq k \leq n$ .

The following result is straightforward.

**Lemma 2.** The square Vandermonde matrix  $\Delta \in \mathbb{R}^{s \times s}$  in (3.6) is invertible. The matrix  $\Theta \in \mathbb{R}^{s \times p}$  in (3.7) is a network matrix, and so it is totally unimodular.

*Proof.* It is easy to see that  $\Delta$  is invertible because it is the Kronecker product  $D^{[1]} \otimes D^{[2]} \otimes \cdots \otimes D^{[m]}$  of  $m$  square Vandermonde matrices

$$(3.8) \quad D^{[j]} = \begin{pmatrix} 1 & 1^0 & 2^0 & \cdots & (\beta_j)^0 \\ 0 & 1^1 & 2^1 & \cdots & (\beta_j)^1 \\ \vdots & \vdots & \vdots & \cdot & \vdots \\ 0 & 1^{\beta_j} & 2^{\beta_j} & \cdots & (\beta_j)^{\beta_j} \end{pmatrix};$$

see e.g. [3, 17]. And each  $D^{[j]}$  is obviously invertible. By inspection it turns out that  $\Theta$  is a *network matrix*, that is, it is a matrix with only  $\{0, \pm 1\}$  entries and with exactly two nonzero entries 1 and  $-1$  in each column. Therefore  $\Theta$  is totally unimodular; see e.g. Schrijver [14, p. 274].  $\square$

**Definition 3.** Given a finite set  $U \subset \mathbb{N}^m$  and a collection of coefficients  $q[u] \in \mathbb{R}$ , we say that the polynomial

$$z \rightarrow Q(z) = \sum_{u \in U} q[u] z^u = \sum_{u \in U} q[u] z_1^{u_1} z_2^{u_2} \cdots z_m^{u_m}$$

has multivariate degree bounded by a vector  $\beta \in \mathbb{N}^m$  if and only if  $u \leq \beta$  for every  $u \in U$ .

The following technical result was essentially shown in [5, 6] but we include the proof for the sake of completeness.

**Theorem 4.** Let  $\beta, b \in \mathbb{N}^m$  and  $A \in \mathbb{N}^{m \times n}$  be such that :

$$(3.9) \quad \beta \geq b \quad \text{and} \quad \beta \geq A_k \quad \text{for all} \quad 1 \leq k \leq n.$$

The following three statements **(a)**, **(b)** and **(c)** are all equivalent :

**(a):** The linear system  $Ax = b$  has a solution  $x \in \mathbb{N}^n$ .

**(b):** The polynomial  $z \mapsto z^b - 1 := z_1^{b_1} z_2^{b_2} \cdots z_m^{b_m} - 1$  can be written as follows :

$$(3.10) \quad z^b - 1 = \sum_{k=1}^n Q_k(z) (z^{A_k} - 1)$$

for some real polynomials  $Q_k \in \mathbb{R}[z_1, z_2, \dots, z_m]$  with nonnegative coefficients and multivariate degree bounded by the vector  $\beta - A_k$ , for all  $1 \leq k \leq n$ .

**(c):** There is a real nonnegative solution  $\mathbf{y} \in \mathbb{R}^p$  for the system of linear equations

$$(3.11) \quad \mathbf{b} = \Theta \mathbf{y},$$

where  $\Theta \in \mathbb{Z}^{s \times p}$  is given as in (3.7) of Definition 1 and the new vector  $\mathbf{b} \in \mathbb{Z}^s$  has entries indexed with the nonnegative vector  $w \in \mathbb{N}^m$ , so that the  $[w]$ -entry is given by

$$(3.12) \quad \mathbf{b}[w] := \begin{cases} -1 & \text{if } w = 0, \\ 1 & \text{if } w = b, \\ 0 & \text{otherwise.} \end{cases} \quad \forall 0 \leq w \leq \beta.$$

Notice that  $\Theta \in \mathbb{Z}^{s \times p}$  in (3.7) and (3.11) is determined only by the entries of  $\beta \in \mathbb{N}^m$  and  $A \in \mathbb{N}^{m \times n}$ , so that  $\Theta$  is independent of  $b \in \mathbb{Z}^m$ . Observe that if  $b \geq A_k$  for every  $1 \leq k \leq n$ , then one may take  $\beta := b$ .

*Proof.* **(a)**  $\Rightarrow$  **(b)**. Suppose that  $b = Ax$  for some  $x \in \mathbb{N}^n$ . Consider the following polynomials (where we use the convention  $\sum_{q=0}^{-1}(\cdot) = 0$ )

$$\begin{aligned} z \mapsto Q_1(z) &= \sum_{q=0}^{x_1-1} z^{qA_1}, \\ z \mapsto Q_2(z) &= z^{x_1A_1} \sum_{q=0}^{x_2-1} z^{qA_2}, \\ z \mapsto Q_3(z) &= z^{x_1A_1} z^{x_2A_2} \sum_{q=0}^{x_3-1} z^{qA_3}, \\ &\dots \\ z \mapsto Q_n(z) &= \left[ \prod_{k=1}^{n-1} z^{x_k A_k} \right] \sum_{q=0}^{x_n-1} z^{qA_n}. \end{aligned}$$

It is easy to see that the polynomials  $Q_k$  satisfy equation (3.10). Moreover each  $Q_k$  has nonnegative coefficients, and the multivariate degree of  $Q_k$  is bounded by the vector  $\beta - A_k$  for  $1 \leq k \leq n$  because  $b \leq \beta$ .

