Available online at www.sciencedirect.com

SCIENCE DIRECT®

Discrete Optimization 1 (2004) 67–75

DISCRETE OPTIMIZATION

www.elsevier.com/locate/disopt

A discrete Farkas lemma☆

Jean B. Lasserre

LAAS, 7 Avenue du Colonel Roche, 31 077 Toulouse Cedex 4, France

Received 13 January 2003; received in revised form 25 July 2003; accepted 6 August 2003

Abstract

Given $A \in \mathbb{Z}^{m\times n}$ and $b \in \mathbb{Z}^m$, we consider the issue of existence of a solution $x \in \mathbb{N}^n$ to the system of linear equations $Ax = b$. We provide a discrete analogue of the celebrated Farkas lemma for linear systems in $\mathbb{R}^n$ and prove that checking existence of integral solutions reduces to solving an explicit linear programming problem of fixed dimension, known in advance.

Keywords: Integer programming; Linear programming; Farkas lemma

1. Introduction

Let $A \in \mathbb{Z}^{m\times n}, b \in \mathbb{Z}^m$ and consider the problem of existence of a solution $x \in \mathbb{N}^n$ of the system of linear equations

$$Ax = b, \tag{1}$$

that is, the existence of a *nonnegative integral* solution of the linear system $Ax = b$. For $m = 1$ and $A \in \mathbb{N}^n$, one retrieves the (old) *Frobenius problem* in Number theory ((1) is also called the (unbounded) *knapsack* equation) for which many results have been known for a long time (e.g. see Ehrhart [9], Laguerre [11, pp. 218–220], Netto [17] and Mitrinovic et al. [16, Chapter XIV.21]). For instance, it is well known that the function $b \mapsto f(b)$ that counts the solutions $x \in \mathbb{N}^n$ of $a'x = b$ is a *quasipolynomial* of degree $n - 1$ (that is, a polynomial of b with periodic coefficients) with period the least common multiple (l.c.m.) of the a_j's. It is also well known that there is a so-called *Frobenius number* $b_0 \in \mathbb{N}$ such that there always exists an integral solution whenever $b > b_0$. For more recent results, the interested reader is referred to Beck et al. [3] and the many references therein.

Contribution: The celebrated *Farkas Lemma* in linear algebra states that

$$\{x \in \mathbb{R}^n_+ \,|\, Ax = b\} \neq \emptyset \quad \Leftrightarrow \quad [u \in \mathbb{R}^m \text{ and } A'u \geqslant 0] \Rightarrow b'u \geqslant 0 \tag{2}$$

(where A', b' denote the respective transposes of A, b). To the best of our knowledge, there is no *explicit* discrete analogue of (2). Indeed, the (test) Gomory and Chvátal functions in Blair and Jeroslow [4] (see also Schrijver [18, Corollary 23.4b]) are defined implicitly and recursively, and do not provide a test directly in terms of the data A, b.

In this paper, we provide a *discrete* analogue of Farkas Lemma for (1) to have a solution $x \in \mathbb{N}^n$. Namely, when A and b have nonnegative entries, that is, when $A \in \mathbb{N}^{m\times n}, b \in \mathbb{N}^m$, we prove that (1) has a solution $x \in \mathbb{N}^n$ *if and only if*

☆ This work was completed while the author was on leave as a senior long-term visitor at the Fields Institute of Mathematical Sciences in Toronto, Canada.

E-mail address: lasserre@laas.fr (J.B. Lasserre).

URL: http://www.laas.fr/∼lasserre

1572-5286/$ - see front matter
doi:10.1016/j.disopt.2004.04.002

the polynomial $z \mapsto z^b - 1$ ($:= z_1^{b_1} \cdots z_m^{b_m} - 1$) in $\mathbb{R}[z_1, \ldots, z_m]$ can be written as

$$z^b - 1 = \sum_{j=1}^{n} Q_j(z)(z^{A_j} - 1) = \sum_{j=1}^{n} Q_j(z)(z_1^{A_{1j}} \cdots z_m^{A_{mj}} - 1) \tag{3}$$

for some polynomials $\{Q_j\}$ in $\mathbb{R}[z_1, \ldots, z_m]$ with *nonnegative* coefficients. In other words,

$$\{x \in \mathbb{N}^n \mid Ax = b\} \neq \emptyset \;\Leftrightarrow\; z^b - 1 = \sum_{j=1}^{n} Q_j(z)(z^{A_j} - 1) \tag{4}$$

for some polynomials $\{Q_j\}$ in $\mathbb{R}[z_1, \ldots, z_m]$ with *nonnegative* coefficients. (Of course, the *if* part of the equivalence in (4) is the hard part of the proof.)

Moreover, the degree of the Q_j's in (3) is bounded by $b^* := \sum_{j=1}^m b_j - \min_k \sum_{j=1}^m A_{jk}$.

