involve
a journal of mathematics

The multidimensional Frobenius problem

Jeffrey Amos, Iuliana Pascu, Vadim Ponomarenko,
Enrique Treviño and Yan Zhang

msp

2011 vol. 4, no. 2

INVOLVE 4:2 (2011)
https://doi.org/10.2140/involve.2011.4.187

The multidimensional Frobenius problem

Jeffrey Amos, Iuliana Pascu, Vadim Ponomarenko,
Enrique Treviño and Yan Zhang

(Communicated by Scott Chapman)

We provide a variety of results concerning the problem of determining maximal vectors g such that the Diophantine system $Mx = g$ has no solution: conditions for the existence of g, conditions for the uniqueness of g, bounds on g, determining g explicitly in several important special cases, constructions for g, and a reduction for M.

1. Introduction

Let m, x be column vectors from the nonnegative integers $\mathbb{N}_0$. Georg Frobenius focused attention on determining the maximal integer g such that the linear Diophantine equation $m^T x = g$ has no solutions. This problem has attracted substantial attention in the last 100 years; for a survey see [Ramírez Alfonsín 2006]. In this paper, we consider the problem of determining maximal vectors g such that the system of linear Diophantine equations $Mx = g$ has no solutions.

For any real matrix X and any $S \subseteq \mathbb{R}$, we write X_S for $\{Xs : s \in S^k\}$, where k denotes the number of columns of X. We write X_1 for the vector in $X_{\{1\}}$. We fix $M \in \mathbb{Z}_{n\times(n+m)}$, and write $M = [A|B]$, where A is $n \times n$. We call $A_{\mathbb{R}_{\geq 0}}$ the *cone*, and $M_{\mathbb{N}_0}$ the *monoid*. $|A|$ denotes henceforth the absolute value of $\det A$, if A is a square matrix; but still the cardinality of A, if A is a set. If $|A| \neq 0$, then we follow [Novikov 1992] and call the cone *volume*. If each column of B lies in the volume cone, then we call M *simplicial*. Unless otherwise noted, we assume henceforth that M is simplicial. Note that if $n \leq 2$ and there is some half-space containing all the columns of M, then we may always rearrange columns to make M simplicial. For $x \in \mathbb{R}^n$, we call $x + M_{\mathbb{R}_{\geq 0}} = x + A_{\mathbb{R}_{\geq 0}}$ the cone at x, writing $\text{cone}(x)$.

Let $u, v \in \mathbb{R}^n$. If $u - v \in A_{\mathbb{Z}}$, then we write $u \equiv v$ and say that u, v are *equivalent mod* A. If $u - v \in A_{\mathbb{R}_{\geq 0}}$, then we write $u \geq v$. If $u - v \in A_{\mathbb{R}_{>0}}$, then we write $u \succ v$. Note that $u \succ v$ implies $u \geq v$, and $u \succ v \geq w$ implies $u \succ w$; however, $u \not\succeq v$ does

MSC2010: 11B75, 11D04, 11D72.
Keywords: Frobenius, coin-exchange, linear Diophantine system.
Research supported in part by NSF grant 0097366.

not imply that $u \succ v$. For $v \in \mathbb{R}^n$, we write $(v)_i$ for the i-th coordinate of v, and $[\succ v] = \{u \in \mathbb{Z}^n : u \succ v\}$. We say that v is *complete* if $[\succ v] \subseteq M_{\mathbb{N}_0}$. We set G, more precisely $G(M)$, to be the set of all $\geq$-minimal complete vectors. We call elements of G *Frobenius vectors*; they are the vector analogue of g that we will investigate.

Set $Q = (1/|A|)\mathbb{Z} \subseteq \mathbb{Q}$. Although G is defined in $\mathbb{R}^n$, in fact it is a subset of Q^n, by the following result. Furthermore, the columns of B are in $A_{Q^{\geq 0}}$; hence $M_{Q^{\geq 0}} = A_{Q^{\geq 0}}$ and without loss we work over Q rather than over $\mathbb{R}$.

