A discrete Farkas lemma

Jean B. Lasserre

LAAS-CNRS
7 Avenue du Colonel Roche, 31077 Toulouse cedex 4, France.
lasserre@laas.fr
http://www.laas.fr/~lasserre

Abstract. Given $A \in \mathbb{Z}^{m \times n}$ and $b \in \mathbb{Z}^m$, we consider the issue of existence of a nonnegative integral solution $x \in \mathbb{N}^n$ to the system of linear equations $Ax = b$. We provide a discrete and explicit 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.

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

$$Ax = b,$$

that is, the existence of a nonnegative integral solution of the linear system $Ax = b$.

Contribution. The celebrated Farkas Lemma in linear algebra states that

$$\{x \in \mathbb{R}_+^n \mid Ax = b\} \neq \emptyset \iff [u \in \mathbb{R}^m \text{ and } A'u \geq 0] \Rightarrow b'u \geq 0$$

(2)

(where $A'$ (resp. $b'$) stands for the transpose of $A$ (resp. $b$)).

To the best of our knowledge, there is no explicit discrete analogue of (2). Indeed, the (test) Gomory and Chvátal functions used by Blair and Jeroslow in [3] (see also Schrijver in [8, 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 and explicit analogue of Farkas Lemma for $\mathbb{N}$ 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 the polynomial $z \mapsto z^b - 1 \,(:= z_1^{b_1} \cdots z_m^{b_m} - 1)$ of $\mathbb{R}[z_1, \ldots, z_m]$, can be written

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

(3)
for some polynomials \( \{Q_j\} \) in \( \mathbb{R}[z_1, \ldots, z_m] \) with nonnegative coefficients. In other words,

\[
\{x \in \mathbb{N}^n \mid Ax = b\} \neq \emptyset \iff z^b - 1 = \sum_{j=1}^n Q_j(z)(z^{A_j} - 1),
\]

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 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 vector space of polynomials of degree \( u \) in \( m \) variables. In addition, all the coefficients of the associated matrix of constraints are all 0 or \( \pm 1 \). For instance, checking the existence of a solution \( x \in \mathbb{N}^n \) to the knapsack equation \( a^t x = b \), 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. 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 \( z := e^\lambda \) and notice that the basic ingredients \( b^\lambda \) and \( A^\lambda \) of (2), also appear in (4) via \( z^b \) which becomes \( e^{b^\lambda} \) and via \( z^{A_j} \) which becomes \( e^{(A_j)\lambda} \). Moreover, if indeed \( z^b - 1 \) has the representation (4), then whenever \( \lambda \in \mathbb{R}^m \) and \( A^\lambda \geq 0 \) (letting \( z := e^\lambda \))

\[
\begin{split}
e^{b^\lambda} - 1 &= \sum_{j=1}^n Q_j(e^{\lambda_1}, \ldots, e^{\lambda_m}) \left[ e^{(A_j)^\lambda} - 1 \right] \geq 0 \\
\end{split}
\]

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

**Methodology.** We use counting techniques based on generating functions as described by Barvinok and Pommersheim in [2] and by Brion and Vergne in [4]. 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 \( f : \mathbb{Z}^n \to \mathbb{N}, b \mapsto f(b) \), that counts the lattice points \( x \in \mathbb{N}^n \) of the convex polytope \( \Omega := \{ x \in \mathbb{R}_+^n \mid Ax = b \} \). Then \( f \) is the inverse \( \mathbb{Z} \)-transform of \( F \) and can be calculated by a complex integral. Existence of a solution \( x \in \mathbb{N}^n \) to (1) is equivalent to showing that \( f(b) \geq 1 \), and by a detailed analysis of this complex integral, we prove that (3) is a necessary and sufficient condition on \( b \) for \( f(b) \geq 1 \).
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 \( e_m \in \mathbb{R}^m \) 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

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

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 \( j \)-th column (equivalently, the \( j \)-th row of \( A' \)); then for every \( z \in \mathbb{C}^m \),

\[
z A_j := z_1^{A_{1j}} \cdots z_m^{A_{mj}} = e(A_j \ln z) = e(A' \ln z)_j.
\]