Therefore, checking the existence of a solution $x \in \mathbb{N}^n$ to $Ax=b$ reduces to checking whether or not there is a *nonnegative* solution y to a system of *linear* equations where (i) y is the vector of unknown nonnegative coefficients of the Q_j's and (ii), the (finitely many) linear equations identify coefficients of same power in both sides of (3). This is a linear programming (LP) problem with $ns(b^*)$ variables and $s(b^* + \max_k \sum_j A_{jk})$ constraints, where $s(u) := \binom{m+u}{u}$ denotes the dimension of the $\mathbb{R}$-vector space of polynomials in m variables, of degree at most u. In addition, all the coefficients of the associated matrix of constraints are all 0 or ± 1. For instance, checking the existence of a solution $x \in \mathbb{N}^n$ to the knapsack equation $a'x = b$ reduces to solving a LP problem with $n(b + 1 - \min_j a_j)$ variables and $b + 1 + \max_j a_j - \min_j a_j$ equality constraints. In fact, when the a_j's are *relatively prime*, it even suffices to consider values of b less than the *Frobenius number* b_0 (because $a'x = b$ has always a solution $x \in \mathbb{N}^n$ whenever $b > b_0$) for which simple explicit upper bounds are available (see Section 3.4). Comparing with the computational complexity of alternative approaches (e.g. dynamic programming) is beyond the scope of the present paper which focuses on the approach. However, this computational issue certainly deserves some further attention.

This result is also extended to the case where $A \in \mathbb{Z}^{m \times n}$, $b \in \mathbb{Z}^m$, that is, when A and b may have nonnegative entries.

We call (4) a *Farkas lemma* because as (2), it states a condition on the *dual* variables z associated with the constraints $Ax = b$. In addition, let $z := \mathrm{e}^{\lambda}$ and notice that the basic terms $b'\lambda$ and $A'\lambda$ in (2) also appear in (4) via z^b which becomes $\mathrm{e}^{b'\lambda}$ and via z^{A_j} which becomes $\mathrm{e}^{(A'\lambda)_j}$. Moreover, if indeed $z^b - 1$ has the representation (4) then whenever $\lambda \in \mathbb{R}^m$ with $A'\lambda \geqslant 0$ (letting $z := \mathrm{e}^{\lambda}$)

$$\mathrm{e}^{b'\lambda} - 1 = \sum_{j=1}^{n} Q_j(\mathrm{e}^{\lambda_1}, \ldots, \mathrm{e}^{\lambda_m})[\mathrm{e}^{(A'\lambda)_j} - 1] \geqslant 0$$

(because all the Q_j have nonnegative coefficients) which implies that $b'\lambda \geqslant 0$. Hence, we retrieve that $b'\lambda \geqslant 0$ whenever $A'\lambda \geqslant 0$, which is to be expected since of course, the existence of integral solutions to (1) implies the existence of real solutions.

Methodology: We use counting techniques based on generating functions as described in Barvinok and Pommersheim [2] and Brion and Vergnes [5,6], to easily obtain a simple explicit expression of the generating function (or, $\mathbb{Z}$-transform) $F : \mathbb{C}^m \to \mathbb{C}$ of the function $f : \mathbb{Z}^m \to \mathbb{N}$, $b \mapsto f(b)$, that counts the lattice points $x \in \mathbb{N}^n$ of the convex polytope $\Omega := \{x \in \mathbb{R}^n_+ \mid Ax = b\}$, pretty much in the spirit of Lasserre and Zeron [14,15]. A similar approach was used in Lasserre and Zeron [12] to compute the volume of a convex polytope via Laplace transform (the continuous analogue of the $\mathbb{Z}$-transform) and also in Lasserre and Zeron [13] to solve a class of multivariate integration problems.

Then, f is the inverse $\mathbb{Z}$-transform of F and can be calculated by a complex integral. The existence of a solution $x \in \mathbb{N}^n$ to (1) is equivalent to showing that $f(b) \geqslant 1$ and by a detailed analysis of this complex integral we prove that (3) is a *necessary and sufficient* condition on b for $f(b) \geqslant 1$.

The paper is organized as follows. In Section 2, we introduce the notation as well as a preliminary result. In Section 3, we present our main result first for the case $A \in \mathbb{N}^{m \times n}$ and then for the general case. We also pay a special attention to the particular case of the unbounded and 0-1 knapsack equations ($m = 1$). For the sake of clarity of exposition, the proof of the main result (Theorem 2) is postponed to Section 4.

2. Notation and preliminary results

For a vector $b \in \mathbb{R}^m$ and a matrix $A \in \mathbb{R}^{m \times n}$, denote by b' and $A' \in \mathbb{R}^{n \times m}$ their respective transpose. Denote by $1_m \in \mathbb{R}^m$ the vector with all entries equal to 1. Let $\mathbb{R}[x_1, \ldots, x_n]$ be the ring of real-valued polynomials in the variables $x_1, \ldots, x_n$.