Proposition 1.1. *Let $v \in \mathbb{R}^n$. There exists $v^\star \in Q^n$ with $[\succ v] = [\succ Av^\star]$ and $v \geq Av^\star$.*

Proof. We choose $v^\star \in Q^n$ such that $A^{-1}v - v^\star = \epsilon = (\epsilon_1, \epsilon_2, \ldots, \epsilon_n)$ with $0 \leq \epsilon_i < 1/|A|$. Multiplying by A we get $v - Av^\star = A\epsilon$; hence $v \geq Av^\star$. We will now show that for $u \in \mathbb{Z}^n$, $u \succ v$ if and only if $u \succ Av^\star$. If $u \succ v$, then $u \succ Av^\star$ because $u \succ v \geq Av^\star$. On the other hand, suppose that $u \succ Av^\star$ and $u \not\succ v$. Hence $u - Av^\star \in A_{\mathbb{R}^{>0}}$ and $u - v \in A_{\mathbb{R}} \setminus A_{\mathbb{R}^{>0}}$. Multiplying by A^{-1} we get $A^{-1}u - v^\star \in I_{\mathbb{R}^{>0}}$ and $A^{-1}u - A^{-1}v \in I_{\mathbb{R}} \setminus I_{\mathbb{R}^{>0}}$. Therefore, there is some coordinate i with $(A^{-1}u - v^\star)_i > 0$ and $(A^{-1}u - A^{-1}v)_i \leq 0$. Because $u \in \mathbb{Z}^n$ and A is an integer matrix, we have $A^{-1}u \in Q^n$; hence in fact $(A^{-1}u - v^\star)_i \geq 1/|A|$. Now, $0 \geq (A^{-1}u - A^{-1}v)_i = (A^{-1}u - v^\star - (A^{-1}v - v^\star))_i = (A^{-1}u - v^\star)_i - \epsilon_i \geq 1/|A| - \epsilon_i$. However, this contradicts $\epsilon_i < 1/|A|$. □

Let $x, y \in M_{Q^{\geq 0}}$. We write $x = Ax'$, $y = Ay'$, with $x', y' \in (Q^{\geq 0})^n$, define z' via $(z')_i = \max((x')_i, (y')_i)$, and set $\operatorname{lub}(x, y) = Az'$. We have $\operatorname{lub}(x, y) \in M_{Q^{\geq 0}}$, although in general $\operatorname{lub}(x, y) \notin M_{\mathbb{N}_0}$ (even if $x, y \in M_{\mathbb{N}_0}$) because $A^{-1}B$ need not have integer entries.

For $u \in M_Q$, we set $V(u) = (u + A_{Q\cap(0,1]}) \cap \mathbb{Z}^n$. It was known to Dedekind [1877] that $|V(u)| = |A|$, and that $V(u)$ is a complete set of coset representatives mod A (as restricted to $\mathbb{Z}^n$). Note that u is complete if and only if $V(u) \subseteq M_{\mathbb{N}_0}$.

The following equivalent conditions on M generalize the one-dimensional notion of relatively prime generators. Portions of the following have been repeatedly rediscovered [Frumkin 1981; Ivanov and Shevchenko 1975; Novikov 1992; Rycerz 2000; Vizvári 1987]. We assume henceforth, unless otherwise noted, that M possesses these properties. We call such M *dense*.

Theorem 1.2. *The following are equivalent*:

(1) *G is nonempty.*

(2) $M_{\mathbb{Z}} = \mathbb{Z}^n$.

(3) *For all unit vectors e_i $(1 \leq i \leq n)$, $e_i \in M_{\mathbb{Z}}$.*

(4) *There is some $v \in M_{\mathbb{N}_0}$ with $v + e_i \in M_{\mathbb{N}_0}$ for all unit vectors e_i.*

(5) *The GCD of all the $n \times n$ minors of M has absolute value* 1.

(6) *The elementary divisors of M are all* 1.

Proof. The proof follows the plan (1) $\iff$ (4) $\iff$ (3) $\iff$ (2) $\iff$ (6) $\iff$ (5).

(1) $\iff$ (4): Let $g \in G$. Choose $v \in [\succ g]$ far enough from the boundaries of the cone so that $v + e_i$ is also in $[\succ g]$ for all unit vectors e_i. Because g is complete, v and $v + e_i$ are all in $M_{\mathbb{N}_0}$. The other direction is proved in [Novikov 1992, Proposition 5].

(4) $\iff$ (3): For one direction, write $e_i = Mf_i$. Set $k = \max_i \|f_i\|_\infty$. Set $v = Mk^n$. We see that $v + e_i = M(k^n + f_i) \subseteq M_{\mathbb{N}_0}$. For the other direction, let $1 \le i \le n$. Write $v = Mw$, $v + e_i = Mw'$, where $w, w' \in \mathbb{N}_0^n$. Hence, $e_i = M(w' - w) \subseteq M_{\mathbb{Z}}$.