**(b)**  $\Leftrightarrow$  **(c)**. Existence of polynomials  $Q_k \in \mathbb{R}[z_1, z_2, \dots, z_m]$  with nonnegative coefficients and multivariate degree bounded by the vector  $\beta - A_k$  (for all  $1 \leq k \leq n$ ) is equivalent to the existence of real coefficients  $y[k, u] \geq 0$  such that

$$Q_k(z) = \sum_{u \in \mathbb{N}^m, u \leq \beta - A_k} y[k, u] z^u \quad \forall \quad 1 \leq k \leq n.$$

Then rewrite equation (3.10) as follows:

$$(3.13) \quad z^b - 1 = \sum_{k=1}^n \sum_{\substack{u \in \mathbb{N}^m, \\ u \leq \beta - A_k}} y[k, u] (z^{u+A_k} - z^u),$$

The vector of coefficients  $\mathbf{y} = (y[k, u]) \geq 0$  satisfies (3.13) if and only if it satisfies the following system of linear equations

$$(3.14) \quad \mathbf{b} = \Theta \cdot \begin{pmatrix} y[1, (0, \dots, 0, 0)] \\ y[1, (0, \dots, 0, 1)] \\ \vdots \\ y[n, (\beta - A_n)] \end{pmatrix},$$

where  $\mathbf{b} \in \mathbb{Z}^s$  is given in (3.12) and the matrix  $\Theta \in \mathbb{Z}^{s \times p}$  is given in (3.7), that is, such that

$$\Theta[w; (k, u)] = \begin{cases} -1 & \text{if } w = u \leq b - A_k, \\ 1 & \text{if } w = u + A_k \leq b, \\ 0 & \text{otherwise.} \end{cases}$$

Each row in (3.14) is indexed with the monomial  $z^w \in \mathbb{N}^m$ , for  $w \in \mathbb{N}^m$  and  $w \leq b$  (according to e.g. the lexicographic ordering).

(c)  $\Rightarrow$  (a). Let  $\mathbf{y} = (y[k, u]) \geq 0$  be a real vector such that (3.11) and (3.14) hold. The matrix  $\Theta$  is totally unimodular according to Lemma 2, and so there exists a nonnegative *integer* solution  $\hat{\mathbf{y}} = (\hat{y}[k, u]) \geq 0$  to (3.11) and (3.14) because the left-hand-side of (3.14) is an integral vector. Therefore (3.13) also holds with the new vector  $\hat{\mathbf{y}}$ , that is:

$$z^b - 1 = \sum_{k=1}^n \sum_{\substack{u \in \mathbb{N}^m, \\ u \leq \beta - A_k}} \hat{y}[k, u] (z^{u+A_k} - z^u).$$

Given a fixed index  $1 \leq j \leq m$ , differentiate both sides of the equation above with respect to the variable  $z_j$  and evaluate at the point  $z = (1, 1, \dots, 1)$ , so as to obtain:

$$(3.15) \quad b_j = \sum_{k=1}^n A_{j;k} x_k, \quad \text{with} \quad x_k := \sum_{\substack{u \in \mathbb{N}^m, \\ u \leq \beta - A_k}} \hat{y}[k, u].$$

The nonnegative integer vector  $x = (x_1, \dots, x_n)' \in \mathbb{N}^n$  satisfies the desired result  $Ax = b$ .  $\square$

**Remark 5.** *One linear constraint in (3.11) is redundant, because the addition of all the rows in (3.11)-(3.12) yields the trivial equality  $0 = 0 \mathbf{y}$  (recall that  $\Theta$  is a matrix with only  $\{0, \pm 1\}$  entries and with exactly two nonzero entries 1 and  $-1$  in each column).*

**Remark 6.** *The matrix  $\Theta \in \mathbb{Z}^{s \times p}$  in (3.7) is independent of  $b$  and contains all information about all the integer problems  $Ax = b$  for  $x \in \mathbb{N}^n$  and  $b \in \mathbb{N}^m$  with  $b \leq \beta$ .*

The linear system  $\mathbf{b} = \Theta \mathbf{y}$  in (3.11) of Theorem 4 is quite interesting in the sense that existence of a real solution  $\mathbf{y} \geq 0$  is totally equivalent to the existence of a nonnegative integer solution  $x \in \mathbb{N}^n$  for the problem  $Ax = b$ , but it is not easy to see at first glance what is the relation between the two solutions  $\mathbf{y}$  and  $x$ . Moreover equation (3.11) in Theorem 4 is not unique at all. We can multiply both sides of (3.11)

by any square invertible matrix  $M \in \mathbb{R}^{s \times s}$  and we obtain that  $\mathbf{y} \geq 0$  is a real solution to (3.11) if and only if  $\mathbf{y}$  is also a solution for

$$M\mathbf{b} = M\Theta\mathbf{y}.$$

An interesting issue is to determine what is an adequate matrix  $M$  such that relationship between the solutions  $\mathbf{y} \geq 0$  and  $x \in \mathbb{N}^n$  is evident. We claim that one of such matrix  $M$  is the square Vandermonde matrix  $\Delta \in \mathbb{N}^{s \times s}$  presented in (3.6) of Definition 1. We use the convention that  $0^0 = 1$  and  $0^z = 0$  whenever  $0 \neq z \in \mathbb{N}^m$ .