A polynomial $f \in \mathbb{R}[x_1,\ldots,x_n]$ is written as

$$x \mapsto f(x) = \sum_{\alpha\in\mathbb{N}^n} f_\alpha x^\alpha = \sum_{\alpha\in\mathbb{N}^n} f_\alpha x_1^{\alpha_1}\cdots x_n^{\alpha_n}$$

for *finitely many* real coefficients $\{f_\alpha\}$.

Given a matrix $A \in \mathbb{Z}^{m\times n}$, let $A_j \in \mathbb{Z}^m$ denote its jth column (equivalently, the jth row of A'); then for every $z \in \mathbb{C}^m$, z^{A_j} stands for

$$z^{A_j} := z_1^{A_{1j}}\cdots z_m^{A_{mj}} = \mathrm{e}^{\langle A_j, \ln z\rangle} = \mathrm{e}^{(A'\ln z)_j},$$

and if all the entries of A_j are nonnegative integers then z^{A_j} is also a monomial of $\mathbb{R}[z_1,\ldots,z_m]$.

2.1. Preliminary result

Let $A \in \mathbb{Z}^{m\times n}$, $b \in \mathbb{Z}^m$ and consider the system of linear equations

$$Ax = b, \quad x \in \mathbb{N}^n \tag{5}$$

and its associated convex polyhedron

$$\Omega := \{x \in \mathbb{R}^n \mid Ax = b;\ x \geqslant 0\}. \tag{6}$$

It is assumed that the *recession cone* $\{x \in \mathbb{R}^n \mid Ax = 0; x \geqslant 0\}$ of Ω reduces to the singleton $\{0\}$, so that Ω is compact (equivalently, Ω is a convex polytope).

By a specialized version of a Farkas Lemma due to Carver, (see e.g. Schrijver [18, (33), p. 95]) this in turn implies that

$$\{\lambda \in \mathbb{R}^m \mid A'\lambda > 0\} \neq \emptyset. \tag{7}$$

Denote by $b \mapsto f(b)$ the function $f : \mathbb{Z}^m \to \mathbb{N}$ that counts the integral solutions $x \in \mathbb{N}^n$ of the system of linear equations (5), that is, the lattice points $x \in \mathbb{N}^n$ of Ω. In view of (7), $f(b)$ is finite for all $b \in \mathbb{Z}^m$ because Ω is compact. Let $F : \mathbb{C}^m \to \mathbb{C}$ be the two-sided $\mathbb{Z}$-transform of f, that is,

$$z \mapsto F(z) := \sum_{u\in\mathbb{Z}^m} f(u)z^{-u} = \sum_{u\in\mathbb{Z}^m} f(u)z_1^{-u_1}\cdots z_m^{-u_m} \tag{8}$$

when the above series converges on some domain $D \subset \mathbb{C}^m$. It turns out that $F(z)$ is well defined on the domain

$$D := \{z \in \mathbb{C}^m \mid |z_1^{A_{1j}}\cdots z_m^{A_{mj}}| > 1,\ j = 1,\ldots,n\}. \tag{9}$$

Then we have:

Proposition 1. *Let $A \in \mathbb{Z}^{m\times n}, b \in \mathbb{Z}^m$ and assume that (7) holds. Then,*

$$F(z) = \frac{1}{\prod_{j=1}^n (1 - z^{-A_j})} = \frac{1}{\prod_{j=1}^n (1 - z_1^{-A_{1j}}\cdots z_m^{-A_{mj}})} \tag{10}$$

for all $z \in \mathbb{Z}^m$ that satisfy

$$|z^{A_j}| = |z_1^{A_{1j}}\cdots z_m^{A_{mj}}| > 1, \quad j = 1,\ldots,n. \tag{11}$$

Moreover,

$$\begin{aligned} f(b) &= \frac{1}{(2\pi\mathrm{i})^m}\int_{|z_1|=\gamma_1}\cdots\int_{|z_m|=\gamma_m} \frac{z^{b-1_m}}{\prod_{j=1}^n (1 - z_1^{-A_{1j}}\cdots z_m^{-A_{mj}})}\,\mathrm{d}z \\ &= \frac{1}{(2\pi\mathrm{i})^m}\int_{z\in\Gamma} \frac{z^{b-1_m}}{\prod_{j=1}^n (1 - z^{-A_j})}\,\mathrm{d}z \end{aligned} \tag{12}$$

with $\Gamma := \{z \in \mathbb{C}^m \mid |z_j| = \gamma_j\}$, and where $\gamma \in \mathbb{R}^m_+$ is fixed and satisfies

$$\gamma^{A_j} = \gamma_1^{A_{1j}}\cdots\gamma_m^{A_{mj}} > 1, \quad j = 1,\ldots,n. \tag{13}$$