(3) $\iff$ (2): Let $v \in \mathbb{Z}^n$; write $v = (v_1, v_2, \dots, v_n)$. Write $e_i = Mf_i$, for $f_i \in \mathbb{Z}^n$. Then $v = M \sum v_i f_i$, as desired. The other direction is trivial.

(2) $\iff$ (6): We place M in Smith normal form: write $M = LNR$, where N is a diagonal matrix of the same dimensions as M, and L, R are square matrices, invertible over the integers. The diagonal entries of N are the elementary divisors of M. We therefore have that (2) $\iff N = [I|0] \iff$ (6).

(6) $\iff$ (5): The product of the elementary divisors is known (see, for example, [van der Waerden 1967, Remark 3 in Section 12.2]) to be the absolute value of the GCD of all $n \times n$ minors of M. If they are each one, then their product is one. Conversely, if their product is one, then they must each be one since they are all nonnegative integers. □

Classically, there is a second type of Frobenius number f, maximal so that $m^T x = f$ has no solutions with x from $\mathbb{N}$ (rather than $\mathbb{N}_0$). This does not alter the situation; in [Brauer and Shockley 1962] it was shown that $f = g + m^T 1$. A similar situation holds in the vector context.

Call v *f-complete* if $[\succ v] \subseteq M_{\mathbb{N}}$.

Proposition 1.3. *Let F be the set of all $\ge$-minimal f-complete vectors. Then $F = G + M_1$.*

Proof. It suffices to show that $v \in Q^n$ is complete if and only if $v + M_1$ is f-complete. The following conditions are equivalent for an integral vector u: (1) $u \in [\succ v + M_1]$; (2) $u \succ v + M_1$; (3) $(u - M_1) - v \in M_{\mathbb{R}_{\ge 0}}$; (4) $(u - M_1) \succ v$; (5) $(u - M_1) \in [\succ v]$. Now, suppose that v is complete. Let $u \in [\succ v + M_1]$; hence $(u - M_1) \in [\succ v] \subseteq M_{\mathbb{N}_0}$ and therefore $u \in M_{\mathbb{N}}$. So $v + M_1$ is f-complete. On the other hand, suppose that $v + M_1$ is f-complete. Let $(u - M_1) \in [\succ v]$; hence $u \in [\succ v + M_1] \subseteq M_{\mathbb{N}}$. Hence $u - M_1 \subseteq M_{\mathbb{N}} - M_1 = M_{\mathbb{N}_0}$, and v is complete. □

Having established the notation and basic groundwork for the problem, we now present two useful techniques: the method of critical elements, and the MIN method. Each will be shown to characterize the set G.

2. The method of critical elements

For a vector u and $i \in [1, n]$, let

$$C^i(u) = \{v : v \in \mathbb{Z}^n \setminus M_{\mathbb{N}_0},\ v = u + Aw,\ (w)_i = 0,\ (w)_j \in (0, 1] \text{ for } j \neq i\}.$$

This set captures all lattice points missing from the monoid, in the i-th face of the cone at u, that are minimal mod A. Let $C(u) = \bigcup_{i \in [1,n]} C^i(u)$, which is a disjoint union of finite sets. We call elements of $C(u)$ *critical*. Note that if $v \in C^i(u)$, then $v + Ae_i \in V(u)$. Critical elements characterize G, as shown by the following theorem.

Theorem 2.1. *Let x be complete. The following statemements are equivalent.*

(1) $x \in G$.

(2) *Each face of* $\text{cone}(x)$ *contains at least one lattice point not in the monoid.*

(3) $C^i(x) \neq \varnothing$ *for all* $i \in [1, n]$.

Proof. We write $x = Ax'$. For each $i \in [1, n]$, set $x^i = x - (1/|A|)Ae_i$ and $S_i = [\succ x^i] \setminus [\succ x]$. Observe that $S_i = \{Au \in \mathbb{Z}^n : (u)_j > (x')_j \text{ (for } j \neq i),\ (u)_i = (x')_i\}$; the S_i are the lattice points in the i-th face of $\text{cone}(x)$.

(1) $\Longrightarrow$ (2) If $S_i \subseteq M_{\mathbb{N}_0}$, then x^i is complete, which violates $x \in G$.