**Theorem 7.** *Let  $\beta, b \in \mathbb{N}^m$  and  $A \in \mathbb{N}^{m \times n}$  be such that :*

$$(3.16) \quad \beta \geq b \quad \text{and} \quad \beta \geq A_k \quad \text{for all} \quad 1 \leq k \leq n.$$

*The following three statements (a), (b) and (c) are all equivalent :*

**(a):** *The linear system  $Ax = b$  has a solution  $x \in \mathbb{N}^n$ .*

**(b):** *There is a real nonnegative solution  $\mathbf{y} = (y[k, u]) \in \mathbb{R}^p$  to the system of linear equations*

$$(3.17) \quad b^z - 0^z = \sum_{k=1}^n \sum_{\substack{u \in \mathbb{N}^m, \\ u \leq \beta - A_k}} y[k, u] ((u + A_k)^z - u^z),$$

*for every  $z \in \mathbb{N}^m$  with  $0 \leq z \leq \beta$ .*

**(c):** *There is a real nonnegative solution  $\mathbf{y} = (y[k, u]) \in \mathbb{R}^p$  to the system of linear equations*

$$(3.18) \quad z^b - 1 = \sum_{k=1}^n \sum_{\substack{u \in \mathbb{N}^m, \\ u \leq \beta - A_k}} y[k, u] (z^{u + A_k} - z^u),$$

*for every  $z \in \mathbb{N}^m$  with  $0 \leq z \leq \beta$ .*

*Proof.* The equivalence **(a)**  $\Leftrightarrow$  **(b)** easily follows from Theorem 4 after noticing that the  $[z; (k, u)]$ -entry (resp.  $[z]$ -entry) of the product  $\Delta\Theta$  (resp.  $\Delta\mathbf{b}$ ) is given by

$$(3.19) \quad (\Delta\Theta)[z; (k, u)] = ((u + A_k)^z - u^z) \in \mathbb{N},$$

$$(3.20) \quad \text{resp.} \quad (\Delta\mathbf{b})[z] = (b^z - 0^z),$$

for all nonnegative indexes  $z \in \mathbb{N}^m$  and  $(k, u) \in \mathbb{N} \times \mathbb{N}^m$  with  $z \leq \beta$ ,  $u \leq \beta - A_k$  and  $1 \leq k \leq n$ .

The equivalence **(a)**  $\Leftrightarrow$  **(c)** is proved in a similar way; we only need to observe that multiplying by the transpose  $\Delta'$  is equivalent to interchange the exponentials  $z \rightarrow w^z$  by powers  $z \rightarrow z^w$ , so that:

$$\begin{aligned} (\Delta' \Theta)[z; (k, u)] &= (z^{u+A_k} - z^u) \in \mathbb{N}, \\ \text{and } (\Delta' \mathbf{b})[z] &= (z^b - z^0). \end{aligned}$$

□

**Remark 8.** *A nonnegative real vector  $\mathbf{y} \in \mathbb{R}^p$  is a solution of equation (3.11) in Theorem 4 if and only if  $\mathbf{y}$  is also a solution of (3.17) and (3.18). Moreover the linear system (3.18) can be directly deduced from (3.10) by evaluating at  $z \in \mathbb{N}^m$  with  $z \leq b$ .*

#### 4. A HIERARCHY OF LINEAR PROGRAMMING RELAXATIONS

Let  $\beta, b \in \mathbb{N}^m$  and  $A \in \mathbb{N}^{m \times n}$  be such that  $\beta \geq b$  and  $\beta \geq A_k$  for all  $1 \leq k \leq n$ . Consider the matrices  $\Delta \in \mathbb{R}^{s \times s}$  and  $\Theta \in \mathbb{R}^{s \times p}$  given in equations (3.6)-(3.7) of Definition 1; and define the new vector  $\mathbf{b} \in \mathbb{Z}^s$  whose entries are indexed with the non negative vector  $w \in \mathbb{N}^m$ , so that the  $[k]$ -entry is given by (3.12) :

$$(4.1) \quad \mathbf{b}[w] := \begin{cases} -1 & \text{if } w = 0, \\ 1 & \text{if } w = b, \\ 0 & \text{otherwise,} \end{cases} \quad \forall 0 \leq w \leq \beta.$$

The fact that  $\Delta$  is invertible (according to Lemma 2) allows us to give two equivalent definitions of the following polytope in  $\mathbb{R}^p$ ,

$$(4.2) \quad \begin{aligned} \mathcal{P} &:= \{\mathbf{y} \in \mathbb{R}^p : \mathbf{y} \geq 0, \Delta \Theta \mathbf{y} = \Delta \mathbf{b}\} \\ &= \{\mathbf{y} \in \mathbb{R}^p : \mathbf{y} \geq 0, \Theta \mathbf{y} = \mathbf{b}\} \subset \mathbb{R}^p. \end{aligned}$$