Proof. The proof is a verbatim copy of that in Lasserre and Zeron [15] where the linear system $Ax \leqslant b$ (instead of $Ax = b$) was considered, but for the sake of completeness we reproduce it here. Apply definition (8) of F to obtain

$$F(z) = \sum_{u\in\mathbb{Z}^m} z^{-u}\left[\sum_{x\in\mathbb{N}^n,\ Ax=u} 1\right] = \sum_{x\in\mathbb{N}^n}\left[\sum_{u=Ax} z_1^{-u_1} z_2^{-u_2}\cdots z_m^{-u_m}\right]$$

$$= \sum_{x\in\mathbb{N}^n} z_1^{-(Ax)_1} z_2^{-(Ax)_2}\cdots z_m^{-(Ax)_m}.$$

Now observe that

$$z_1^{-(Ax)_1} z_2^{-(Ax)_2}\cdots z_m^{-(Ax)_m} = \prod_{k=1}^{n} (z_1^{-A_{1k}} z_2^{-A_{2k}}\cdots z_m^{-A_{mk}})^{x_k} = \prod_{k=1}^{n} (z^{-A_k})^{x_k}.$$

Hence, when (11) holds we obtain

$$F(z) = \prod_{k=1}^{n}\sum_{x_k=0}^{\infty} (z^{-A_k})^{x_k} = \prod_{k=1}^{n} [1 - z^{-A_k}]^{-1}$$

which is (10), and (12) is obtained by a direct application of the inverse $\mathbb{Z}$-transform (see e.g. Conway [8]).

It remains to show that, indeed, the domain defined in (11) is not empty. But this follows from (7). Indeed, take $z_k := e^{\lambda_k}$ for all $k = 1,\ldots,m$, for any λ that satisfies (7). □

3. Main result

Let $A \in \mathbb{Z}^{m\times n}, b \in \mathbb{Z}^m$ and consider the issue of existence of solutions $x \in \mathbb{N}^n$ to the linear system

$$Ax = b. \tag{14}$$

Before proceeding to the general case $A \in \mathbb{Z}^{m\times n}$, we first consider the case $A \in \mathbb{N}^{m\times n}$, where A (and thus b) has only nonnegative entries.

3.1. The case $A \in \mathbb{N}^{m\times n}$

In this section, we assume that $A \in \mathbb{N}^{m\times n}$ and thus, necessarily $b \in \mathbb{N}^m$, otherwise, $\Omega = \emptyset$.

Theorem 2. *Let $A \in \mathbb{N}^{m\times n}, b \in \mathbb{N}^m$. Then the following two statements* (i) *and* (ii) *are equivalent*:

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

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

$$z^b - 1 = \sum_{j=1}^{n} Q_j(z)(z^{A_j} - 1) \tag{15}$$

for some real-valued polynomials $Q_j \in \mathbb{R}[z_1,\ldots,z_m]$, $j = 1,\ldots,n$, all of them with nonnegative coefficients.

In addition, the degree of the Q_j's in (15) is bounded by

$$b^* := \sum_{j=1}^{m} b_j - \min_k \sum_{j=1}^{m} A_{jk}. \tag{16}$$

For a proof see Section 4.

3.2. Discussion

(a) With b^* as in (16) denote by $s(b^*) := \binom{m+b^*}{b^*}$ the dimension of the $\mathbb{R}$-vector space of polynomials in m variables, of degree at most b^*. In view of Theorem 2, and given $b \in \mathbb{N}^m$, checking the existence of a solution $x \in \mathbb{N}^n$ to $Ax = b$ reduces to checking whether or not there exists a nonnegative solution y to a system of linear equations with:

- $n \times s(b^*)$ variables, the nonnegative coefficients of the Q_j's.
- $s(b^* + \max_k \sum_{j=1}^{m} A_{jk})$ equations to identify the terms of same power in both sides of (15).

This in turn reduces to solving a LP problem with $ns(b^*)$ variables and $s(b^* + \max_k \sum_j A_{jk})$ equality constraints. Observe that in view of (15), this LP has a matrix of constraints with only 0 and ± 1 coefficients.

(b) In fact, from the proof of Theorem 2, it follows that one may even enforce the weights Q_j in (15) to be polynomials in $\mathbb{Z}[z_1,\ldots,z_m]$ (instead of $\mathbb{R}[z_1,\ldots,z_m]$) with nonnegative coefficients (and even with coefficients in $\{0,1\}$) However, (a) above shows that the strength of Theorem 2 is precisely to allow $Q_j \in \mathbb{R}[z_1,\ldots,z_m]$ as it permits to check feasibility by solving a (continuous) linear program. Enforcing $Q_j \in \mathbb{Z}[z_1,\ldots,z_m]$ would result in an *integer* program of size larger than that of the original problem.

(c) Theorem 2 reduces the issue of existence of a solution $x \in \mathbb{N}^n$ to a particular *ideal membership problem*, that is, $Ax=b$ has a solution $x \in \mathbb{N}^n$ if and only if the polynomial $z^b - 1$ belongs to the *binomial ideal* $I = \langle z^{A_j} - 1\rangle_{j=1,\ldots,n} \subset \mathbb{R}[z_1,\ldots,z_m]$ *and* for some weights Q_j all with *nonnegative coefficients*.

