2007/51

■

Integral Farkas type lemmas for systems with equalities and inequalities

Kent Andersen, Quentin Louveaux
and Robert Weismantel

CORE DISCUSSION PAPER
2007/51

Integral Farkas type lemmas for systems with equalities and inequalities

Kent ANDERSEN[1], Quentin LOUVEAUX[2]
and Robert WEISMANTEL[3]

July 2007

Abstract

A central result in the theory of integer optimization states that a system of linear Diophantine equations $Ax = b$ has no integral solution if and only if there exists a vector in the dual lattice, y^TA integral such that y^Tb is fractional. We extend this result to systems that both have equations and inequalities $\{Ax = b, Cx \leq d\}$. We show that a certificate of integral infeasibility is a linear system with rank (C) variables containing no integral point.

[1] Department of Mathematical Sciences, University of Copenhagen, Denmark. E-mail: kha@math.ku.dk
[2] CORE and INMA, Université catholique de Louvain, Belgium. E-mail: Quentin. louveaux@uclouvain.be
[3] Department of Mathematics, Otto-von-Guericke Universität Magdeburg, Germany. E-mail: weismant@mail.uni-magdeburg.de

This paper presents research results of the Belgian Program on Interuniversity Poles of Attraction initiated by the Belgian State, Prime Minister's Office, Science Policy Programming. The scientific responsibility is assumed by the authors.

1 Introduction

It is a fundamental result in the theory of integer optimization that one can give a certificate for a vector not being a member of a lattice. This result can be viewed as a sort of an integer Farkas Lemma.

Theorem 1 *[4] Let $A \in \mathbb{Z}^{m\times n}$ of full row rank and let $b \in \mathbb{Z}^m$. The system $Ax = b$ has no integral solution iff the system $y^T A$ integer, $y^T b$ fractional is solvable over the rational numbers.*

Among other applications, this result is important in developing the theory of totally dual integral systems and for proving finiteness of cutting plane algorithms in the pure integer case, see [5]. Its applicablility is, however, limited to systems of equations and unbounded variables. Indeed, if inequalities or if bounds on the variables are present, then it is easy to design examples even in three variables for which a certificate of this kind cannot be given, see also Example 2 in Section 2 for such an example.

It is the purpose of this paper to develop certificates for systems of inequalities and equations,

$$\begin{array}{rcl} A\,x & = & b \\ C\,x & \leq & d \end{array}, \tag{1}$$

in integer variables $x \in \mathbb{Z}^n$.

We derive in Section 2 a certificate similar to the one in Theorem 1 that applies to the integer solutions of system (1) when the rank of C is equal to one. In order to generalize this result to higher order ranks of the inequality system, we next develop the geometry of so-called split bodies. Roughly speaking, those bodies are maximal lattice point free bodies in their interior. We present a general result about lattice point free polyhedra in Section 3 that, in turn, allows us to develop in Section 4 an algebraic certificate, when System (1) has no integer solution. This certificate is a linear integral system using as many variables as rank(C).

In this paper we use the +-operator to denote the Minkowski-sum of two sets in $\mathbb{R}^n$. The linear space generated by the vectors $w^1, \ldots, w^d$ is denoted by $\text{lin}(w^1, \ldots, w^d)$, while the null space of a matrix B is denoted by $\ker(B)$. For a set $S \subseteq \mathbb{R}^n$, the symbol $S^\perp$ denotes the linear space generated by the orthogonal complement of the vectors in S.

2 The classical integer Farkas Lemma revisited

Theorem 1 can be interpreted geometrically. To this end, let A be of full row rank and let b be an integral vector. Then, $Ax = b$ defines an affine space that we can represent in the form $\{v^*\} + \text{lin}\,(w^1, \ldots, w^d)$, where $v^* \in \mathbb{Q}^n$ and $w^1, \ldots, w^d \in \mathbb{Z}^n$ are linearly independent vectors. Then it follows that the set $\{y^T A \mid y \in \mathbb{Q}^m\}$ is a subset of $\text{lin}\,(w^1, \ldots, w^d)^\perp$. Hence, Theorem 1 is equvalent to the following result

Theorem 2

$$\left(\{v^*\} + \text{lin}\,(w^1, \ldots, w^d)\right) \cap \mathbb{Z}^n = \emptyset$$

iff there exists $\pi \in \text{lin}\,(w^1, \ldots, w^d)^\perp \cap \mathbb{Z}^n$ such that $\pi^\top v^* \notin \mathbb{Z}$.

Note that the latter condition, $\pi \in \text{lin}\,(w^1,\ldots,w^d)^\perp \cap \mathbb{Z}^n$ such that $\pi^\top v^* \notin \mathbb{Z}$, is equivalent to saying that the body

$$L = \left\{x \in \mathbb{R}^n \mid \lfloor \pi^\top v^* \rfloor \leq \pi^\top x \leq \lceil \pi^\top v^* \rceil\right\} \text{ contains } v^* + \text{lin}\,(w^1,\ldots,w^d)$$

fully in its interior.