As it is state in Remark 8, any nonnegative vector  $\mathbf{y} \in \mathbb{R}^p$  is a solution to (3.17) if and only if  $\mathbf{y}$  lies in  $\mathcal{P}$ . Let  $\mathbf{y} = (y[k, u])$  be an element of  $\mathcal{P}$ . The entries of  $\mathbf{y}$  are indexed according to Theorems 4 and 7. Equation (3.17) implies that  $x \in \mathbb{R}^n$  with  $x_k := \sum_u y[k, u]$ , is a solution to  $Ax = b$ . Indeed  $b_j = \sum_k A_{j;k} x_k$  for  $1 \leq j \leq m$  after evaluating (3.17) at  $z = e_j$ , the basic vector whose entries are all equal to zero, except the  $j$ -entry which is equal to one, so that  $w^{e_j} = w_j$  for all  $w \in \mathbb{Z}^m$ . The relationship between  $x$  and  $\mathbf{y}$  comes from a multiplication

by some matrix  $E \in \mathbb{N}^{n \times p}$ , that is :

$$(4.3) \quad x = E\mathbf{y} \quad \text{with} \quad E := \begin{pmatrix} \overbrace{1 \dots 1}^{p_1} & \overbrace{0 \dots 0}^{p_2} & \dots & \overbrace{0 \dots 0}^{p_n} \\ 0 \dots 0 & 1 \dots 1 & \dots & 0 \dots 0 \\ \dots & \dots & \dots & \dots \\ 0 \dots 0 & 0 \dots 0 & \dots & 1 \dots 1 \end{pmatrix},$$

where  $p_k := \prod_{j=1}^m (1 + \beta_j - A_{j;k})$  for  $1 \leq k \leq n$ , so that  $p = \sum_k p_k$  according to (3.5) in Definition 1. We obtain the following result as a consequence of Theorem 7.

**Corollary 9.** *Let  $\beta, b \in \mathbb{N}^m$  and  $A \in \mathbb{N}^{m \times n}$  be such that  $\beta \geq b$  and  $\beta \geq A_k$  for each index  $1 \leq k \leq n$ .*

**(a):** *Existence of a nonnegative integral solution  $x \in \mathbb{N}^n$  to the linear system  $Ax = b$  reduces to the existence of a nonnegative real solution  $\mathbf{y} = (y[k, u]) \in \mathbb{R}^p$  to the system of linear equations :*

$$(4.4) \quad b_i = \mathbf{y}'A^{(e_j)}, \quad \forall 1 \leq j \leq m;$$

$$(4.5) \quad b_i b_j = \mathbf{y}'A^{(e_i + e_j)}, \quad \forall 1 \leq i \leq j \leq m;$$

$$\dots = \dots$$

$$(4.6) \quad b_1^{z_1} \dots b_m^{z_m} = \mathbf{y}'A^{(z)}, \quad \left( \begin{array}{l} \forall 0 \leq z_j \leq b_j, \\ z_1 + \dots + z_m = \delta; \end{array} \right)$$

$$\dots = \dots$$

$$(4.7) \quad b_1^{\beta_1} \dots b_m^{\beta_m} = \mathbf{y}'A^{(\beta)};$$

for some appropriate nonnegative integer vectors  $A^{(e_j)}, A^{(e_i + e_j)}, A^{(z)} \in \mathbb{N}^p$  with  $z \in \mathbb{N}^m$  and  $z \leq \beta$ . The parameter  $\delta \geq 1$  in (4.6) is the degree of the monomial  $b \mapsto b^z$ , and we use the indexation for the entries of  $\mathbf{y}$  given in Theorems 4 and 7. In particular all vectors  $A^{(z)}$  are independent of  $b$ , and the entries of  $A^{(e_j)} \in \mathbb{N}^p$  in (4.4) are given by :

$$A^{(e_j)}[k, u] := A_{j;k},$$

for all  $u \in \mathbb{N}^m$ ,  $1 \leq j \leq m$ , and  $1 \leq k \leq n$  with  $u \leq \beta - A_k$ .

**(b):** *Let  $\mathbf{y} \in \mathbb{R}^p$  be a nonnegative real solution to (4.4)-(4.7) and  $\hat{x} = E\mathbf{y}$ , i.e.  $\hat{x}_k := \sum_u y[k, u]$  for  $1 \leq k \leq n$ . Then  $\hat{x}$  belongs to the integer hull  $H$  of  $\{x \in \mathbb{R}^n : Ax = b, x \geq 0\}$ . Therefore a certificate of  $b \neq Ax$  for any  $x \in \mathbb{N}^n$  is obtained as soon as any subsystem of (4.4)-(4.7) has no solution  $\mathbf{y} \in \mathbb{R}^p$ .*

Moreover, any nonnegative vector  $\mathbf{y} \in \mathbb{R}^p$  is a solution to (4.4)-(4.7) if and only if  $\mathbf{y} \in \mathcal{P}$  (with  $\mathcal{P}$  as in (4.2)); and there is a one-to-one correspondance between the vertices of  $H$  and  $\mathcal{P}$ .