Interestingly, consider the ideal $J \subset \mathbb{R}[z_1,\ldots,z_m,y_1,\ldots,y_n]$ generated by the binomials $z^{A_j} - y_j$, $j=1,\ldots,n$, and let G be a Gröbner basis of J, where the ordering of variables satisfies $z > y$. Using the Conti–Traverso algebraic approach [7] (see also Adams and Loustaunau [1, Section 2.8]), it is known that $Ax = b$ has a solution $x \in \mathbb{N}^n$ if and only if the monomial z^b is reduced (with respect to G) to some monomial y^α, in which case $\alpha \in \mathbb{N}^n$ is a feasible solution. Observe that this is not a Farkas lemma as we do not know in advance $\alpha \in \mathbb{N}^n$ (we look for it!) to test whether $z^b - y^\alpha \in J$. One has to apply Buchberger's algorithm to (i) find a reduced Gröbner basis G of J, and (ii) reduce z^b with respect to G and check whether the final result is a monomial y^α. Moreover, note that the latter approach uses polynomials in $n+m$ (primal) variables y and (dual) variables z, in contrast with the (only) m dual variables z in Theorem 2.

3.3. The general case

In this section, we consider the general case $A \in \mathbb{Z}^{m\times n}$ so that A may have negative entries. The above arguments cannot be repeated because of the occurrence of negative powers. However, let $\alpha \in \mathbb{N}^n, \beta \in \mathbb{N}$ be such that

$$\hat{A}_{jk} := A_{jk} + \alpha_k \geqslant 0, \qquad \hat{b}_j := b_j + \beta \geqslant 0, \qquad k=1,\ldots,n, \quad j=1,\ldots,m. \tag{17}$$

Note that once $\alpha \in \mathbb{N}^n$ is fixed, we can choose $\beta \in \mathbb{N}$ as large as desired. Moreover, as Ω defined in (6) is compact we have that

$$\max_{x\in\mathbb{N}^n}\left\{\sum_{j=1}^n \alpha_j x_j \mid Ax=b\right\} \leqslant \max_{x\in\mathbb{R}^n; x\geqslant 0}\left\{\sum_{j=1}^n \alpha_j x_j \mid Ax=b\right\} =: \rho^*(\alpha) < \infty. \tag{18}$$

Observe that given $\alpha \in \mathbb{N}^n$, the scalar $\rho^*(\alpha)$ is easily calculated by solving a LP problem. Therefore, we decide to choose $\beta \geqslant \rho^*(\alpha)$. Let $\hat{A} \in \mathbb{N}^{m\times n}$, $\hat{b} \in \mathbb{N}^m$ be as in (17) with $\beta \geqslant \rho^*(\alpha)$. Then the existence of solutions $x \in \mathbb{N}^n$ to $Ax = b$ is equivalent to the existence of solutions $(x,u) \in \mathbb{N}^n \times \mathbb{N}$ to the system of linear equations

$$\mathbb{Q}\begin{cases} \hat{A}x + u1_m = \hat{b}, \\ \displaystyle\sum_{j=1}^n \alpha_j x_j + u = \beta. \end{cases} \tag{19}$$

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

$$Ax + 1_m \sum_{j=1}^n \alpha_j x_j - 1_m \sum_{j=1}^n \alpha_j x = b + (\beta - \beta)1_m$$

or equivalently,

$$\hat{A}x + \left(\beta - \sum_{j=1}^n \alpha_j x_j\right) 1_m = \hat{b}$$

and thus, as $\beta \geqslant \rho^*(\alpha) \geqslant \sum_{j=1}^n \alpha_j x_j$ (cf. (18)), we see that (x,u) with $\beta - \sum_{j=1}^n \alpha_j x_j =: u \in \mathbb{N}$ is a solution of (19). Conversely, let $(x,u) \in \mathbb{N}^n \times \mathbb{N}$ be a solution of (19). Using the definitions of $\hat{A}$ and $\hat{b}$, it then follows immediately that

$$Ax + 1_m \sum_{j=1}^n \alpha_j x_j + u1_m = b + \beta 1_m, \qquad \sum_{j=1}^n \alpha_j x_j + u = \beta$$

so that $Ax = b$. The system of linear equations (19) can be put in the form

$$B\begin{bmatrix} x \\ u \end{bmatrix} = \begin{bmatrix} \hat{b} \\ \beta \end{bmatrix} \quad \text{with } B := \begin{bmatrix} \hat{A} & | & 1_m \\ - & & - \\ \alpha' & | & 1 \end{bmatrix} \tag{20}$$

and as B has only entries in $\mathbb{N}$, we are back to the case analyzed in Section 3.1.