(2) $\Longrightarrow$ (3) Pick any minimal $y \in S_i \setminus M_{\mathbb{N}_0}$. Suppose that $(A^{-1}(y - x))_j \notin (0, 1]$ for $j \neq i$; in this case, $y - Ae_j$ would also be in $S_i \setminus M_{\mathbb{N}_0}$, violating the minimality of y. Hence $y \in C^i(x)$, and thus $C^i(x) \neq \varnothing$.

(3) $\Longrightarrow$ (1) If $x^\star < x$, then $x^\star \leq x^i$ for some i. But no x^i is complete; hence $x^\star$ is not complete. Thus x is $\geq$-minimal and complete and thus $x \in G$. $\square$

Critical elements can also be used to test for uniqueness of Frobenius vectors. Set $\bar{e}_i = \overline{1} - e_i = (1, 1, \ldots, 1, 0, 1, 1, \ldots, 1)$.

Theorem 2.2. *Let $g \in G$. Then $|G| = 1$ if and only if for each $i \in [1, n]$ there is some $c^i \in C^i(g)$ with $c^i + kA\bar{e}_i \notin M_{\mathbb{N}_0}$ for all $k \in \mathbb{N}_0$.*

Proof. Suppose that for each $i \in [1, n]$ there is some $c^i \in C^i(g)$ with $c^i + kA\bar{e}_i \notin M_{\mathbb{N}_0}$ for all k. Let $g' \in G$. If $g' \neq g$, then for some i we must have $(A^{-1}g')_i < (A^{-1}g)_i$. As $k \to \infty$, $(A^{-1}c^i + k\bar{e}_i)_j \to \infty$ (for $j \neq i$), but also $(A^{-1}c^i + k\bar{e}_i)_i = (A^{-1}g)_i$ for all k. Therefore, for some k we have $c^i + kA\bar{e}_i \succ g'$. Hence g' is not complete, which is violative of our assumption. Hence $|G| = 1$.

Now, let $g \in G$ be unique, let $i \in [1, n]$ be such that each $c^i \in C^i(g)$ has some $k(i)$ with $c^i + k(i)A\bar{e}_i \in M_{\mathbb{N}_0}$. If $c^i + kA\bar{e}_i \in M_{\mathbb{N}_0}$, then $c^i + k'A\bar{e}_i \in M_{\mathbb{N}_0}$ for any $k' \geq k$; hence because $|C^i(g)| < \infty$ there is some $K \in \mathbb{N}_0$ with $c^i + KA\bar{e}_i \in M_{\mathbb{N}_0}$

for all $c^i \in C^i(g)$. Now, set

$$g^\star = g + (K+1)A\bar{e}_i - (1/|A|)Ae_i,$$
$$S = [\succ g^\star]\backslash[\succ g] \subseteq \{u \in \mathbb{Z}^n : (A^{-1}(u-g))_i = 0,\ (A^{-1}(u-g))_j \geq K+1\ (j \neq i)\}.$$

We now show that $S\backslash M_{\mathbb{N}_0}$ is empty; otherwise, choose u therein. Set $u' = u - Aa$, where $(a)_i = 0$ and, for $j \neq i$,

$$(a)_j = \begin{cases} \lfloor (A^{-1}(u-g))_j \rfloor & \text{if } (A^{-1}(u-g))_j \notin \mathbb{Z}, \\ (A^{-1}(u-g))_j - 1 & \text{if } (A^{-1}(u-g))_j \in \mathbb{Z}, \end{cases}$$

Then $u' \in \mathbb{Z}^n \setminus M_{\mathbb{N}_0}$, since otherwise $u \in M_{\mathbb{N}_0}$. We also have $(A^{-1}(u'-g))_i = 0$ and $(A^{-1}(u'-g))_j \in (0, 1]$ for $j \neq i$; hence $u' \in C^i(g)$. But then $u' + KA\bar{e}_i \in M_{\mathbb{N}_0}$ and hence $u \in M_{\mathbb{N}_0}$ since $u - (u' + KA\bar{e}_i) \in A_{\mathbb{N}_0}$. Hence $S \subseteq M_{\mathbb{N}_0}$ and $g^\star$ is complete. Now take $g' \in G$ with $g' \leq g^\star$. We have $(A^{-1}g')_i \leq (A^{-1}g^\star)_i < (A^{-1}g)_i$ and hence $g' \neq g$, which is violative of our hypothesis. □

Our next result generalizes a one-dimensional reduction result in [Johnson 1960] which is very important because it allows the assumption that the generators are pairwise relatively prime. The vector generalization unfortunately does not permit us an analogous assumption in general.

