Conductor in a Sylvester's formula on lattices

Anna Rycerz
A G H University of Science and Technology
Faculty of Applied Mathematics
al. Mickiewicza 30, 30 – 059 Cracow, Poland
rycerz@uci.agh.edu.pl

April 6, 2006

Abstract

Sylvester proved that if α_1 and α_2 are relatively prime positive integers then the set of all nonnegative integer linear combinations of α_1 and α_2 includes all integers greater than $F = \alpha_1\alpha_2 - (\alpha_1 + \alpha_2)$. Thus $K = F + 1$ called *conductor* is the smallest integer such that for every integer k with $K \leq k$ the equation $\alpha_1 x_1 + \alpha_2 x_2 = k$ has a solution over nonnegative integers. The vector version of Sylvester's result, provided an analogue of F, was obtained by Knight [3] and recently again by Simpson and Tijdeman [5]. The purpose of this note is to show that the concept of the conductor K could be generalized as well as F.

Keywords:
Sylvester's formula, Frobenius number, integral monoid, Hilbert basis

MSC: (2000) 90C27, 52C07, 11D04

1 Introduction

A well known result due to Sylvester [7] is that

$$F = \alpha_1\alpha_2 - (\alpha_1 + \alpha_2) \tag{1.1}$$

is the largest integer not expressible as a nonnegative integer linear combination (shortly: *integer conic combination*) of α_1, α_2 if α_1, α_2 are positive relatively prime integers.

The integer

$$K = F + 1, \tag{1.2}$$

called *conductor*, is thus the smallest integer such that for every integer k with $K \leq k$ the equation $\alpha_1 x_1 + \alpha_2 x_2 = k$ has a solution over nonnegative integers.

It has been known for a long time that if $\alpha_1, ..., \alpha_n$ $(n \geq 3)$ are positive relatively prime integers then there exists a greatest integer F (called *Frobenius number*) which cannot be written as an integer conic combination of them. Clearly, if k is an integer greater than F, then the equation

$$\alpha_1 x_1 + ..., + \alpha_n x_n = k$$

has a solution over the nonnegative integers.

For the case of $n = 2$ we have (1.1), while no such solution is known for $n = 3$.

However, this result does generalize to vectors. This was made by Knight [3] and again by Simpson and Tijdeman [5]. We state their result in a new form as a Theorem 1.1.

Throughout this paper we resort to the following notation, definitions and claims. Additionally, we refer to [4] for the terminology and the standard notation.

- $\{a_1, ..., a_{n+1}\}$ denotes the set of $n+1$ integral column vectors in $\mathbb{Z}^n$.
- A is an $n \times (n+1)$ integral matrix of rank n with columns $a_1, ..., a_{n+1}$ and
- $L(A) = \{\sum_{i=1}^{i=n+1} a_i x_i \colon\ x_i \in \mathbb{Z}\} \subseteq \mathbb{Z}^n$ denotes the n-dimensional *lattice* generated by the columns of A.

- The set $\mathrm{mon}(A) = \{Ax\colon\ x \in \mathbb{Z}_+^{n+1}\}$ is an *integral monoid* in $\mathbb{Z}^n$ generated by the columns of A (or by A).
- Analogously, $\mathrm{cone}(A) = \{Ax\colon\ x \in \mathbb{R}_+^{n+1}\}$ is a *convex cone* in $\mathbb{R}^n$ generated by A.
- Suppose $a_{n+1} \in \mathrm{int}(\mathrm{cone}(a_1, ..., a_n))$ and
- $d = \det(a_1, ..., a_n) > 0$.
- Denote $d_i = \det(a_1, ..., a_{i-1}, a_{n+1}, a_{i+1}, ..., a_n)$ for $i = 1, ..., n$.

An element $s \in \mathrm{mon}(A)$ is called a *swelling-point* if each integral vector in the set $\{s + \mathrm{cone}(A)\}$ can be expressed as an integer conic combination of $a_1, ..., a_{n+1}$, i.e.,

$$(s + \mathrm{cone}(A)) \cap Z^n \subseteq \mathrm{mon}(A),$$

where $\{s + \mathrm{cone}(A)\}$ denotes the set of elements $s + x$ with $x \in \mathrm{cone}(A)$.

- S denotes the set of all swelling-points in $\mathrm{mon}(A)$.

Theorem 1.1 [3], [5] *Let the set of columns of A generates the standard lattice $\mathbb{Z}^n$. There exists a unique vector $F \in \mathbb{Z}^n$,*

$$F = d \cdot a_{n+1} - (a_1 + \cdots + a_n + a_{n+1}) \tag{1.3}$$

not expressible as an integer conic combination of $a_1, ..., a_{n+1}$ such that

$$int(F + \mathrm{cone}(A)) \cap \mathbb{Z}^n = S. \tag{1.4}$$

■

In other words, the equation (1.4) means that for each integral vector b with

$$b \in \mathrm{int}(F + \mathrm{cone}(A)) \tag{1.5}$$

the system $Ax = b$ has a nonnegative integral solution x.