Next, we would like to generalize this result to polyhedra that one can represent as the Minkowski sum of an edge plus a linear span. We obtain

Theorem 3 *Let $v_1^*, v_2^* \in \mathbb{Q}^n$ and let $E^* = \text{conv}(v_1^*, v_2^*)$ denote an edge.*

$$\left(E^* + \text{lin}\,(w^1,\ldots,w^d)\right) \cap \mathbb{Z}^n = \emptyset$$

iff there exists a vector $\pi \in \text{lin}\,(w^1,\ldots,w^d)^\perp \cap \mathbb{Z}^n$ such that

$$\pi^\top v \notin \mathbb{Z} \text{ for all } v \in E^*.$$

Proof: We begin to show that both systems cannot have a solution simultaneously. Suppose that $\left(E^* + \text{lin}\,(w^1,\ldots,w^d)\right) \cap \mathbb{Z}^n \neq \emptyset$ Then it follows that there exists an $x^* \in \mathbb{Z}^n$ and multipliers $0 \leq \lambda \leq 1$, $\mu_1,\ldots,\mu_d \in \mathbb{Q}$ such that $x^* = \lambda v_1^* + (1-\lambda)v_2^* + \sum \mu_i w^i$. This implies that for all $\pi \in \text{lin}\,(w^1,\ldots,w^d)^\perp \cap \mathbb{Z}^n$ we have that

$$\pi^\top\left(\lambda v_1^* + (1-\lambda)v_2^*\right) = \pi^\top\left(\lambda v_1^* + (1-\lambda)v_2^* + \sum \mu_i w^i\right) = 0 + \pi^\top x^* \in \mathbb{Z},$$

i.e., the system

$$\pi \in \text{lin}\,(w^1,\ldots,w^d)^\perp \cap \mathbb{Z}^n,\ \pi^\top v \notin \mathbb{Z} \text{ for all } v \in E^*$$

is inconsistent.

As a next step we want to show that if the primal system is not solvable, then the dual has a solution. Let us assume that $\left(E^* + \text{lin}\,(w^1,\ldots,w^d)\right) \cap \mathbb{Z}^n = \emptyset$. The following two cases may be distinguished. In the first case, the set $\left(v_1^* + \text{lin}\,(w^1,\ldots,w^d, v_2^* - v_1^*\right) \cap \mathbb{Z}^n = \emptyset$. Then the result follows directly from the classical Farkas Lemma using v_1^* in place of v^*. Otherwise, there exist smallest positive rational numbers $\lambda_1^*,\ \lambda_2^* \in \mathbb{Q}$ such that

$$\begin{array}{l}\text{interior}\ \left(v_2^* + \lambda_2(v_2^* - v_1^*) + \text{lin}\,(w^1,\ldots,w^d)\right) \cap \mathbb{Z}^n \neq \emptyset, \\ \text{interior}\ \left(v_1^* + \lambda_1(v_1^* - v_2^*) + \text{lin}\,(w^1,\ldots,w^d)\right) \cap \mathbb{Z}^n \neq \emptyset.\end{array}$$

Let us denote by z^1 and z^2 the corresponding integer points, respectively, i.e.,

$$\begin{array}{rcl} z_1 & = & v_1^* + \lambda_1(v_1^* - v_2^*) + \sum_{i=1}^d \mu_{i,1} w^i, \text{ for some } \mu_{i,1} \in \mathbb{Q}, \\ z_2 & = & v_2^* + \lambda_2(v_2^* - v_1^*) + \sum_{i=1}^d \mu_{i,2} w^i, \text{ for some } \mu_{i,2} \in \mathbb{Q}. \end{array}$$

Noting that $\lambda_1 > 0$ and $\lambda_2 > 0$, it follows that for all $0 < \sigma < 1$ we have that

$$(1) \qquad \text{interior}\ \left(\{z_1 + \sigma(z_2 - z_1)\} + \text{lin}(w^1,\ldots,w^d)\right) \cap \mathbb{Z}^n = \emptyset.$$

As a next step we consider the following system of equations in integer variables $\pi_1,\ldots,\pi_n$:

$$\begin{array}{lcl} (z_2 - z_1)^\top & \pi & = & 1 \\ w_1^\top & \pi & = & 0 \\ \vdots & & & \\ w_d^\top & \pi & = & 0 \\ & \pi & \in & \mathbb{Z}^n. \end{array}$$

If this system is inconsistent, then by invoking Theorem 1 we may conclude that the following dual system is solvable:

There exists $y \in \mathbb{Q}^{d+1}$ such that

$$(z_2 - z_1)y_1 + \sum_{i=1}^{d} w^i y_i \in \mathbb{Z}^n, \text{ but } y_1 \notin \mathbb{Z}.$$

Since $z_2 - z_1 \in \mathbb{Z}^n$, we can assume without loss of generality that $0 < y_1 < 1$. This, however, implies that $z_1 + y_1(z_2 - z_1) + \sum w^i y^i \in \mathbb{Z}^n$, contradicting Equation (1). Hence, the primal integral system is feasible and determines the desired split with normal vector π. This completes the proof. ■

Interestingly, this geometric statement can be turned into an algebraic certificate for the inconsistency of a system of equations and an inequality system of row rank equal to one.

Corollary 4 *The set $X = \{x \in \mathbb{R}^n | Ax = b, l \leq c^T x \leq u\}$ has no integral solution if and only if there exist $y \in \mathbb{Q}^m$ and $z \in \mathbb{Q}_+$ such that $(y^T, z)\begin{pmatrix} A \\ c \end{pmatrix} \in \mathbb{Z}^n$ and the interval $[y^T b + zl, y^T b + zu]$ contains no integer point.*