If \( A_j \in \mathbb{N}^m \) then \( z A_j \) is 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

\[
Ax = b; \quad x \in \mathbb{N}^n,
\]

and its associated convex polyhedron

\[
\Omega := \{ x \in \mathbb{R}^n \mid Ax = b; \ x \geq 0 \}.
\]

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

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

\[
\{ \lambda \in \mathbb{R}^m \mid A' \lambda > 0 \} \neq \emptyset.
\]

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

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

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

\[
D := \{ z \in \mathbb{C}^m \mid |z_1^{A_{1j}} \cdots z_m^{A_{mj}}| > 1 \quad j = 1, \ldots, n \}.
\]
Proposition 1. Let \( A \in \mathbb{Z}^{m \times n} \), \( b \in \mathbb{Z}^n \) and assume that (7) holds. Then:

\[
F(z) = \frac{1}{\prod_{j=1}^{n} (1 - z^{-A_j})} = \frac{1}{\prod_{j=1}^{n} (1 - z^{-A_{1j}} \cdots z^{-A_{mj}})}
\]  

(10)

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

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

(11)

Moreover,

\[
f(b) = \frac{1}{(2\pi i)^m} \int_{|z|=\gamma} \cdots \int_{|z|=\gamma} \frac{z^b}{\prod_{j=1}^{n} (1 - z^{-A_{1j}} \cdots z^{-A_{mj}})} \, dz
\]

(12)

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

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

(13)

Proof. The proof is a verbatim copy of that of Lasserre and Zeron in [7] where the linear system \( Ax \leq b \) (instead of \( Ax = b \)) was considered, but for the sake of completeness we reproduce it here. Apply the definition (8) of \( F \) to obtain:

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

Now observe that

\[
z_1^{-(Ax)_1} z_2^{-(Ax)_2} \cdots z_m^{-(Ax)_m} = \prod_{k=1}^{m} \left( z_1^{-A_{1k}} z_2^{-A_{2k}} \cdots z_m^{-A_{mk}} \right)^{x_k} = \prod_{k=1}^{m} \left( z^{-A_k} \right)^{x_k}.
\]

Hence, when (11) holds we obtain

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

which is (10), and (12) is obtained by a direct application of the inverse \( \mathbb{Z} \)-transform (see e.g. Conway in [6]). 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 \( \lambda \) that satisfies (7).

3 Main result

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 $A \in \mathbb{N}^{m \times n}$ and thus, necessarily $b \in \mathbb{N}^m$ (otherwise $\Omega = \emptyset$).

**Theorem 1.** 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

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

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 (14) is bounded by

$$b^* := \sum_{j=1}^m b_j - \min_k \sum_{j=1}^m A_{jk}. \quad (15)$$

For a proof see §4.

### 3.2 Discussion

(a) Let $s(u) := \binom{m+u}{u}$ the dimension of the vector space of polynomials of degree $u$ in $m$ variables. In view of Theorem 1 and with $b^*$ as in (15), 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 (14).

This in turn reduces to solving a LP problem with $ns(b^*)$ variables and $s(b^* + \max_k \sum_{j=1}^m A_{jk})$ equality constraints. Observe that in view of (14), this LP has a matrix of constraints with only 0 and ±1 coefficients.

(b) In fact, from the proof of Theorem 1 it follows that one may even enforce the weights $Q_j$ in (14) 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 1 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 1 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 $J$. Using the algebraic approach described by Adams and Loustaunau in [1, §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 $y^\alpha$, 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 $y^\alpha$. 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 [1]

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 powers. 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

$$\hat{A}_{jk} := A_{jk} + \alpha_k \geq 0; \quad \hat{b}_j := b_j + \beta \geq 0; \quad k = 1, \ldots, n; \ j = 1, \ldots, m. \quad (16)$$

Note that once $\alpha \in \mathbb{N}^n$ is fixed as in (16), we can choose $\beta \in \mathbb{N}$ as large as desired. Moreover, as $\Omega$ defined in (6) is compact, we have

$$\max_{x \in \mathbb{N}^n} \left\{ \sum_{j=1}^n \alpha_j x_j \mid Ax = b \right\} \leq \max_{x \in \Omega} \left\{ \sum_{j=1}^n \alpha_j x_j \mid x \in \Omega \right\} =: \rho^*(\alpha) < \infty. \quad (17)$$