*Proof.* **(a)** It is straightforward to see that (4.4)-(4.7) is just an explicit description of (3.17) in Theorem 7. The right-hand-side terms of (4.4)-(4.7) are the function  $b^z - 0^z$  evaluated at  $z \in \mathbb{N}^m$  with  $z \leq \beta$  and  $\sum_j z_j$  equal to 1, 2, 3, etc., until the maximal degree  $\sum_j \beta_j$ . Each vector  $A^{(z)} \in \mathbb{N}^p$  is then the transpose of the  $[z]$ -row of the product  $\Delta\Theta$  calculated in (3.19), so that

$$A^{(z)}[k, u] := (\Delta\Theta)[z; (k, u)] = ((u + A_k)^z - u^z) \in \mathbb{N},$$

for all appropriated indices  $z$ ,  $k$ , and  $u$ . Evaluating (3.17) at  $z = 0$  yields the trivial identity  $0 = 0\mathbf{y}$  (recall Remark 5), because we are using the convention that  $0^0 = 1$  and  $0^w = 0$  for every  $w \neq 0$ . While evaluating (3.17) at  $z = e_j$ , yields the linear constraints

$$b_j = \sum_{k=1}^n A_{j;k} \sum_{\substack{u \in \mathbb{N}^m, \\ u \leq \beta - A_k}} y[k, u] \quad \forall 1 \leq j \leq m,$$

because  $w^{e_j} = w_j$  for all  $w \in \mathbb{Z}^m$ . Constraints (4.4) are easily deduced after defining the vectors  $A^{(e_j)} \in \mathbb{N}^p$  by  $A^{(e_j)}[k, u] := A_{j;k}$  for all  $u$  and  $1 \leq k \leq n$ . We also have that  $b = A\hat{x}$  with  $\hat{x} = E\mathbf{y}$  and  $E \in \mathbb{N}^{n \times p}$  the matrix given in (4.3), e.g.  $\hat{x}_k = \sum_u y[k, u]$  for  $1 \leq k \leq n$ .

**(b)** Let  $\mathcal{P} \in \mathbb{R}^p$  be the polytope given in (4.2), and  $H \subset \mathbb{R}^n$  be the integer hull of  $\{x \in \mathbb{R}^n : Ax = b, x \geq 0\}$ . From Theorem 4 and the proof of Theorem 7, any nonnegative vector  $\mathbf{y} \in \mathbb{R}^p$  is a solution to (3.17) if and only if  $\mathbf{y} \in \mathcal{P}$ , because  $\Theta\mathbf{y} = \mathbf{b}$ ; and we have already stated in the proof of **(a)** that (4.4)-(4.7) is completely equivalent to (3.17). We also deduced that  $\hat{x} = E\mathbf{y}$  is a solution to  $A\hat{x} = b$  for any feasible solution  $\mathbf{y} \in \mathcal{P}$ . Conversely, given any nonnegative integer solution  $x \in \mathbb{N}^n$  to  $Ax = b$  and working as in the proof of Theorem 4, we can associate with  $x$  a nonnegative integer vector  $\mathbf{y}(x) \in \mathbb{N}^p$  such that  $\Theta\mathbf{y}(x) = \mathbf{b}$  and  $x = E\mathbf{y}(x)$ ; hence  $\mathbf{y}(x) \in \mathcal{P}$ .

Let  $\{\mathbf{y}^{[\ell]} \in \mathbb{N}^p\}$  be the vertices of  $\mathcal{P}$ . Every  $\mathbf{y}^{[\ell]}$  has nonnegative integer entries, because  $\Theta$  is totally unimodular and the vector  $\mathbf{b}$  in (4.1) has integer entries. Each vector  $E\mathbf{y}^{[\ell]} \in \mathbb{N}^n$  has nonnegative integer entries and satisfies  $A E\mathbf{y}^{[\ell]} = b$ , so that  $E\mathbf{y}^{[\ell]} \in H$ . Any feasible solution  $\mathbf{y} \in \mathcal{P}$  can be expressed as the sum  $\mathbf{y} = \sum_\ell \xi_\ell \mathbf{y}^{[\ell]}$  with  $\sum_\ell \xi_\ell = 1$  and  $\xi_\ell \geq 0$  for each  $l$ . Hence,

$$E\mathbf{y} = \sum_\ell \xi_\ell E\mathbf{y}^{[\ell]} \quad \text{with} \quad E\mathbf{y}^{[\ell]} \in H \quad \forall \ell,$$

and so  $\hat{x} := E\mathbf{y} \in H$ . Conversely, let  $\{x^{[c]} \in \mathbb{N}^n\}$  be the vertices of  $H$ . We claim that every  $\mathbf{y}(x^{[c]})$  is a vertex of  $\mathcal{P}$ ; otherwise if  $\mathbf{y}(x^{[c]}) =$

$\sum_{\ell} \xi_{\ell} \mathbf{y}^{[\ell]}$  for  $0 \leq \xi_{\ell} < 1$ , then

$$x^{[c]} = E\mathbf{y}(x^{[c]}) = \sum_{\ell} \xi_{\ell} E\mathbf{y}^{[\ell]} \quad \text{with} \quad E\mathbf{y}^{[\ell]} \in H,$$

is a combination of vertices ( $E\mathbf{y}^{[\ell]}$ ) of  $H$ , in contradiction with the fact that  $x^{[c]}$  itself is a vertex of  $H$ .  $\square$