Proof:
Case 1: If X is empty, then the result follows from Theorem 1.
Case 2: Suppose that for all x such that $Ax = b$, we have $l \leq c^T x \leq u$. Then we can apply Theorem 1 to the system $Ax = b$ and obtain a vector y such that $y^T A$ is integral and $y^T b$ is fractional. Then, $(y, 0)$ yields the desired result.
Case 3: In this case we have that $\text{rank}(A) \leq n - 1$, otherwise we are in one of the two previous cases. Notice also that if c is in the subspace spanned by the rows of A, we are in one of the two previous cases. We can therefore express the set X as $X = \{x \in \mathbb{R}^n | x = \lambda x^0 + (1 - \lambda)x^1 + \sum_{i=1}^{n-m} \mu^i y^i, \lambda \in [0, 1]\}$, where x^0 satisfies $Ax = b, c^T x = l$ and x^1 satisfies $Ax = b, c^T x = u$ and (y^i) are a basis of $Ax = 0, c^T x = 0$. We now obtain the result from Theorem 2. ■

Example 1. Consider the system

$$\begin{array}{rl} X = \{x \in \mathbb{R}^4 | & 2x_1 + x_2 + 3x_3 - x_4 = 3 \quad (2) \\ & 6x_1 - x_2 - 2x_3 + x_4 = 5 \quad (3) \\ 5 \leq & 4x_2 + x_3 - 4x_4 \leq 8 \quad \}. \quad (4) \end{array}$$

It is possible to provide a short proof of the fact that X has no integral solution. Indeed, computing $\frac{2}{5}(2) + \frac{1}{5}(3) + \frac{1}{5}(4)$, we obtain that the integral quantity $2x_1 + x_2 + x_3 - x_4$ must be included in the interval $[\frac{16}{5}, \frac{19}{5}]$. Since this is not possible, this implies that $X \cap \mathbb{Z}^4 = \emptyset$.

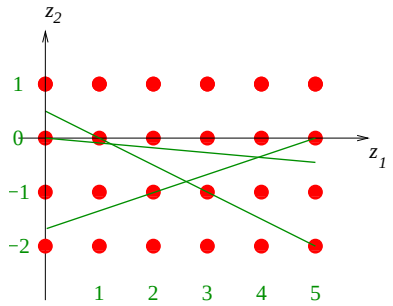

Figure 1: A certificate that X has no integral solution

In the remainder of this paper we refer to a certificate in the sense of Corollary 4 as a *certificate of interval-type*. This is motivated by the fact that $[y^T b + zl, y^T b + zu]$ defines an interval that is lattice point free.

Of course, we cannot hope for a certificate of interval-type for every system as in Corollary 4 because, if this were true, then integral infeasibility could always be verified by split cuts of rank one. This is however known to be false, see [2].

Example 2. Consider the system

$$\begin{aligned} X = \{x \in \mathbb{R}^3 |\quad & x_1 + 2x_2 + 3x_3 = 0 && (5)\\ & -3x_1 + 4x_2 \quad\ \le 0 && (6)\\ & -\ x_1 - 2x_2 \quad\ \le -3 && (7)\\ & 2x_1 -\ x_2 \quad\ \le 5 \quad \}. && (8) \end{aligned}$$

Remark that the system can be written in the form $X = \{x \in \mathbb{R}^n | Ax = b, Cx \le d\}$ with $\operatorname{rank}(C) = 2$. It is readily checked that both $Ax = b$ and $Cx \le d$ have integral solutions considered as single systems. It can also be proven that no "interval-certificate" exists for X. To prove that $X \cap \mathbb{Z}^3 = \emptyset$, we first write the following three valid relaxations of X,

$$\begin{aligned} -\frac{2}{3}(5) - \frac{1}{3}(7): \quad & -2x_2 - 2x_3 \le x_1 - 1 && (9)\\ (5) - (8): \quad & 3x_2 + 3x_3 \ge x_1 - 5 && (10)\\ 4(5) + (6): \quad & 12x_2 + 12x_3 \le -x_1 && (11) \end{aligned}$$

The quantities $x_2 + x_3$ and x_1 must be integral. By denoting $z_1 := x_1$ and $z_2 := x_2 + x_3$, we are able to write (9)-(11) as

$$Y = \{(z_1, z_2) \in \mathbb{R}^2 | -z_1 - 2z_2 \le -1, z_1 - 3z_2 \le 5, z_1 + 12z_2 \le 0\}.$$

Y defines a two-dimensional triangle that has no integral solution as can be read off from Fig. 1. Henceforth, the initial feasible region X does not contain any integral point.

Example 2 illustrates that in order to verify integral infeasibility for a system with at least two linearly independent inequalities, then this requires to derive a certificate using two integral variables z_1 and z_2 and several constraints. It turns out that this can be formalized, indeed.

3 From edges to higher dimensional polyhedra

With the developments in this section we pave the way for generalizing Corollary 4 to inequality systems with arbitrary rank. Our point of departure is that if the Minkowski sum of an edge with a linear space does not contain any integer point, then this set can be extended to a full dimensional body that is (i) lattice point free in its full interior; (ii) each of its facets contains an integer point and (iii), it fully contains the given set in its strict interior. This is, roughly speaking, what we define to be a split body.