Theorem 2.3. *Let $d \in \mathbb{N}$ and let $M = [A|B]$ be simplicial. Suppose that $N = [A|dB]$ is dense. Then M is dense, and $G(N) = dG(M) + (d-1)A_1$.*

Proof. Each $n \times n$ minor of M divides a corresponding minor of N, and hence M is dense. Further, d divides all minors of N apart from $|A|$, and hence $\gcd(|A|, d) = 1 = \gcd(|A|^2, d)$. We can therefore pick $d^\star \in \mathbb{N}$ with $d^\star d \in 1 + |A|^2\mathbb{N}_0$. For any $v \in Q^n$, we observe that $d^\star dv - v \in \mathbb{N}_0|A|^2Q^n = \mathbb{N}_0|A|\mathbb{Z}^n \subseteq A_{\mathbb{Z}}$; hence $d^\star dv \equiv v$. Set $\theta(x) = dx + (d-1)A1^n$. We will show for any $x \in Q^n$ that $x \in M_{\mathbb{N}_0}$ if and only if $\theta(x) \in N_{\mathbb{N}_0}$ (in particular, if $\theta(x) \in N_{\mathbb{N}_0}$, then $x \in \mathbb{Z}^n$). One direction is trivial; for the other, assume $\theta(x) \in N_{\mathbb{N}_0}$. We have $dx + dA1^n = A(y + 1^n) + dBz$, for $y \in \mathbb{N}_0^n$, and $z \in \mathbb{N}_0^m$. We observe that $x + A1^n = A(1/d)(y + 1^n) + Bz$, so $x + A1^n \geq Bz$. Also, $d^\star d(x + A1^n) = Ad^\star(y + 1^n) + d^\star dBz$, and hence $x + A1^n \equiv Bz$. Therefore $x + A1^n - Bz = Aw$ for some $w \in \mathbb{N}_0^n$. Further, $w = (1/d)(y + 1^n)$ so in fact $w \in \mathbb{N}^n$. Hence, $x = A(w - 1^n) + Bz \in M_{\mathbb{N}_0}$.

Next, we show that x is M-complete if and only if $\theta(x)$ is N-complete. First suppose that $\theta(x)$ is N-complete. Let $u \in [\succ x]$; we have $\theta(u) \in [\succ \theta(x)] \subseteq N_{\mathbb{N}_0}$. Hence $u \in M_{\mathbb{N}_0}$ so x is M-complete. Now suppose that x is M-complete. Let $u \in V(\theta(x))$. Set $u' \in V(x)$ with $du' \equiv u$. We have $u = \theta(x) + A\epsilon$, $u' = x + A\epsilon'$, where $\epsilon, \epsilon' \in (0, 1]^n$. We compute $u - du' = A\omega$, where $\omega = d(1^n - \epsilon') + (\epsilon - 1^n)$. Because $u \equiv du'$ we also have $u - du' = A\alpha$ with $\alpha \in \mathbb{Z}^n$. Since $|A| \neq 0$, we have $\omega = \alpha \in \mathbb{Z}^n$. Further, since $\epsilon, \epsilon' \in (0, 1]^n$, each coordinate of $d(1^n - \epsilon') + (\epsilon - 1^n)$

is strictly greater than -1 and hence $\omega \in \mathbb{N}_0^n$. We have $u' \in M_{\mathbb{N}_0}$ since x is M-complete. But then $du' \in N_{\mathbb{N}_0}$, and thus $u = du' + A\omega \in N_{\mathbb{N}_0}$. Hence $V(\theta(x)) \subseteq N_{\mathbb{N}_0}$ and thus $\theta(x)$ is N-complete.