**4.1. A hierarchy of LP-relaxations.** Let  $|z| := z_1 + \dots + z_m$  for every  $z \in \mathbb{N}^m$ . Consider the following integer and linear programming problems, for  $1 \leq \ell \leq |\beta|$ ,

$$(4.8) \quad J_{\bullet} := \min_x \{c'x : Ax = b, x \in \mathbb{N}^n\};$$

$$(4.9) \quad J_{\ell} := \min_{\mathbf{y}} \left\{ c'E\mathbf{y} : \begin{array}{l} b^z = \mathbf{y}'A^{(z)}, \mathbf{y} \in \mathbb{R}^p, \mathbf{y} \geq 0, \\ z \in \mathbb{N}^m, 1 \leq |z| \leq \ell \end{array} \right\}.$$

We easily have the following result.

**Corollary 10.** *Let  $\beta, b \in \mathbb{N}^m$  and  $A \in \mathbb{N}^{m \times n}$  be such that  $\beta \geq b$  and  $\beta \geq A_k$  for every index  $1 \leq k \leq n$ . Let  $J_{\bullet}$  and  $J_{\ell}$  be as in (4.8) and (4.9) respectively.*

*Then :  $J_1 \leq J_2 \leq \dots \leq J_{|\beta|}$  and  $J_{|\beta|} = J_{\bullet}$ .*

*Proof.* It is obvious that  $J_{\ell} \leq J_{\ell^*}$  whenever  $\ell \leq \ell^*$ . Moreover :

$$J_{\bullet} = \min_x \{c'x : x \in H\} \quad \text{and} \quad J_{|\beta|} = \min_{\mathbf{y}} \{c'E\mathbf{y} : \mathbf{y} \in \mathcal{P}\},$$

where  $H$  is the integer convex hull of  $\{x \in \mathbb{R}^n : Ax = b, x \geq 0\}$  and  $\mathcal{P}$  is given in (4.2). Thus  $J_{\bullet} = c'x^{[d]}$  for some vertex  $x^{[d]}$  of  $H$ . Working as in the proof of Corollary 9,  $\mathbf{y}(x^{[d]})$  is a vertex of  $\mathcal{P}$  and  $x^{[d]} = E\mathbf{y}(x^{[d]})$ , so that

$$J_{|\beta|} \leq c'E\mathbf{y}(x^{[d]}) = J_{\bullet}.$$

On the other hand,  $J_{|\beta|} = c'E\mathbf{y}^{[\kappa]}$  for some vertex  $\mathbf{y}^{[\kappa]}$  of  $\mathcal{P}$ . Again, as in the proof of Corollary 9,  $E\mathbf{y}^{[\kappa]} \in H$ , so that

$$J_{\bullet} \leq c'E\mathbf{y}^{[\kappa]} = J_{|\beta|}.$$

$\square$

Hence the sequence of LP problems  $\{J_{\ell}\}_{1 \leq \ell \leq |\beta|}$  in (4.9) provides a monotone sequence of lower bounds for  $J_{\bullet}$  with finite convergence limit  $J_{|\beta|} = J_{\bullet}$ . Observe that all linear programs (4.9) have the same number  $p$  of variables (since  $\mathbf{y} \in \mathbb{R}^p$ ) and an increasing number of constraints starting from  $m$  when  $\ell = 1$  to  $s = \prod_j (\beta_j + 1)$  when  $\ell = |\beta|$ . The most interesting case happens when we take  $b = \beta \geq A_k$  (for every index  $1 \leq k \leq n$ ).

Of course  $p (< ns)$  is large; but in principle the LP problems (4.9) are amenable to computation for reasonable values of  $\ell$  by using column generation techniques (in order to avoid handling the full vector  $\mathbf{y} \in \mathbb{R}^p$ ). However the vectors  $A^{(z)} \in \mathbb{N}^p$  may contain very large values when  $|z| = \ell$  is large, and so some numerical ill-conditioned cases are likely to appear for large values of  $\ell$ .

Therefore it is not completely clear whether the hierarchy of linear relaxations presented in Corollary 9 is useful from a computational point of view, but we think this hierarchy provides some new insights into integer programming problems from a theoretical point of view.

**4.2. A polynomial certificate.** Let  $\beta, b \in \mathbb{N}^m$  and  $A \in \mathbb{N}^{m \times n}$  be such that  $\beta \geq b$  and  $\beta \geq A_k$  for every index  $1 \leq k \leq n$ . Consider the matrices  $\Delta \in \mathbb{N}^{s \times s}$  and  $\Theta \in \mathbb{Z}^{s \times p}$  given in (3.6)-(3.7) of Definition 1. Lemma 2 states that  $\Delta$  is invertible, and so Theorem 4 implies that existence of a nonnegative integer solution  $x \in \mathbb{N}^n$  to  $Ax = b$  is equivalent to the existence of a nonnegative real solution  $\mathbf{y} \in \mathbb{R}^p$  to

$$(4.10) \quad \Delta\Theta\mathbf{y} = \Delta\mathbf{b} \quad \text{and} \quad \mathbf{y} \geq 0,$$

where  $\mathbf{b} \in \mathbb{Z}^s$  is given in (3.12) or (4.1). Moreover it was already stated in (3.20) that the entries of the product  $\Delta\mathbf{b}$  can be indexed with the nonnegative vector  $z \in \mathbb{N}^m$  with  $z \leq \beta$ , and that they have the simple representation :

$$(4.11) \quad (\Delta\mathbf{b})[z] = (b^z - 0^z) = \begin{cases} 0 & \text{if } z = 0, \\ b^z & \text{if } z \neq 0, \end{cases}$$

using the conventions  $0^0 = 1$  and  $0^w = 0$  for every  $w \neq 0$ .