Definition 1 *$L \subseteq \mathbb{R}^n$ is a* split body *if*

- $\dim(L) = n$.
- *interior* $(L) \cap \mathbb{Z}^n = \emptyset$;
- *each facet F of L contains an integer point and can be represented by an integer vector $(\pi, \pi_0) \in \mathbb{Z}^{n+1}$ as*

$$F = \left\{x \in L \;\middle|\; \pi^T x = \pi_0\right\}.$$

- *L can be represented as the orthogonal Minkowski-sum of a polytope plus a linear space, i.e., there exist affinely independent vectors $v^1, \dots v^s$ and linearly independent vectors $w^1, \dots, w^d \in \mathbb{Z}^n$ such that $(w^i)^T v^j = 0$ for all $i = 1, \dots, d$ and $j = 1, \dots, s$ such that*

$$L = \quad \{x \in \mathbb{R}^n \;\mid\; x = \textstyle\sum_{i=1}^s \lambda_i v^i + \sum_{j=1}^d \mu_j w^j \qquad \sum_{i=1}^s \lambda_i = 1, \lambda_i \geq 0\}.$$

The split-dimension *of L is defined to be $n - d$.*

A split body of split-dimension 1 is the Minkowski sum of an edge $\text{conv}(\{v^1, v^2\})$ and the linear space generated by $n-1$ linearly independent integer vectors in the orthogonal complement of the edge such that the two parallel hyperplanes passing through v^1 and v^2 contain integer points, respectively. Clearly, such a body can be represented by a split

$$L = \left\{x \in \mathbb{R}^n \mid \pi^\top v^1 \leq \pi^\top x \leq \pi^\top v^2\right\}.$$

This outer description of L provides us with an algebraic certificate for the infeasibility of the mixed integer system

$$Ax = b + \lambda v,\ x \in \mathbb{Z}^n,\ 0 \leq \lambda \leq 1.$$

The question emerges whether this can be generalized to higher dimensional polytopes on the right hand side of the system, i.e., when we consider systems of the kind

$$Ax = b + \sum_i \lambda_i v^i,\ x \in \mathbb{Z}^n,\ \lambda \geq 0,\ \sum_i \lambda_i \leq 1.$$

One major difficulty arises in this context. Unlike in very low dimensions we cannot expect to have an explicit description for all the maximal split-bodies when the dimension is allowed to vary. We next show a general result along these lines that we use in Section 4 to state an algebraic certificate for a primal system with linear equations and inequalities to be infeasible.

Theorem 5 *Let $P^* \subseteq \mathbb{R}^n$ be a polytope of dimension p and let $w^1, \ldots, w^d$, $d \leq n - p$ be linearly independent vectors. Then,*

$$\left(P^* + \lin\left(w^1, \ldots, w^d\right)\right) \cap \mathbb{Z}^n = \emptyset$$

iff there exists a split body L of split-dimension at most p such that $P^* + \lin\left(w^1, \ldots, w^d\right)$ is strictly contained in the interior of L.

Proof: If $\left(P^* + \lin\left(w^1, \ldots, w^d\right)\right) \cap \mathbb{Z}^n \neq \emptyset$, then there cannot exist a split body L of dimension at most p such that $P^* + \lin\left(w^1, \ldots, w^d\right)$ is strictly contained in the interior of L. Conversely, let us assume that

$$\left(P^* + \lin\left(w^1, \ldots, w^d\right)\right) \cap \mathbb{Z}^n = \emptyset.$$

Without loss of generality we can assume that $P^* \subseteq \{v^*\} + \lin(l^1, \ldots, l^p)$ such that the vectors $l^1, \ldots, l^p$ are linearly independent and all lie in the orthogonal complement of $\lin(w^1, \ldots, w^d)$. (Otherwise, we can work with the projection of P^* on the orthogonal complement of $\lin(w^1, \ldots, w^d)$.) Next we proceed using induction on p. If $p = 1$, then, by Theorem 2, the result follows. Hence, let us assume that the result is correct for all split-dimensions less than or equal to $p - 1$. We recall the following facts from linear algebra and polyhedral theory. P^* is a p-dimensional polyhedron in $\mathbb{R}^n$. Hence, there exists a description of P^* that satisfies

$$\begin{array}{l} P^* = \{x \in \mathbb{R}^n \mid \ Ax = a,\ Cx \leq c\} \text{ with } A \in \mathbb{Z}^{(n-p)\times n},\ C \in \mathbb{Z}^{m\times n}. \\ A_{i\cdot} l^j = 0 \text{ for all } i = 1, \ldots, n-p,\ j = 1, \ldots, p. \\ \lin(w^1, \ldots, w^d) \subseteq \{x \in \mathbb{R}^n \mid \ C_{i\cdot}^T x = 0\} \text{ for all } i = 1, \ldots, d. \end{array}$$

As a next step we consider the recursive extension of the polytope P^* along each of the directions l^i. If there exists an index i such that

$$\text{interior } \left(P^* + \lin\left(w^1, \ldots, w^d, l^i\right)\right) \cap \mathbb{Z}^n = \emptyset,$$

then the result follows from the induction hypothesis. Otherwise, we proceed with the order of the indices $i = 1, \ldots, p$. Let us define

$$P_0^* := \left(P^* + \lin\left(w^1, \ldots, w^d\right)\right).$$

Iteratively, we determine smallest nonnegative rational numbers $\lambda_+^*,\ \lambda_-^* \in \mathbb{Q}_+$ such that

$$\begin{array}{l} \text{interior } \left(P_{i-1}^* + \lambda_+ l^i + \lin\left(w^1, \ldots, w^d\right)\right) \cap \mathbb{Z}^n \neq \emptyset, \\ \text{interior } \left(P_{i-1}^* - \lambda_- l^i + \lin\left(w^1, \ldots, w^d\right)\right) \cap \mathbb{Z}^n \neq \emptyset. \end{array}$$

We define

$$P_i^* := \left(P_{i-1}^* + \lambda l^i + \lin\left(w^1, \ldots, w^d\right)\right), \text{ where } \lambda \in [-\lambda_-, \lambda_+].$$

Let z^j, $j \in J$ denote all the integer points that lie on a facet of P_i^*. It follows that an outer description of P_i^* is given by

$$P_i^* = \{x \in \mathbb{R}^n \mid \ Ax = a,\ Cx \leq c^i\} \text{ with } c^i \geq c$$

and $c_k^i \in \mathbb{Z}$, whenever $\{x \in \mathbb{R}^n \mid \ C_{k\cdot}^T x = c_k^i\} \cap \{z^j \mid \ j \in J\} \neq \emptyset$.