Theorem 3. *Let $A \in \mathbb{Z}^{m\times n}$, $b \in \mathbb{Z}^m$ and assume that Ω defined in (6) is compact. Let $\hat{A} \in \mathbb{N}^{m\times n}$, $\hat{b} \in \mathbb{N}^m$, $\alpha \in \mathbb{N}^n$ and $\beta \in \mathbb{N}$ be as in (17) with $\beta \geqslant \rho^*(\alpha)$ (cf. (18)). Then the following two statements* (i) *and* (ii) *are equivalent*

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

(ii) *The real-valued polynomial $z \mapsto z^b(zy)^\beta - 1 \in \mathbb{R}[z_1, \ldots, z_m, y]$ can be written as*

$$z^b(zy)^\beta - 1 = Q_0(z, y)(zy - 1) + \sum_{j=1}^{n} Q_j(z, y)(z^{A_j}(zy)^{\alpha_j} - 1) \tag{21}$$

for some real-valued polynomials $\{Q_j\}_{j=0}^n$ in $\mathbb{R}[z_1, \ldots, z_m, y]$, all with nonnegative coefficients.

In addition, the degree of the Q_j's in (21) is bounded by

$$(m+1)\beta + \sum_{j=1}^{m} b_j - \min\left[m+1, \min_{k=1,\ldots,n}\left[(m+1)\alpha_k + \sum_{j=1}^{m} A_{jk}\right]\right].$$

Proof. Apply Theorem 2 to the equivalent form (20) of the system $\mathbb{Q}$ in (19), where B and $(\hat{b}, \beta)$ have only entries in $\mathbb{N}$, and use definition (17) of $(\hat{b}, \beta)$ and $\hat{A}$. □

3.4. The knapsack equation

The (unbounded) knapsack (or Frobenius) equation is a particular case where $A = a \in \mathbb{N}^n$, $b \in \mathbb{N}$, that is, $m = 1$ and one considers the equation

$$a'x := \sum_{j=1}^{n} a_j x_j = b. \tag{22}$$

Therefore, as a direct consequence of Theorem 2, we obtain:

Corollary 4. *Let $(a, b) \in \mathbb{N}^n \times \mathbb{N}$. The following two statements* (i) *and* (ii) *are equivalent*:

(i) *The knapsack equation $a'x = b$ has a solution $x \in \mathbb{N}^n$.*

(ii) *The univariate polynomial $z \mapsto z^b - 1$ in $\mathbb{R}[z]$ can be written as*

$$z^b - 1 = \sum_{j=1}^{n} Q_j(z)(z^{a_j} - 1) \tag{23}$$

for some polynomials $Q_j \in \mathbb{R}[z]$ with nonnegative coefficients.

In addition, the degree of the Q_j's in (23) is bounded by $b^* := b - \min_k a_k$.

From (a) in the discussion after Theorem 2, and in the present context of the knapsack equation, given $b \in \mathbb{N}$ one may test the existence of a solution $x \in \mathbb{N}^n$ to (22) by solving a LP problem with

- $n(b + 1 - \min_k a_k)$ variables (the unknown coefficients of the Q_j's in (23)).
- $b + 1 + \max_k a_k - \min_k a_k$ equality constraints (the linear equations that identify coefficients of same power in both sides of (23)).

A particular case of importance: It is well known that if the a_j's are *relatively prime* there are several explicit upper bounds for the *Frobenius number* b_0 such that (22) has always a solution $x \in \mathbb{N}^n$ whenever $b > b_0$. For instance, as mentioned in Beck et al. [3], and with $a_1 < a_2, \cdots < a_n$, Erdös and Graham [10] provide the bound $2a_n\lfloor a_1/n\rfloor - a_1$, whereas Selmer [19] provides the bound $2a_{n-1}\lfloor a_n/n\rfloor - a_n$.

Therefore, if the a_j's are relatively prime, to check whether (22) has a solution $x \in \mathbb{N}^n$ it suffices to consider only those b less than (for instance) Selmer's bound $2a_{n-1}\lfloor a_n/n\rfloor - a_n$. In this case, in view of Corollary 4, one has to solve a LP

problem with at most

- $2a_{n-1}\lfloor a_n/n\rfloor + 1 - a_1$ constraints.
- $n(2a_{n-1}\lfloor a_n/n\rfloor + 1 - a_n - a_1)$ variables.

3.5. The 0-1 knapsack equation

The 0-1 knapsack equation is the same as (22) except that now we search for solutions $x \in \{0,1\}^n$ instead of $x \in \mathbb{N}^n$ in the unbounded case. But this is the same as solving (22) over $x \in \mathbb{N}^n$, with the additional constraints $x_i \leqslant 1$ for all $i = 1,\ldots,n$. The latter constraints can in turn be replaced by the equality constraints $x_i + u_i = 1$, by adding n additional *slack* variables u_i, also constrained to be in $\mathbb{N}$.