Given $\alpha \in \mathbb{N}^n$, the scalar $\rho^*(\alpha)$ is easily calculated by solving a LP problem. Next, choose $\rho^*(\alpha) \leq \beta \in \mathbb{N}$, and let $\hat{A} \in \mathbb{N}^{m \times n}, \hat{b} \in \mathbb{N}^m$ be as in (16). 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

$$Q \begin{cases} \hat{A}x + u e_m = \hat{b} \\ \sum_{j=1}^n \alpha_j x_j + u = \beta. \end{cases} \quad (18)$$

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

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

or, equivalently,

$$\hat{A}x + \left( \beta - \sum_{j=1}^n \alpha_j x_j \right) e_m = \hat{b},$$
and thus, as \( \beta \geq \rho^* (\alpha) \geq \sum_{j=1}^{n} \alpha_j x_j \) (cf. (17)), we see that \((x, u)\) with \( \beta - \sum_{j=1}^{n} \alpha_j x_j =: u \in \mathbb{N}\), is a solution of (18). Conversely, let \((x, u) \in \mathbb{N}^n \times \mathbb{N}\) be a solution of (18). Then, using the definitions of \(\hat{A}\) and \(\hat{b}\),

\[
Ax + e_m \sum_{j=1}^{n} \alpha_j x_j + u e_m = b + \beta e_m; \quad \sum_{j=1}^{n} \alpha_j x_j + u = \beta,
\]

so that \(Ax = b\). The system of linear equations (18) can be put in the form

\[
B \begin{bmatrix} x \\ u \end{bmatrix} = \begin{bmatrix} \hat{b} \\ \beta \end{bmatrix} \quad \text{with} \quad B := \begin{bmatrix} \hat{A} & e_m \\ - \alpha' & 1 \end{bmatrix},
\]

and as \(B \in \mathbb{N}^{(m+1) \times (n+1)}\), we are back to the case analyzed in §3.1.

**Theorem 2.** Let \(A \in \mathbb{Z}^{m \times n}\), \(b \in \mathbb{Z}^m\) and assume that \(\Omega\) 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 (16) with \(\beta \geq \rho^* (\alpha)\) (cf. (17)). 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 \(z \mapsto z^\beta (zy)^\alpha - 1 \in \mathbb{R}[z, \ldots, z, y]\) can be written

\[
z^\beta (zy)^\alpha - 1 = Q_0(z, y)(zy - 1) + \sum_{j=1}^{n} Q_j(z, y)(z^{A_j}(zy)^\alpha_j - 1)
\]

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

In addition, the degree of the \(Q_j\’s\) in (20) 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 1 to the equivalent form (19) of the system \(Q\) in (18) (since \(B \in \mathbb{N}^{(m+1) \times (n+1)}\) and \((\hat{b}, \beta) \in \mathbb{N}^{m+1}\)), and use the definition (16) of \((\hat{b}, \beta)\) and \(\hat{A}\).

**4 Proof of Theorem 1**

**Proof.** (ii) \(\Rightarrow\) (i). Assume that \(z^\beta - 1\) can be written as in (14) for some polynomials \(\{Q_j\}\) with nonnegative coefficients \(\{Q_{j\alpha}\}\), that is,

\[
Q_j(z) = \sum_{\alpha \in \mathbb{N}^n} Q_{j\alpha} z^\alpha = \sum_{\alpha \in \mathbb{N}^n} Q_{j\alpha} z_{\alpha_1} \cdots z_{\alpha_m},
\]
for finitely many nonzero (and nonnegative) coefficients \( \{Q_{j\alpha}\} \). By Proposition 1, the number \( f(b) \) of nonnegative integral solutions \( x \in \mathbb{N}^n \) to the equation \( Ax = b \), is given by

\[
f(b) = \frac{1}{(2\pi i)^m} \int |z_1| = \gamma_1 \ldots \int |z_m| = \gamma_m \prod_{k=1}^n (1 - z^{-A_k}) dz.
\]