After p steps we have generated a polyhedron P_d^* that fully contains P_0^*. Let us denote by C^d and M^d the submatrix of C and the index set of rows, for which $c_k^d \in \mathbb{Z}$, respectively. We claim that

$$L = \{x \in \mathbb{R}^n \mid \ Ax = a,\ C_k^d x \leq c_k^d,\ k \in M^d\}$$

is the desired split body. Indeed, it can be verified that L satisfies the conditions of Definition 1. Moreover, L contains the initial set P_0^* in its full interior. This completes the proof. ■

According to Theorem 5, every lattice point free polyhedron is contained in a split body of appropriate dimension. This fact together with the characterization of one-dimensional split bodies enable us to give an algebraic certificate for the corresponding primal system to have no integer solution. In fact, for a one-dimensional split body, $\{x \in \mathbb{R}^n \mid \alpha \leq \pi^T x \leq \alpha + 1\}$, say, we know that the interior satisfies that $\pi^T x \notin \mathbb{Z}$. In higher dimensions, the situation is much more complex. In such cases, a lattice-point free body is restricted by many hyperplanes and it is by no means obvious to characterize the interior of such a body as nicely as in the one-dimensional case. We next shed some light on this complication.

Our point of departure is that every lattice-point-free polyhedron of dimension greater or equal than two can be represented as

$$L = \left\{x \in \mathbb{R}^n \mid \Pi x \leq \Pi^0\right\},$$

where Π^0 is an integral vector of right hand sides and where $\Pi \in \mathbb{Z}^{t \times n}$. We associate with such a matrix $\Pi \in \mathbb{Z}^{t \times n}$ the following lattices,

$$\mathcal{L} = \{x \in \mathbb{Q}^n \mid \Pi x \in \mathbb{Z}^t\} \text{ and } im(\mathcal{L}) = \{\Pi x \mid x \in \mathcal{L}\}.$$

Notice, that $\mathcal{L}$ is a refinement of $\mathbb{Z}^n$, because Π is an integral matrix. In the special situation, when $\mathcal{L} = \mathbb{Z}^n$, then all the points x in the interior of a lattice-point-free body satisfy $\Pi x \notin \mathbb{Z}^t$. This is quite similar to the situation in the one-dimensional case. However, in the general case the situation is more complicated since there are typically interior points x in the split body for which Πx is integral. In order to cope with this situation we define $B_\Pi \in \mathbb{Z}^{n \times n}$ to be a basis of $\mathcal{L}$, i.e., $\mathcal{L} = \{B_\Pi \lambda \mid \lambda \in \mathbb{Z}^n\}$. We call B_Π the basis transformation matrix associated with Π. B_Π is unique up to multiplication with a unimodular matrix. We obtain

Theorem 6 *Let $L = \{x \in \mathbb{R}^n : \Pi x \leq \Pi^0\}$ be a lattice-point-free polyhedron. There exists a basis transformation matrix B_Π such that*

$$\textit{interior}(L) \subseteq \{x \in \mathbb{R}^n \mid \Pi B_\Pi x \notin \mathbb{Z}^t\}.$$

Proof: For a given lattice-point-free body L, there exists $\Pi \in \mathbb{Z}^{t \times n}$ such that

$$L = \left\{x \in \mathbb{R}^n \mid \Pi x \leq \Pi^0\right\},$$

where Π^0 is an integral vector of right hand sides. Moreover, L does not contain integer points in its interior. We claim that

$$\Pi x \in \mathbb{Z}^t \iff B_\Pi^{-1} x \in \mathbb{Z}^n.$$

Once this claim is verified, we obtain our desired result because in a a lattice-point-free body there does not exist any interior integer point. Hence,

$$\text{interior}(L) \subseteq \{x \in \mathbb{R}^n \mid x = B_\Pi^{-1} B_\Pi x \notin \mathbb{Z}^n\} = \{x \in \mathbb{R}^n \mid \Pi B_\Pi x \notin \mathbb{Z}^t\}.$$

It remains to verify that $\Pi x \in \mathbb{Z}^t \iff B_\Pi^{-1} x \in \mathbb{Z}^n$. In order to see this, we remark that $\Pi x \in \mathbb{Z}^t$ if and only if $x \in \mathcal{L}$. This is equivalent to the statement that $x = B_\Pi \lambda,\ \lambda \in \mathbb{Z}^n$ has a solution. Multiplying both sides of the equation by B_Π^{-1}, we obtain that latter condition is equivalent to $B_\Pi^{-1} x = \lambda \in \mathbb{Z}^n$. This completes the proof. ■

With our preparations in this section we can turn Theorem 5 into an algebraic characterization for the corresponding infeasibility of a system (1) in integer variables. This is the topic to be addressed next.

4 An algebraic certificate

In the previous section we developped a geometric view towards integral infeasibility for systems with equalities and inequalities. In this section, we turn this geometry insight into an algebraic certificate. The certificate per se, however, must become more and more elaborate as the rank of the matrix C increases as it was already pointed in Section 2. The proof of our main theorem requires two basic lemmas on representations of polyhedral sets that we stae first.