Therefore, with $I \in \mathbb{N}^{n\times n}$ being the identity matrix, solving the 0-1 knapsack equation is the same as solving the system of linear equations

$$\begin{bmatrix} a' & | & 0 \\ - & & - \\ I & | & I \end{bmatrix} \begin{bmatrix} x \\ - \\ u \end{bmatrix} = \begin{bmatrix} b \\ - \\ e_n \end{bmatrix}$$

in $\mathbb{N}^{2n}$. As the matrix of the above linear system has only entries in $\mathbb{N}$, we are in position to apply Theorem 2, that is,

Corollary 5. *Let $(a,b) \in \mathbb{N}^n \times \mathbb{N}$. The following two statements* (i) *and* (ii) *are equivalent*:

(i) *The* 0-1 *knapsack equation $a'x = b$ has a solution $x \in \{0,1\}^n$.*

(ii) *The polynomial $(z,y) \mapsto z^b y_1 \cdots y_n - 1$ in $\mathbb{R}[z, y_1,\ldots,y_n]$ can be written as*

$$z^b y_1 \cdots y_n - 1 = \sum_{j=1}^{n} Q_j(z,y)(z^{a_j} y_j - 1) + \sum_{j=1}^{n} P_j(z,y)(y_j - 1) \tag{24}$$

for some polynomials $\{P_j, Q_j\}$ in $\mathbb{R}[z, y_1,\ldots,y_n]$, all with nonnegative coefficients.

In addition, the degree of the polynomials Q_j, P_j in (24) is bounded by $b^* = b + n - 1 - \min_k a_k$.

Proof. Corollary 5 is a direct consequence of Theorem 2. □

Observe that the discrete Farkas lemma for the 0-1 knapsack equation is considerably more complicated than for the unbounded knapsack equation. Indeed, if in the latter b is not bounded, on the other hand, we have to search for n *univariate* polynomials Q_j of degree at most $b - \min_j a_j$, whereas in the former, even if b is bounded by $s = \sum_j a_j$, we still have to search for $2n$ polynomials of degree at most $b + n - 1 - \min_j a_j$, in $n+1$ variables! (Recall that a polynomial in n variables and of degree at most d has $\binom{n+d}{d}$ coefficients.)

4. Proof of Theorem 2

Proof. (ii) $\Rightarrow$ (i). Assume that $z^b - 1$ can be written as in (15) for some polynomials $\{Q_j\}$ with nonnegative coefficients $\{Q_{j\alpha}\}$, that is,

$$Q_j(z) = \sum_{\alpha\in\mathbb{N}^m} Q_{j\alpha} z^\alpha = \sum_{\alpha\in\mathbb{N}^m} Q_{j\alpha} z_1^{\alpha_1} \cdots z_m^{\alpha_m}$$

for finitely many nonzero (and nonnegative) coefficients $\{Q_{j\alpha}\}$. By Proposition 1, the number $f(b)$ of integral solutions $x \in \mathbb{N}^n$ to the equation $Ax = b$ is given by

$$f(b) = \frac{1}{(2\pi\mathrm{i})^m} \int_{|z_1|=\gamma_1} \cdots \int_{|z_m|=\gamma_m} \frac{z^{b-1_m}}{\prod_{j=1}^n (1 - z^{-A_k})}\, \mathrm{d}z.$$

Writing z^{b-1_m} as $z^{-1_m}(z^b - 1 + 1)$ we obtain

$$f(b) = B_1 + B_2$$

with

$$B_1 = \frac{1}{(2\pi\mathrm{i})^m} \int_{|z_1|=\gamma_1} \cdots \int_{|z_m|=\gamma_m} \frac{z^{-1_m}}{\prod_{k=1}^n (1 - z^{-A_k})}\, \mathrm{d}z$$

and

$$B_2 := \frac{1}{(2\pi \mathrm{i})^m} \int_{|z_1|=\gamma_1} \cdots \int_{|z_m|=\gamma_m} \frac{z^{-1_m}(z^b - 1)}{\prod_{k=1}^n (1 - z^{-A_k})}\, \mathrm{d}z$$

$$= \sum_{j=1}^n \frac{1}{(2\pi \mathrm{i})^m} \int_{|z_1|=\gamma_1} \cdots \int_{|z_m|=\gamma_m} \frac{z^{A_j - 1_m} Q_j(z)}{\prod_{k \neq j} (1 - z^{-A_k})}\, \mathrm{d}z$$

$$= \sum_{j=1}^n \sum_{\alpha \in \mathbb{N}^m} \frac{Q_{j\alpha}}{(2\pi \mathrm{i})^m} \int_{|z_1|=\gamma_1} \cdots \int_{|z_m|=\gamma_m} \frac{z^{A_j + \alpha - 1_m}}{\prod_{k \neq j} (1 - z^{-A_k})}\, \mathrm{d}z.$$

From (12) in Proposition 1 (with $b := 0$) we recognize in B_1 the number of solutions $x \in \mathbb{N}^n$ to the linear system $Ax = 0$, so that $B_1 = 1$. Next, again from (12) in Proposition 1 (now with $b := A_j + \alpha$), each term

$$C_{j\alpha} := \frac{Q_{j\alpha}}{(2\pi \mathrm{i})^m} \int_{|z_1|=\gamma_1} \cdots \int_{|z_m|=\gamma_m} \frac{z^{A_j + \alpha - 1_m}}{\prod_{k \neq j} (1 - z^{-A_k})}\, \mathrm{d}z$$

is equal to

$$Q_{j\alpha} \times \text{the number of integral solutions } x \in \mathbb{N}^{n-1}$$

of the linear system $\hat{A}^{(j)} x = A_j + \alpha$, where $\hat{A}^{(j)}$ is the matrix in $\mathbb{N}^{m \times (n-1)}$ obtained from A by deleting its jth column. As by hypothesis each $Q_{j\alpha}$ is nonnegative, it follows that

$$B_2 = \sum_{j=1}^n \sum_{\alpha \in \mathbb{N}^m} C_{j\alpha} \geqslant 0,$$

so that $f(b) = B_1 + B_2 \geqslant 1$. In other words, the system $Ax = b$ has at least one solution $x \in \mathbb{N}^n$.