Let $g \in G(M)$. We will show that $\theta(g) \in G(N)$. Let $i \in [1, n]$. By Theorem 2.1, there is $u \in [0, 1]^n$ with $u_i = 0$, $u_j > 0$ (for $j \neq i$), such that $g + Au \in \mathbb{Z}^n \setminus M_{\mathbb{N}_0}$. We have $\theta(g + Au) \in \mathbb{Z}^n \setminus N_{\mathbb{N}_0}$. We write $\theta(g + Au) = d(g + Au) + (d-1)A1^n = \theta(g) + Adu$. Write $du = u' + u''$ where $(u')_i = 0$, $(u')_j \in (0, 1]$, and $u'' \in \mathbb{N}_0^n$. We have $\theta(g) + Au' \in C^i(\theta(g))$; considering all i gives $\theta(g) \in G(N)$. Now, let $g \in G(N)$. We will show that $\theta^{-1}(g) = (1/d)(g - (d-1)A1^n) \in G(M)$. We again apply Theorem 2.1 to get an appropriate u with $g + Au \in \mathbb{Z}^n \setminus N_{\mathbb{N}_0}$. Note that $g + A(u + d1^n) \in N_{\mathbb{N}_0}$; hence

$$\begin{aligned}\theta^{-1}(g + A(u + d1^n)) &= (1/d)(g + Au + dA1^n - (d-1)A1^n) \\ &= \theta^{-1}(g) + (1/d)Au + A1^n \in M_{\mathbb{N}_0} \subseteq \mathbb{Z}^n.\end{aligned}$$

Thus, $\theta^{-1}(g + Au) = (1/d)(g + Au - (d-1)A1^n) = \theta^{-1}(g) + (1/d)Au \in \mathbb{Z}^n$. We therefore have $\theta^{-1}(g + Au) \in C^i(\theta^{-1}(g))$; considering all i gives $\theta^{-1}(g) \in G(M)$. □

3. The MIN method

Let $\mathrm{MIN} = \{x : x \in M_{\mathbb{N}_0};\ \text{for all } y \in M_{\mathbb{N}_0},\ \text{if } y \equiv x \text{ then } y \geq x\}$. Provided M is dense, MIN will have at least one representative of each of the $|A|$ equivalence classes mod A. MIN is a generalization of a one-dimensional method in [Brauer and Shockley 1962]; the following result shows that it characterizes the set G.

Theorem 3.1. *Let $g \in G$. Then $g = \mathrm{lub}(N) - A_1$ for some complete set of coset representatives $N \subseteq \mathrm{MIN}$. Further, if $n < |A|$ then there is some $N' \subseteq N$ with $|N'| = n$ and $\mathrm{lub}(N) = \mathrm{lub}(N')$.*

Proof. Observe that $V(g) \subseteq [\succ g]$, and hence $V(g) \subseteq M_{\mathbb{N}_0}$ since g is complete. Let $\mathrm{MIN}' = \{u \in \mathrm{MIN} : \exists v \in V(g), u \equiv v, u \leq v\}$. Now, for $v \in C^i(g)$, we have $v + Ae_i \in V(g)$. Let $v_{\mathrm{MIN}} \in \mathrm{MIN}'$ with $v_{\mathrm{MIN}} \equiv v + Ae_i$ and $v_{\mathrm{MIN}} \leq v + Ae_i$. We must have $(A^{-1}v_{\mathrm{MIN}})_i \geq (A^{-1}v)_i + 1 = (A^{-1}g)_i + 1$ because otherwise $v \in v_{\mathrm{MIN}} + A_{\mathbb{N}_0}$ and therefore $v \in M_{\mathbb{N}_0}$, which is violative of $v \in C^i(g)$. Set $N' = \{v_{\mathrm{MIN}} : i \in [1, n]\}$. We have $\mathrm{lub}(N') \geq g + A_1$, but also we have $g + A_1 = \mathrm{lub}(V(g)) \geq \mathrm{lub}(\mathrm{MIN}') \geq \mathrm{lub}(N')$. Hence all the inequalities are equalities, and in fact $\mathrm{lub}(N') = \mathrm{lub}(N)$ for any N with $N' \subseteq N \subseteq \mathrm{MIN}'$. Finally, we note that $|N'| \leq n$ but also we may insist that $|N'| \leq |A|$ because $|V(g)| = |A|$. □

Elements of MIN have a particularly nice form. This is quite useful in computations.