Lemma 1 *Let $P = \{x \in \mathbb{R}^n | Cx \leq d\}$ with $\text{rank}(C) = l$. Then there exist $p^1, \ldots, p^r, z^1, \ldots, z^s, w^1, \ldots, w^{n-l} \in \mathbb{R}^n$ such that*

$$P = \text{conv}\{p^1, \ldots, p^r\} + \text{cone}\{z^1, \ldots, z^s\} + \text{lin}\{w^1, \ldots, w^{n-l}\},$$

with $\dim(\text{conv}\{p^1, \ldots, p^r\} + \text{cone}\{z^1, \ldots, z^s\}) = l$.

Proof: Since $\text{rank}(C) = l$, there exist linearly independent vectors $w^1, \ldots, w^{n-l}$ such that $\ker(C) = \text{lin}\{w^1, \ldots, w^{n-l}\}$. Furthermore we can extend the collection of vectors w to a basis $w^1, \ldots, w^n$ of $\mathbb{R}^n$. In that basis any $x \in \mathbb{R}^n$ can be expressed as $x = \sum_{i=1}^n \lambda_i w^i$. With respect to such a representation, we also define a projection operator, namely $\text{proj}(x) = \sum_{i=n-l+1}^n \lambda_i w^i$. Furthermore, by Minkowski's theorem on representation of polyhedra, we can express P as

$$P = \text{conv}\{\bar{p}^1, \ldots, \bar{p}^r\} + \text{cone}\{\bar{z}^1, \ldots, \bar{z}^s\}. \tag{12}$$

The result is obtained by observing that (12) together with the expression of $\ker(C)$ allows us to write P as

$$P = \text{conv}\{\text{proj}(\bar{p}^1), \ldots, \text{proj}(\bar{p}^r)\} + \text{cone}\{\text{proj}(\bar{z}^1), \ldots, \text{proj}(\bar{z}^s)\} + \text{lin}\{w^1, \ldots, w^{n-l}\}.$$

Furthermore, the first two terms are included in a l-dimensional linear space and therefore represent a polyhedron that is at most l-dimensional. ■

Lemma 2 *Let $P = \text{conv}\{p^1, \ldots, p^d\} + \text{cone}\{r^1, \ldots, r^s\} + \text{lin}\{w^1, \ldots, w^t\}$ and let $Q = \text{conv}\{p^1, \ldots, p^d\} + \text{lin}\{r^1, \ldots, r^s, w^1, \ldots, w^t\}$, with $p^i, r^j, w^k \in \mathbb{Z}^n$ for all i, j, k. We have $P \cap \mathbb{Z}^n = \emptyset \iff Q \cap \mathbb{Z}^n = \emptyset$.*

Proof: Since $P \subseteq Q$, the implication from right to left is trivial. Assume $Q \cap \mathbb{Z}^n \neq \emptyset$. We prove that this implies that $P \cap \mathbb{Z}^n \neq \emptyset$. Indeed consider $x \in Q \cap \mathbb{Z}^n$. There exist $\lambda_1, \ldots, \lambda_d \geq 0$ and $\mu_1, \ldots, \mu_s, \nu_1, \ldots, \nu_t \in \mathbb{R}$ with $x = \sum_{i=1}^{d} \lambda_i p^i + \sum_{j=1}^{s} \mu_j r^j + \sum_{k=1}^{t} \nu_k w^k$ and $\sum_{i=1}^{d} \lambda_i = 1$. Let $J = \{j | \mu_j < 0\}$. Since all rays are integers, we can add integral combinations of rays r^j to x keeping its integrality. Therefore $y := x + \sum_{j \in J} \lfloor \mu_j \rfloor r^j \in \mathbb{Z}^n$. We also have $y \in P$ which proves the lemma. ■

We are now prepared for the main result of this paper. It states that a system $X = \{x \in \mathbb{R}^n | Ax = b, Cx \leq d\}$ has no integral solution if and only if there exists a system with $\text{rank}(C)$ variables which has no integral solution. In fact, this system is derived from combinations of the constraints describing X.

Theorem 7 *Let $A \in \mathbb{Z}^{m \times n}$, $C \in \mathbb{Z}^{p \times n}$ and let $l = \text{rank}\,(C)$. For integer vectors b and d, the primal system*

$$\begin{array}{rcl} A\,x & = & b \\ C\,x & \leq & d \end{array}, \quad x \in \mathbb{Z}^n.$$

is empty if and only if there exist rational vectors $y^1, \ldots, y^t \in \mathbb{Q}^m \times \mathbb{Q}^p_+$, and at most l linearly independent integral vectors $v^1, \ldots, v^l \in \mathbb{Z}^n$ such that

$$(y^k)^T \begin{bmatrix} A \\ C \end{bmatrix} = \sum_{i=1}^{l} \lambda_i^k v^i \quad \in \mathbb{Z}^n \text{ with } \lambda_i^k \in \mathbb{Z}\ \forall i = 1, \ldots, l,\ k = 1, \ldots, t.$$

Introducing variables z_i, $i \in \{1, \ldots, l\}$ (representing $(v^i)^T x$), the following system of t inequalities in l variables has no integral solution.

$$\sum_{j=1}^{l} \lambda_j^k z_j \quad \leq \quad y_k^T \begin{bmatrix} b \\ d \end{bmatrix} \text{ for all } k = 1, \ldots, t.$$