(i) $\Rightarrow$ (ii). Let $x \in \mathbb{N}^n$ be a solution of $Ax = b$, and write

$$z^b - 1 = z^{A_1 x_1} - 1 + z^{A_1 x_1}(z^{A_2 x_2} - 1) + \cdots + z^{\sum_{j=1}^{n-1} A_j x_j}(z^{A_n x_n} - 1)$$

and if $x_j \neq 0$

$$z^{A_j x_j} - 1 = (z^{A_j} - 1)\left[1 + z^{A_j} + \cdots + z^{A_j(x_j - 1)}\right], \quad j = 1, \ldots, n$$

to obtain (15) with

$$z \mapsto Q_j(z) := z^{\sum_{k=1}^{j-1} A_k x_k}[1 + z^{A_j} + \cdots + z^{A_j(x_j - 1)}], \quad j = 2, \ldots, n.$$

$$Q_1(z) = (1 + z^{A_1} + \ldots + z^{A_1(x_1 - 1)}).$$

We immediately see that each Q_j has all its coefficients nonnegative (and even in $\{0, 1\}$).

Finally, the bound on the degree follows immediately from the proof of (i) $\Rightarrow$ (ii). $\square$

References

[1] W.W. Adams, P. Loustaunau, An Introduction to Gröbner Bases, American Mathematical Society, Providence, RI, 1994.

[2] A.I. Barvinok, J.E. Pommersheim, An algorithmic theory of lattice points in polyhedra, in: New Perspectives in Algebraic Combinatorics, Billera, Loui J. (Eds.) et al., Cambridge, Cambridge University Press, Math. Sci. Res. Inst. Publ. 38, 91–147.

[3] M. Beck, R. Diaz, S. Robins, The Frobenius problem, rational polytopes, and Fourier–Dedekind sums, J. Number Theory 96 (2002) 1–21.

[4] C.E. Blair, R.G. Jeroslow, The value function of an integer program, Math. Programming 23 (1982) 237–273.

[5] M. Brion, M. Vergne, Lattice points in simple polytopes, J. Amer. Math. Soc. 10 (1997) 371–392.

[6] M. Brion, M. Vergne, Residue formulae, vector partition functions and lattice points in rational polytopes, J. Amer. Math. Soc. 10 (1997) 797–833.

[7] P. Conti, C. Traverso, Buchberger algorithm and integer programming, in: H.F. Mattson, T. Mora, T.R.N. Rao (Eds.), Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, Lecture Notes in Computer Science, Vol. 539, Springer, Berlin, 1991, pp. 130–139.

[8] J.B. Conway, Functions of a Complex Variable I, 2nd Edition, Springer, New York, 1978.

[9] E. Ehrhart, Sur les équations diophantiennes linéaires, C. R. Acad. Sci. Paris Ser. A 288 (1979) 785–787.

[10] P. Erdös, R.L. Graham, On a linear diophantine problem of Frobenius, Acta Arith. 21 (1972) 399–408.

[11] E. Laguerre, Oeuvres, Vol. I, Gauthier-Villars, Paris, 1898.

[12] J.B. Lasserre, E.S. Zeron, A Laplace transform algorithm for the volume of a convex polytope, J. ACM 48 (2001) 1126–1140.
[13] J.B. Lasserre, E.S. Zeron, Solving a class of multivariate integration problems via Laplace techniques, Appl. Math. (Warsaw) 28 (2001) 391–405.
[14] J.B. Lasserre, E.S. Zeron, Solving the knapsack problem via $\mathbb{Z}$-transform, Oper. Res. Lett. 30 (2002) 394–400.
[15] J.B. Lasserre, E.S. Zeron, Counting integral points in a convex rational polytope, Math. Oper. Res., 28 (2003) 853–870.
[16] D.S. Mitrinović, J. Sándor, B. Crstici, Handbook of Number Theory, Kluwer Academic Publishers, Dordrecht, 1996.
[17] E. Netto, Lehrbuch der Combinatorik, 2nd Edition, B.G. Teubner, Leipzing, Berlin, 1927.
[18] A. Schrijver, Theory of Linear and Integer Programming, Wiley, Chichester, 1986.
[19] E.S. Selmer, On a linear diophantine problem of Frobenius, J. Reine Angew. Math. 293/294 (1977) 1–17.