The importance of Theorem 1.1 is that the vector F given by (1.3) may be considered as an analogue of Frobenius number. Hence, we call F the *Frobenius vector*.

Example 1.2 Let

$$A = \begin{pmatrix} 3 & 1 & 2 \\ 2 & 3 & 2 \end{pmatrix}.$$

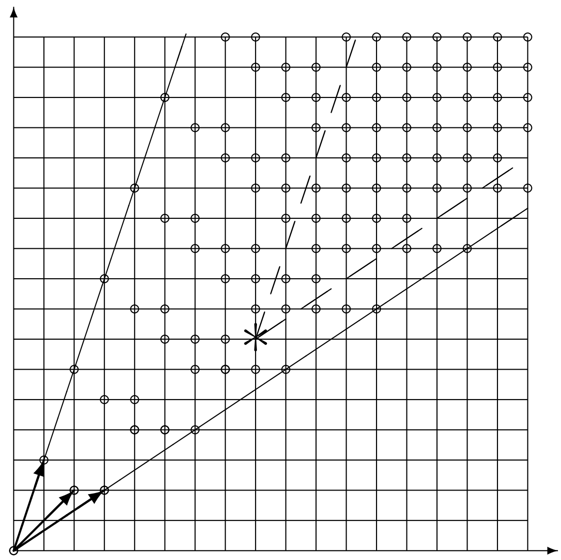

Figure 1: The elements of mon(A) are denoted by circles. The Frobenius vector F (see - the asterisk) is equal to $(8,7)^T$.

2 Main results

Before specializing further we give some general lemmas, some of which are almost immediate.

Lemma 2.1 *If $G \subseteq I\!N_o^n$, $G \neq \emptyset$, $I\!N_o = I\!N \cup \{0\}$, there exists a finite subset $\{g_1, ..., g_t\} \subseteq G$ for which*

$$g \in G \ \text{ implies } \ g_j \leq g \ \text{ for at least one } j = 1, ..., t. \tag{2.1}$$

Proof. Define

$$M = \{g \in G\colon \text{ no element } g' \in G \text{ with } g' \neq g \text{ satisfies } g' \leq g\}. \tag{2.2}$$

Since elements of M are incomparable, M is finite and $M = \{g_1, ..., g_t\}$. By definition (2.2) of M, (2.1) holds, since an infinite descending chain

$$v_1 \ngeq v_2 \ngeq v_3 \ngeq \cdots \tag{2.3}$$

of elements $v_j \in G$ is impossible, as $G \subseteq \mathbb{N}_o^n$.

■

Let $\text{GCD}(d, d_1, ..., d_n)$ be the greatest common divisor of $d, d_1, ..., d_n$. The following lemma is immediate.

Lemma 2.2

$$\text{GCD}(d, d_1, ..., d_n) = 1 \tag{2.4}$$

if and only if the set of columns of A generates the standard lattice $\mathbb{Z}^n$.

Proof. (2.4) is equivalent to the fact that the *Smith Normal Form* [1], [2] of the matrix A is of the form

$$\text{SNF}(A) = (I_{n\times n}, 0)$$

where $I_{n\times n}$ is an identity $n \times n$ matrix and 0 is the column vector of zeros. Clearly, two equivalent matrices A and $\text{SNF}(A)$ generate the same lattice, i.e., the standard lattice $\mathbb{Z}^n$.

■

Lemma 2.3 *If* $\text{GCD}(d, d_1, ..., d_n) = 1$ *and* $d, d_1, ..., d_n > 1$ *then* $F \in \text{cone}(A)$.

Proof. Suppose $d = 1$. This means that the set $\{a_1, ..., a_n\}$ forms a Hibert basis for the cone generated by the vectors $a_1, ..., a_n$.

(A finite set of integral vectors $\{a_1, ..., a_m\}$ is called a *Hilbert basis* (cf. [4]) if each integral vector in $\text{cone}(a_1, ..., a_m)$ is an integer conic combination of $a_1, ..., a_m$.)

Hence, as $\text{mon}(A) = \text{mon}(a_1, ..., a_n) = \text{cone}(A) \cap \mathbb{Z}^n$, $F \notin \text{cone}(A)$. On the other hand, for $d = 1$ by (1.3) clearly $F \notin \text{cone}(A)$.