Proof: We can assume that A has full row rank and that

$$\text{rank} \begin{bmatrix} A \\ C \end{bmatrix} = m + l.$$

Let $X = \{x \in \mathbb{R}^n \mid x \text{ satisfies } (1)\}$. From Lemma 1 and Lemma 2 it follows that there exist $w^1, \ldots, w^{n-m-l} \in \mathbb{Z}^n$ and a polyhedron P^* of dimension $m + l$ such that X has no integral solution if and only if $P^* + \text{lin}\,(w^1, \ldots, w^{n-m-l})$ has no integral solution. Therefore, we may assume from now on that

$$X = P^* + \text{lin}\,(w^1, \ldots, w^{n-m-l}).$$

If $X \cap \mathbb{Z}^n = \emptyset$, then by applying Theorem 5 we conclude that there exists a split-body L of split dimension l such that $X \subseteq L$. Then, L must be of the form

$$L = L^* + \text{lin}\,(w^1, \ldots, w^{n-m-l},\ w^{n-m-l+1}, \ldots, w^{n-l}),$$

where L^* is a polytope of dimension l, $w^{n-m-l+1}, \ldots, w^{n-l} \in \mathbb{Z}^n$ and the matrix $W = [w^1 \ldots w^{n-l}] \in \mathbb{Z}^{n \times (n-l)}$ has rank $n - l$, i.e., all its column vectors are linearly independent. We can then complete $w^1, \ldots w^{n-l}$ to a basis of $\mathbb{R}^n$ by adding some vectors $v^1, \ldots, v^l \in \mathbb{Z}^n$ in a way such that $(w^j)^T v^k = 0$ for all $j \in \{1, \ldots, n-l\}$ and $k \in \{1, \ldots, l\}$. L can be described by linear inequalities,

$$L = \left\{x \in \mathbb{R}^n \mid \pi_1^T x \leq \pi_1^0, \ldots, \pi_t^T x \leq \pi_t^0\right\}$$

with integral normal vectors $\pi_1, \ldots, \pi_t$ and integral right-hand-side vector π^0. In fact, since $L = L^* + \lin(w^1, \ldots, w^{n-m-l},\ w^{n-m-1}, \ldots, w^{n-l})$, we can conclude that $\pi_k^T w^j = 0$ for all k and $j \leq n-l$, i.e.,

$$\begin{array}{lcl} \pi_k & = & \sum_{i=1}^{l} \lambda_i^k v^i,\ \lambda_i^k \in \mathbb{Z} \text{ for all } k \\ \pi_k^T x & \in & \mathbb{Z} \text{ for all } x \in \mathbb{Z}^n. \end{array} \tag{13}$$

On the other hand, since X is fully contained in the interior of L, we have that $\max\{\pi_k^T x \mid x \in X\} < \pi_k^0$ for all $k = 1, \ldots, t$. Therefore, this maximum value exists. From linear programming duality we obtain that

$$\begin{array}{llcll} \max & \pi_k^T x & = & & \min[b^T, d^T]\ y_k \\ \text{s.t.} & Ax = b, & & \text{s.t.} & [A^T, C^T] y_k = \pi_k \\ & Cx \leq d & & & y_{k,m+1}, \ldots, y_{k,m+l} \geq 0 \end{array}$$

Hence, the minimum-value in the LP-duality relation satisfies $[b^T, d^T]\ y_k < \pi_k^0$. This relation together with Eq. (13) allows us to set up a certificate for $X \cap \mathbb{Z}^n = \emptyset$:

$$\sum_{i=1}^{l} \lambda_i^k (v^i)^T z = \pi_k^T z \leq y_k^T [b^T, d^T] \text{ for all } k = 1, \ldots, t.$$

This system has no integer solution and hence, proves the result. ■

Example 2 revisited. Consider again the system

$$\begin{aligned} X = \{x \in \mathbb{R}^3 |\quad & x_1 + 2x_2 + 3x_3 = 0 && (14)\\ & -3x_1 + 4x_2 \leq 0 && (15)\\ & -\ x_1 - 2x_2 \leq -3 && (16)\\ & 2x_1 -\ x_2 \leq 5 \quad \}. && (17) \end{aligned}$$

One can verify that $\ker(A) = \lin\left\{\begin{pmatrix} 2 \\ -1 \\ 0 \end{pmatrix}, \begin{pmatrix} 3 \\ 0 \\ -1 \end{pmatrix}\right\} = \lin\{w^1, w^2\}$ and $\ker(C) = \lin\left\{\begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}\right\}$. It can be also checked that $X = \conv\{p^1, p^2, p^3\}$. Notice also that $X \subseteq \ker(A) = \lin\{w^1, w^2\}$. We can then extend $\{w^1, w^2\}$ to a unimodular matrix using $w^3 = \begin{pmatrix} 0 \\ -1 \\ 1 \end{pmatrix}$. Therefore $\{w^1, w^2, w^3\}$ is a basis of $\mathbb{Z}^3$. Hence if $X \cap \mathbb{Z}^3 = \emptyset$, then $P = X + \lin\{w^3\} = \conv\{p^1, p^2, p^3\} + \lin\{w^3\}$ is a (non-maximal) split body of split-dimension 2. We next extend $\{w^3\}$ by two linearly independent orthogonal vectors v^1, v^2, for example $v^1 = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$ and $v^2 = \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix}$. It is now possible to express P using inequalities $\pi_k^T x \leq \pi_k^0$ that can be written as

$$\pi_k = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} \lambda_1^k + \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix} \lambda_2^k.$$

Using p^1, p^2, p^3, we can compute a representation of P as follows:

$$\begin{aligned}
\pi_1 &= (-1,\ -2,\ -2)^T, \quad \pi_1^0 = -1,\\
\pi_2 &= (1,\ -3,\ -3)^T, \quad \pi_2^0 = 5,\\
\pi_3 &= (1,\ 12,\ 12)^T, \quad \pi_3^0 = 0.
\end{aligned}$$