Theorem 3.2. $\mathrm{MIN} \subseteq \{Bx : x \in \mathbb{N}_0^m, \|x\|_1 \leq |A| - 1\}.$

Proof. Let $v \in \mathrm{MIN} \subseteq M_{\mathbb{N}_0}$. Write $v = Mv'$, where $v' \in \mathbb{N}_0^{n+m}$. Suppose that $(v')_i > 0$, for $1 \le i \le n$. Set $w' = v' - e_i$, and $w = Mw'$. We see that $w \equiv v$, $w \le v$, and $w \in M_{\mathbb{N}_0}$; this contradicts that $v \in \mathrm{MIN}$. Hence $\mathrm{MIN} \subseteq B_{\mathbb{N}_0}$. Let $z = Bx \in \mathrm{MIN}$. Suppose that $\|x\|_1 \ge |A|$. Start with 0 and increment one coordinate at a time, building a sequence $B0 = Bv_0 \lneq Bv_1 \lneq Bv_2 \lneq \cdots \lneq Bv_{\|x\|_1} = z$ where each $v_i \in \mathbb{N}_0^m$. We may do this since M is simplicial. Because there are at least $|A|+1$ terms, two (say $Bv_a \lneq Bv_b$) are congruent mod A. We have $z - Bv_b \in M_{\mathbb{N}_0}$ and so $y = z - (Bv_b - Bv_a) \in M_{\mathbb{N}_0}$, but $y \lneq z$ and $y \equiv z$. This violates that $z \in \mathrm{MIN}$. □

Corollary 3.3. $|G|$ *is finite.*

The following result, proved first in [Knight 1980] and rediscovered in [Simpson and Tijdeman 2003], generalizes the classical one-dimensional result on two generators that $g(a_1, a_2) = a_1a_2 - a_1 - a_2$. Note that in the special case where $m = 1$, we must have that $|G| = 1$ and $G \subseteq \mathbb{Z}^n$. Neither of these necessarily holds for $m > 1$.

Corollary 3.4. *If* $m = 1$ *then* $G = \{|A|B - A_1 - B\}$.

Proof. By Theorem 3.2, we have $\mathrm{MIN} = \{0, B, 2B, \ldots, (|A|-1)B\}$, a complete set of coset representatives. By Theorem 3.1, any $g \in G$ must have $g + A_1 = \mathrm{lub}(MIN) = (|A|-1)B$. □

Corollary 3.4 can be extended to the case where the column space of B is one dimensional, using as an oracle function the (one-dimensional) Frobenius number. In this special case we again have $|G| = 1$ and $G \subseteq \mathbb{Z}^n$.

Theorem 3.5. *Consider a dense* $M = [A|B]$ *with* B *a column* $(n \times 1)$ *vector, i.e., the special case* $m = 1$. *Let* $C = [c_1, c_2, \ldots, c_m] \in \mathbb{N}^m$. *Suppose that* $P = [\,|A|\mid C\,]$ *is dense. Then* $N = [A|BC]$ *is dense, and* $G(N) = \{G(P)B + |A|B - A_1\}$.

Proof. By Theorem 3.2, we have $\mathrm{MIN}(M) = \{0, B, \ldots, (|A|-1)B\}$. Hence $\mathbb{Z}^n/A\mathbb{Z}^n$ is cyclic, and B is a generator. Let S denote the set of all $n \times n$ minors of M, apart from $|A|$. Using the denseness of M and P, we have

$$\begin{aligned}\gcd(|A|, \{c_i s : 1 \le i \le m, s \in S\}) &= \gcd(|A|, \gcd(c_1, c_2, \ldots, c_m)\gcd(S))\\ &= \gcd(|A|, \gcd(S)) = 1;\end{aligned}$$

hence N is dense. Again by Theorem 3.2, we have $\mathrm{MIN}(N) \subseteq B_{\mathbb{N}_0}$. We now show that $G(P)B \notin M_{\mathbb{N}_0}$. Suppose otherwise. We then write $G(P)B = Ax + BCy$ and hence $Ax = Bq$ for $q = (G(P) - Cy)$. We conclude that $qB \equiv 0 \bmod A$ and hence $q = k|A|$ for some $k \in \mathbb{N}$ ($k > 0$ since M is simplicial) since B generates $\mathbb{Z}^n/A\mathbb{Z}^n$. We now have $BG(P) = Bk|A| + BCy$, and hence $G(P) = k|A| + Cy$. But now $G(P) - 1$ is complete (with respect to P), which violates the definition of $G(P)$. Therefore $G(P)B \notin M_{\mathbb{N}_0}$. On the other hand, if $\alpha \in \mathbb{Z}$ and $\alpha > G(P)$ we have $\alpha = k|A| + Cy$, for some $k, y \in \mathbb{N}_0$. Therefore, we have $B\alpha = k|A|B + BCy =$