Writing \( z^{b-e_m} \) as \( z^{-e_m}(z^b - 1) \) we obtain

\[
f(b) = B_1 + B_2,
\]

with

\[
B_1 = \frac{1}{(2\pi i)^m} \int |z_1| = \gamma_1 \ldots \int |z_m| = \gamma_m \prod_{k=1}^n (1 - z^{-A_k}) dz,
\]

and

\[
B_2 := \frac{1}{(2\pi i)^m} \int |z_1| = \gamma_1 \ldots \int |z_m| = \gamma_m \sum_{j=1}^n \frac{1}{(2\pi i)^m} \int |z_1| = \gamma_1 \ldots \int |z_m| = \gamma_m \prod_{k \neq j} (1 - z^{-A_k}) dz
\]

\[
= \sum_{j=1}^n \sum_{\alpha \in \mathbb{N}^m} \frac{Q_{j\alpha}}{(2\pi i)^m} \int |z_1| = \gamma_1 \ldots \int |z_m| = \gamma_m \prod_{k \neq j} (1 - z^{-A_k}) dz.
\]

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

\[
C_{j\alpha} := \frac{Q_{j\alpha}}{(2\pi i)^m} \int |z_1| = \gamma_1 \ldots \int |z_m| = \gamma_m \prod_{k \neq j} (1 - z^{-A_k}) dz,
\]

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 \( j \)-th column \( A_j \). As by hypothesis, each \( Q_{j\alpha} \) is nonnegative, it follows that

\[
B_2 = \sum_{j=1}^n \sum_{\alpha \in \mathbb{N}^m} C_{j\alpha} \geq 0,
\]

and so \( f(b) = B_1 + B_2 \geq 1 \). 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

\[
z^b - 1 = z^{A_1 x_1} - 1 + z^{A_2 x_2} - 1 + \cdots + z^{A_{n-1} x_{n-1}} - 1 + z^{A_n x_n} - 1,
\]

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

\[
f(b) = \frac{1}{(2\pi i)^m} \int |z_1| = \gamma_1 \ldots \int |z_m| = \gamma_m \prod_{k=1}^n (1 - z^{-A_k}) dz.
\]
and
\[ z^{A_j x_j} - 1 = (z^{A_j} - 1) \left[ 1 + z^{A_j} + \cdots + z^{A_j (x_j - 1)} \right] \quad j = 1, \ldots, n, \]
to obtain (14) with
\[ z \mapsto Q_j(z) := z \sum_{k=1}^{x_j - 1} A_k x_k \left[ 1 + z^{A_j} + \cdots + z^{A_j (x_j - 1)} \right], \quad j = 2, \ldots, n, \]
and
\[ z \mapsto Q_1(z) := 1 + z^{A_1} + \cdots + z^{A_1 (x_1 - 1)}. \]
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 expression of the \( Q_j \)'s in the proof of (i) \( \Rightarrow \) (ii).

References

1. Adams, W.W., Loustaunau, P.: An Introduction to Gröbner Bases. American Mathematical Society, Providence, RI, 1994.
2. Barvinok, A.I., Pommersheim J.E.: An algorithmic theory of lattice points in polyhedra. In New Perspectives in Algebraic Combinatorics, MSRI Publications 38 (1999) 91–147.
3. Blair, C.E., Jeroslow, R.G.: The value function of an integer program. Math. Prog. 23 (1982) 237-273.
4. Brion, M., Vergne, M.: Lattice points in simple polytopes. J. Amer. Math. Soc. 10 (1997) 371–392.
5. Brion, M., Vergne, M.: Residue formulae, vector partition functions and lattice points in rational polytopes. J. Am. Math. Soc. 10 (1997) 797–833.
6. Conway, J.B.: Functions of a complex variable I. 2nd ed., Springer, New York, (1978).
7. Lasserre, J.B., Zeron, E.S.: On counting integral points in a convex rational polytope, Technical report #01353, LAAS-CNRS, Toulouse, France, 2001. To appear in Math. Oper. Res.
8. Schrijver, A.: Theory of Linear and Integer Programming, John Wiley & Sons, Chichester, 1986.