We are now able to write three linear programs

$$\begin{aligned}
&\min[b^T, d^T]y_k\\
&(A^T, C^T)y_k = \pi_k\\
&y_{k,m+1}, \ldots, y_{k,m+l} \geq 0
\end{aligned}$$

whose optimal solution provides us with the coefficients leading to the certificate. For example, with $\pi_1 = (-1\ -2\ -2)^T$ we associate the linear program

$$\begin{array}{lrcl}
\min & -3y_3+5y_4 & & \\
\text{s.t.} & y_1 -3y_2- y_3 +2y_4 & = & -1\\
& 2y_1+4y_2-2y_3- y_4 & = & -2\\
& 3y_1 & = & -2\\
& y_2,\quad y_3,\quad y_4 & \geq & 0.
\end{array}$$

The corresponding optimal solution is $y_1 = -\frac{2}{3},\ y_2 = 0,\ y_3 = \frac{1}{3},\ y_4 = 0$ which results in exactly the combination (9) in Example 2. Using $\pi_2 = (1\ -3\ -3)^T$, we obtain another linear program with optimal solution $y_1 = -1,\ y_2 = 0,\ y_3 = 0,\ y_4 = 1$ yielding to (10). Finally, if we use $\pi_3 = (1\ 12\ 12)^T$, we obtain multipliers $y_1 = 4, y_2 = 3$ which leads to (11).

At this point it is in order to analyze the special case of Theorem 7 when the dimension of the polyhedron P^* is equal to two. The reason for this is that we can classify the set of all potential two-dimensional split bodies. In particular, any maximal lattice point free two-dimensional body with integer points on each of its facets is either a triangle or a quadrilateral. Indeed, this result follows from elementary two-dimensional geometric considerations.

Lemma 3 *[1] A split body of split-dimension two is the Minkowski sum of either a triangle or a quadrilateral plus a linear space of dimension $n-2$.*

We can, hence, specialize Theorem 7 to the situation where rank $(C) \leq 2$.

Theorem 8 *Let $A \in \mathbb{Z}^{m\times n}$, $C \in \mathbb{Z}^{p\times n}$ and let $1 \leq l =$ rank $(C) \leq 2$. For integer vectors b and d, the primal system*

$$\begin{array}{rcl} A\,x & = & b\\ C\,x & \leq & d \end{array}, \quad x \in \mathbb{Z}^n.$$

is empty if and only if there exist $t \in \{2,3,4\}$ rational vectors $y^1, \ldots, y^t \in \mathbb{Q}^m \times \mathbb{Q}^p_+$, and at most 2 linearly independent integral vectors $v^1, \ldots, v^2 \in \mathbb{Z}^n$ such that

$$y_k^T \begin{bmatrix} A \\ C \end{bmatrix} = \lambda_1^k v^1 + \lambda_2^k v^2 \in \mathbb{Z}^n \text{ with } \lambda_1^k,\ \lambda_2^k \in \mathbb{Z}\ \forall\ k = 1, \ldots, t,$$

with the following system of t inequalities in 1 or 2 variables has no integral solution

$$\lambda_1^k z_1 + \lambda_2^k z_2 \quad \leq \quad y_k^T \begin{bmatrix} b \\ d \end{bmatrix} \text{ for all } k = 1, \ldots, t.$$

Theorem 7 shows that determining infeasibility of a system $\{x \in \mathbb{Z}^n | Ax = b, Cx \leq d\}$ can be reduced to an integer programming problem in dimension $\text{rank}(C)$. The certificate per se, however, consists of t inequalities and hence, it might not be short in comparison with the number of variables. From a theorem of Doignon [3] it follows that if the reduced program in $\text{rank}(C)$ variables has no integral solution, then at most $2^{\text{rank}(C)}$ inequalities suffice to determine an infeasible integral system. Henceforth, if the number $\text{rank}(C)$ is fixed, then we see that the feasibility problem for $\{x \in \mathbb{Z}^n | Ax = b, Cx \leq d\}$ is in co-NP.

More specific information regarding our certificate is available for systems in one or two variables. In the first case it is required to check whether an interval has integer points. This is easiliy checkable. For two variables, we have seen that all systems can be reduced to systems with at most four inequalities, a number that appears reasonable for performing computations. It can be shown however that as soon as there are at least three variables present, then the number of inequalities required for the certificate might explode. This limits at least practically the applicability of Theorem 7 for larger values of $\text{rank}(C)$.

Acknowledgements. The authors greatly appreciated the support of the European Union as this research was carried out within the TMR-network ADONET 504438. We are also grateful to Laurence Wolsey for his comments on an earlier version of this paper. This second author is supported by FRS-FNRS as a postdoctoral researcher. This paper presents results of the Belgian Program on Interuniversity Poles of Attraction initiated by the Belgian State, Prime Minister's Office, Science Policy Programming. The scientfic responsability is assumed by the authors.

References

[1] K. Andersen, Q. Louveaux, R. Weismantel, L. Wolsey, *Inequalities from two rows of a simplex tableau* IPCO 2007, Lecture Notes in Computer Science, Springer, (2007).

[2] W.J. Cook, R. Kannan, A. Schrijver, *Chvátal closures for mixed integer programming*, Mathematical Programming 47, 155 – 174, (1990).

[3] J. P. Doignon, *Convexity in crystallographic lattices*, Journal of Geometry 3, 71 – 85, (1973).

[4] L. Kronnecker, *Näherungsweise ganzzahlige Auflösung linearer Gleichungen*, Monatsberichte der Königlich Preussischen Akademie der Wissenschaften zu Berlin , 1179 – 1193, (1884).

[5] A. Schrijver, *Theory of linear and integer programming*, Wiley Chichester (1986).