To obtain a polynomial certificate we apply Farkas lemma to the linear programming problem (4.10). Consider the polyhedral cone  $C_\beta \subset \mathbb{R}^s$  defined by

$$(4.12) \quad C_\beta := \{ \xi \in \mathbb{R}^s : (\Delta\Theta)'\xi \geq 0 \}.$$

With every element  $\xi = (\xi_z) \in C_\beta$ , we can associate a specific polynomial  $p_\xi \in \mathbb{R}[u_1, \dots, u_m]$  defined by:

$$(4.13) \quad u \mapsto p_\xi(u) := \sum_{\substack{z \in \mathbb{N}^m, \\ z \neq 0, z \leq \beta}} \xi_z u^z,$$

and notice that in view of (4.11),  $p_\xi(b) = \xi'\Delta\mathbf{b}$ .

**Theorem 11.** *Let  $\beta, b \in \mathbb{N}^m$  and  $A = [A_1 | \dots | A_n] \in \mathbb{N}^{m \times n}$  be such that  $\beta \geq b$  and  $\beta \geq A_k$  for every index  $1 \leq k \leq n$ . Consider the polyhedral cone  $C_\beta \subset \mathbb{R}^s$  given in (4.12) and the following two statements :*

**(a):** *The system  $Ax = b$  has an integer solution  $x \in \mathbb{N}^n$ .*

**(b):**  $p_\xi(b) < 0$  for some  $\xi \in C_\beta$  and  $p_\xi \in \mathbb{R}[u]$  as in (4.13).

Then one and only one of statements **(a)** or **(b)** is true.

*Proof.* The fact that  $\Delta$  is invertible (because of Lemma 2) and Theorem 4 imply that the system  $Ax = b$  has a nonnegative integer solution  $x \in \mathbb{N}^n$  if and only if (4.10) holds for some real nonnegative vector  $\mathbf{y} \in \mathbb{R}^p$ . Farkas lemma implies that (4.10) holds if and only if  $\xi' \Delta \mathbf{b} \geq 0$  for every  $\xi \in C_\beta$ ; however from (4.11),

$$0 \leq \xi' \Delta \mathbf{b} = \sum_{\substack{z \in \mathbb{N}^m, \\ z \neq 0, z \leq \beta}} \xi_z b^z = p_\xi(b),$$

the desired result.  $\square$

It is interesting to compare Theorem 11 with the standard Farkas lemma for (continuous) linear systems. The *continuous* Farkas lemma provides a *linear* certificate of the form  $\omega' b < 0$  for some  $\omega \in \mathbb{R}^m$  that satisfies  $A' \omega \geq 0$ ; in contrast (the *discrete*) Theorem 11 provides a *non-linear* polynomial certificate  $p_\xi(b) < 0$ .

**Example 12.** Let  $A := [3, 4] \in \mathbb{N}^2$ ,  $\beta = 5$ , and  $0 \leq b \leq 5$ ; i.e. the Frobenius equation  $3x_1 + 4x_2 = b$  with  $x_1, x_2 \in \mathbb{N}$ . Then  $s = 6$ ,

$$\Delta = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 2 & 3 & 4 & 5 \\ 0 & 1 & 4 & 9 & 16 & 25 \\ 0 & 1 & 8 & 27 & 64 & 125 \\ 0 & 1 & 16 & 81 & 256 & 625 \\ 0 & 1 & 32 & 243 & 1024 & 3125 \end{bmatrix}, \quad \text{and} \quad \Theta = \begin{bmatrix} -1 & 0 & 0 & -1 & 0 \\ 0 & -1 & 0 & 0 & -1 \\ 0 & 0 & -1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \end{bmatrix}.$$

The pair (4.10)-(4.11) reads as follows :

$$\begin{bmatrix} 0 & 0 & 0 & 0 & 0 \\ 3 & 3 & 3 & 4 & 4 \\ 9 & 15 & 21 & 16 & 24 \\ 27 & 63 & 117 & 64 & 124 \\ 81 & 255 & 609 & 256 & 624 \\ 243 & 1023 & 3093 & 1024 & 3124 \end{bmatrix} \begin{bmatrix} y[1, 0] \\ y[1, 1] \\ y[1, 2] \\ y[2, 0] \\ y[2, 1] \end{bmatrix} = \begin{bmatrix} 0 \\ b \\ b^2 \\ b^3 \\ b^4 \\ b^5 \end{bmatrix}.$$

Notice that  $\Delta \Theta = \begin{bmatrix} 0 \\ S \end{bmatrix}$  with  $S \in \mathbb{N}^{5 \times 5}$  an invertible matrix. Whence there is a nonnegative solution  $\mathbf{y} \geq 0$  if and only if

$$\mathbf{y}(b) = S^{-1}[b, b^2, b^3, b^4, b^5]' \geq 0.$$

We can easily verify that  $\mathbf{y}(5) = [0, -1, 0, 1, 1] \not\geq 0$ . We also have that  $\mathbf{y}(b) \geq 0$  for  $b = 0, 3, 4$ ; and that  $\mathbf{y}(b) \not\geq 0$  for  $b = 1, 2, 5$ .