Now let $d_i = 1$ for some $i \in \{1, ..., n\}$, i.e., the set of vectors $\{a_1, ..., a_{i-1}, a_{n+1}, a_{i+1}, ..., a_n\}$ forms a Hilbert basis for the cone generated by the vectors $a_1, ..., a_{i-1}, a_{n+1}, a_{i+1}, ..., a_n$. Suppose $F \in \text{cone}(A)$. Then there exists a face $f(F)$ of $\{F + \text{cone}(A)\}$ and a swelling-point s which is an element of the set

$$f(F) \cap \text{mon}(a_1, ..., a_{i-1}, a_{n+1}, a_{i+1}, ..., a_n)$$

contradicting the fact of Theorem 1.1 that all swelling-points belong to $\text{int}(F + \text{cone}(A))$.

■

We further claim that

- A is a $n \times (n+1)$ nonnegative integral matrix of rank n, hence cone(A) is *pointed*, i.e., the origin is a vertex of it and
- $\text{GCD}(d, d_1, ..., d_n) = 1$ and $d, d_1, ..., d_n > 1$.

Corollary 2.4 *Let $G = S$. There exists a finite subset $k(F) = \{k_1, ..., k_r\} \subset S$ for which*

$$s \in S \;\text{ implies }\; k_j \leq s \;\text{ for at least one } j = 1, ..., r.$$

Proof. By Lemma 2.1 this is straightforward.

■

Let the set $H = \{h_1, ..., h_l\}$ be the minimal Hilbert basis for the cone(A). As cone(A) is a pointed cone, such minimal (w.r.t. inclusions) Hilbert basis is uniquely determined [4] and can be computed by program *4ti2* developed by R.Hemmecke [6].

We say that the set $\{a_1, ..., a_n\}$ of columns of A *generates* a Hilbert basis $\{h_1, ..., h_n\}$ for cone(A) if there are positive integers $\alpha_1, ..., \alpha_n$ such that $\alpha_i h_i = a_i$ for $i = 1, ..., n$.

Let

$$D = \{\sum_{i=1}^{n} \lambda_i a_i \colon\; 0 \leq \lambda_i \leq 1,\; i = 1, ..., n\} \tag{2.5}$$

and denote by

$$H_{int} = H \cap (int(D) \cap \mathbb{Z}^n) \tag{2.6}$$

the set of vectors of H which lie in the interior of D.

Next, if all vectors of $H = \{h_1, ..., h_l\}$ lie on the faces of cone(A), consider the finite set of vectors

$$v(H) = \{v_J\colon\ v_J = \sum_{i \in J} h_i, \quad J \subset \{1, ..., l\}\}$$

in $int(D)$. Let $c(H)$ be the set of conically independent elements of $v(H)$.

(A finite set of vectors $\{v_1, ..., v_k\}$ is called *conically independent* with respect to A if $v_p - v_q = \sum_{i=1}^n m_i a_i$ with $m_i \in R_+$ implies $m_i = 0$ for $i = 1, ..., n$ and $p \neq q$.)

Define

$$1\!\!1(H) = \begin{cases} \sum_{i=1}^n h_i & if \quad a_1, ..., a_n \ generate\ Hilbert\ basis \\ c(H) & if \quad H \cap int(\text{cone}(A)) = \emptyset \\ H_{int}, & \quad\quad otherwise \end{cases} . \tag{2.7}$$

Theorem 2.5

$$(K(F) + \text{cone}(A)) \cap \mathbb{Z}^n = S, \tag{2.8}$$

where

$$K(F) = F + 1\!\!1(H). \tag{2.9}$$

Proof. Here the inclusion $\subseteq$ is trivial.

To prove the reverse inclusion, suppose $s \in S$. By Theorem 1.1, $s \in int(F + \text{cone}(A)) \cap \mathbb{Z}^n$. Then there are $\mu_1, ..., \mu_n \geq 0$ such that

$$s = F + \sum_{i=1}^n \mu_i a_i = F + \sum_{i=1}^n \lfloor \mu_i \rfloor a_i + \sum_{i=1}^n (\mu_i - \lfloor \mu_i \rfloor) a_i,$$

where for any real number t, $\lfloor t \rfloor$ denotes the greatest integer no greater than t. Because s, F and $\sum_{i=1}^n \lfloor \mu_i \rfloor a_i$ are integer vectors,

$$\sum_{i=1}^n (\mu_i - \lfloor \mu_i \rfloor) a_i \tag{2.10}$$

is an integer element of the set D given by (2.5).

We may assume $s \in (int(F+D)) \cap \mathbb{Z}^n$ with D defined by (2.5). Hence

$$s - F = \sum_{i=1}^{n} \lambda_i a_i, \quad 0 < \lambda_i < 1 \;\; for\ i = 1, ..., n \tag{2.11}$$

is an integral vector in the interior of D. Consider three cases.