On the other hand, we can use the transpose  $\Delta'$  instead of  $\Delta$  in equations (4.10) to (4.12). Thus existence of a nonnegative integer

solution  $x \in \mathbb{N}^n$  to  $Ax = b$  is equivalent to existence of a nonnegative real solution  $\mathbf{y} \in \mathbb{R}^p$  to

$$\Delta' \Theta \mathbf{y} = \Delta' \mathbf{b}, \quad \text{where} \quad (\Delta' \mathbf{b})[z] = (z^b - 1).$$

Consider the polyhedral cone  $C_\beta^* \subset \mathbb{R}^s$  defined by

$$C_\beta^* := \{ \xi \in \mathbb{R}^s : \Theta' \Delta \xi \geq 0 \},$$

and with every  $\xi = (\xi_z) \in C_\beta^*$ , associate the exponential-like function

$$(4.14) \quad \sum_{z \in \mathbb{N}^m, z \leq \beta} \xi_z \cdot (z^u - 1).$$

Observe that  $f_\xi(b) = \xi' \Delta' \mathbf{b}$ . By Farkas lemma, one and only one of the following statements holds :

- (a): The system  $Ax = z$  has an integer solution  $x \in \mathbb{N}^n$ .
- (b\*):  $f_\xi(b) < 0$  for some  $\xi \in C_\beta^*$  and  $f_\xi$  as in (4.14).

#### REFERENCES

- [1] D. S. Dummit, R. M. Foote. *Abstract Algebra. 2nd edition*. John Wiley and Sons, New York, 1999.
- [2] R.E. Gomory, E.L. Johnson. The group problem and subadditive functions, in: *Mathematical Programming*, T.C. Hu and S.M. Robinson, editors. Academic Press, New York, 1973.
- [3] R.A. Horn, C.R. Johnson. *Topics in Matrix Analysis*. Cambridge University Press, Cambridge, 1991.
- [4] E.L. Johnson, *Integer Programming: Facets, Subadditivity, and Duality for Group and Semi-group Problems*, Society for Industrial and Applied Mathematics, Philadelphia, 1980.
- [5] J.B. Lasserre. A discrete Farkas lemma. *Discr. Optim.* **1** (2004), 67–75.
- [6] J.B. Lasserre. Integer programming duality and superadditive functions. *Contemp. Math.* **374** (2005), 139–150.
- [7] J. B. Lasserre. Global optimization with polynomials and the problem of moments. *SIAM J. Optim.* **11** (2001), 796–817.
- [8] J. B. Lasserre. An explicit equivalent positive semidefinite program for nonlinear 0-1 programs. *SIAM J. Optim.* **12** (2002), 756–769.
- [9] J.B. Lasserre. *Linear and Integer Programming versus Linear Integration and Counting*, Springer, New York, 2009.
- [10] M. Laurent. A comparison of the Sherali-Adams, Lovász-Schrijver, and Lasserre relaxations for 0-1 programming. *Math. Oper. Res.* **28** (2003), 470–496.
- [11] L. Lovász and A. Schrijver. Cones of matrices and set-functions and 0-1 optimization. *SIAM J. Optim.* **1** (1991), 166–190.
- [12] H.D. Sherali and W.P. Adams. A hierarchy of relaxations between the continuous and convex hull representations for zero-one programming problems. *SIAM J. Discr. Math.* **3** (1990), 411–430.

- [13] H.D. Sherali and W.P. Adams. *A reformulation-linearization technique for solving discrete and continuous nonconvex problems*. Kluwer Academic Publishers, Dordrecht, 1999.
- [14] A. Schrijver. *Theory of Linear and Integer Programming*. John Wiley & Sons, Chichester, 1986.
- [15] V.N. Shevchenko. *Qualitative Topics in Integer Linear Programming*, Translations of Mathematical Monographs, volume 156. American Mathematical Society, Providence, 1997.
- [16] L.A. Wolsey. Integer programming duality: Price functions and sensitivity analysis. *Math. Program.* **20** (1981), 173–195.
- [17] F. Zhang. *Matrix Theory, Basic Results and Techniques*. Springer-Verlag, New York, 1999.

LAAS-CNRS AND INSTITUTE OF MATHEMATICS, LAAS 7 AVENUE DU COLONEL  
ROCHE, 31077 TOULOUSE CEDEX 4, FRANCE  
*E-mail address:* `lasserre@laas.fr`

DEPTO. MATEMÁTICAS, CIVESTAV-IPN, APDO. POSTAL 14740, MEXICO  
D.F. 07000, MÉXICO.  
*E-mail address:* `eszeron@math.cinvestav.mx`