(a) If for each $i = 1, ..., n$ $(\lambda_i a_i)$ is an integral vector with $\lambda_i a_i = x_i h_i$ for some $x_i \in \mathbb{Z}_+$ and h_i is an integral vector such that its components are relatively prime integers then by [4] it is immediate that the set $\{h_1, ..., h_n\}$ forms a minimal Hilbert basis for cone(A).

Thus, $s - F = \sum_{i=1}^{n} h_i + \sum_{i=1}^{n} \alpha_i h_i$, $\alpha_i \in \mathbb{Z}_+$. So s is an element of the set $(K(F) + \text{cone}(A)) \cap \mathbb{Z}^n$, with $K(F) = F + \sum_{i=1}^{n} h_i$.

(b) Given

$$H = \{h_1, ..., h_l\} \tag{2.12}$$

a Hilbert basis for cone(A). Assume $a_1, ..., a_n$ do not generate a Hilbert basis and $H \cap int(D) = \emptyset$. As w defined by (2.10) for $(s - F)$ given by (2.11) is an integer vector in $int(D)$ then

$$w = \sum_{i=1}^{l} \alpha_i h_i, \;\; \alpha_i \in \mathbb{Z}_+ \; for\ i = 1, ..., l. \tag{2.13}$$

Now the vector $(\sum_{i \in J} h_i) \in c(H)$ occurs in the right side of (2.13).

(c) Let $a_1, ..., a_n$ do not generate a Hilbert basis for cone(A) and let H given by (2.12) satisfy $H \cap int(D) \neq \emptyset$. As w which is equal to (2.10) for $(s - F)$ given by (2.11) is an integer vector in $int(D)$ then either w belongs to H_{int} or

$$w = \sum_{i=1}^{l} \beta_i h_i, \;\; \beta_i \in \mathbb{Z}_+ \; for\ i = 1, ..., l. \tag{2.14}$$

Now the vector

$$(\sum h_i, \quad h_i \in H_{int})$$

and hence $h_i \in H_{int}$ occurs in the right side of (2.14).

This implies inclusion $\supseteq$.

■

It is easy to see that the formula (2.9) is an analogue to the formula (1.2), i.e., to $K = F + 1$.

Moreover, observe that Corollary 2.4 is satisfied if we replace $k(F)$ by $K(F)$ given by (2.9).

Example 2.6 Let A be as in Example 1.2.

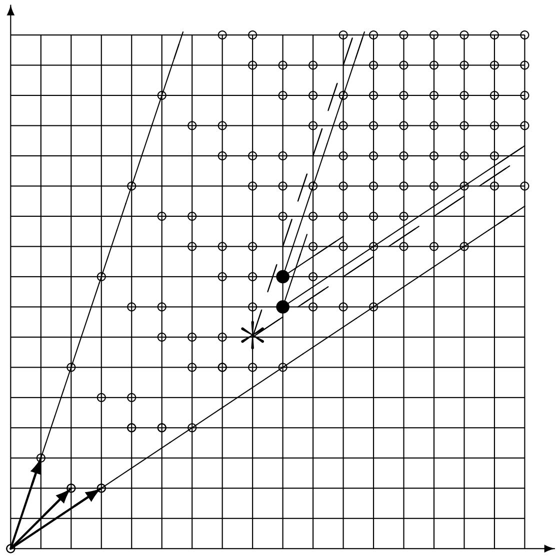

Figure 2: The conductor $K(F)$ consists of black circles $(9,8)^T$ and $(9,9)^T$.

References

[1] Bachem A., The theory of polyhedra and discrete optimization, University of Bonn, Bonn 1979.

[2] Kannan R., Bachem A., Polynomial algorithms for computing the Smith and Hermite normal forms of an integer matrix, SIAM J. Comput. 8 (1979) 499-507.

[3] Knight M. J., A generalization of a result of Sylvester's, Journal of Number Theory 12 (1980) 364-366.

[4] Schrijver A., Theory of linear and integer programming, Wiley-Chichester, 1986.

[5] Simpson R.J., Tijdeman R., Multi-dimensional versions of a theorem of Fine and Wilf and a formula of Sylvester, Proc. Amer. Math. Soc. 131 (2003) 1661-1671.

[6] Sturmfels B., Algebraic recipes for integer programming, in: Hoşten S., Lee J., Thomas R.R., eds., Trends in Optimization, Proceedings of Symposia in Applied Mathematics, AMS, 61 (2004) 99-113.

[7] Sylvester J.J., Mathematical questions with their solutions, Educational Times 41 (1884) 21.