$A\left(k|A|A^{-1}B\right)+BCy \in M_{\mathbb{N}_0}$ (note that $A^{-1}B \in Q^{\geq 0}$ since M is simplicial). Hence, $T=\{G(P)B+kB : k \in [1,|A|]\} \subseteq M_{\mathbb{N}_0}$, with $\text{lub}(T)=G(P)B+|A|B=\beta$. Let $g \in G(N)$, and let M be chosen as in Theorem 3.1 with $|M|=|A|$. Since T is a complete set of coset representatives and both T and $\text{MIN}(N)$ lie on $B\mathbb{R}$, we have $\text{lub}(M) \leq \text{lub}(\text{MIN}(N)) \leq \text{lub}(T)=G(P)B+|A|B=\beta$. However, the coset of β is precisely $\{G(P)B+k|A|B : k \in \mathbb{Z}\}$. Therefore, β is the unique representative of its equivalence class in MIN, and thus $\beta \in M$ and $\text{lub}(M)=\beta$. Hence $g+A_1=\beta$ for all $g \in G$, as desired. □

Example 3.6. Consider $N=\left(\begin{smallmatrix}5 & 0 & 84 & 105\\ 0 & 4 & 84 & 105\end{smallmatrix}\right)$. We have $N=[A|BC]$, for $A=\left(\begin{smallmatrix}5 & 0\\ 0 & 4\end{smallmatrix}\right)$, $B=\left(\begin{smallmatrix}3\\ 3\end{smallmatrix}\right)$, and $C=(28,35)$. Following Theorem 3.5, we have $P=(20,28,35)$. $\gcd(20,28,35)=1$ so P is dense; we now calculate $G(P)=197$ using our one-dimensional oracle. Therefore N is dense and $G(N)=\left\{\left(\begin{smallmatrix}646\\ 647\end{smallmatrix}\right)\right\}$.

We give three more results using this method. First, we present a $\leq$-bound for G. This generalizes a one dimensional bound, attributed to Schur in [Brauer 1942]: $g(a_1,a_2,\ldots,a_k) \leq a_1a_k-a_1-a_k$ (where $a_1<a_2<\cdots<a_k$). Note that Corollary 3.4 shows that equality is sometimes achieved.

Theorem 3.7. *For all $g \in G$, $g \leq \text{lub}\left(\{|A|b-A_1-b : b \text{ a column of } B\}\right)$.*

Proof. Let $x \in \text{MIN}$, fix $1 \leq i \leq n$, and write

$$(A^{-1}x)_i=(A^{-1}Bx')_i=\Bigl(\sum_b (x')_b A^{-1}b\Bigr)_i,$$

where b ranges over all the columns of B. Set $b^\star$ to be a column of B with $(A^{-1}b^\star)_i$ maximal. By Theorem 3.2, we have that $(A^{-1}x)_i \leq (A^{-1}b^\star)_i\|x'\|_1 \leq (A^{-1}b^\star)_i(|A|-1)$. By the choice of $b^\star$, and by varying i, we have shown that $x \leq \text{lub}(\{(|A|-1)b\})$ and hence $\text{lub}(\text{MIN}) \leq \text{lub}(\{(|A|-1)b\})$. For any $g \in G$, we apply Theorem 3.1 and have $g+A_1 \leq \text{lub}(\text{MIN}) \leq \text{lub}(\{(|A|-1)b\})$. □

Next, we characterize possible G in our context for the special case $m=1$. This generalizes a one-dimensional construction found in [Rosales et al. 2004]. If we allow $m=2$, then it is an open problem to determine whether all G are possible.

Theorem 3.8. *Let $g \in \mathbb{Z}^n$. There exists a simplicial, dense, M with $m=1$ and $G=\{g\}$ if and only if $\frac{1}{2}g \notin \mathbb{Z}^n$.*

Proof. Suppose $\frac{1}{2}g \notin \mathbb{Z}^n$. By applying an invertible change of basis, if necessary, we assume without loss that $g \in \mathbb{N}^n$ and that $\frac{1}{2}(g)_1 \notin \mathbb{Z}$. Set $A=\text{diag}(2,1,1,\ldots,1)$, and set $B=A_1+g$. For $i \in [1,n]$, define $A^{\underline{i}}$ to be A with the i-th column replaced by B. Note that $\det A=2$ and $\det A^{\underline{1}}=2+(g)_1$ (which is odd), and hence M is dense. We now apply Corollary 3.4 to get $G=\{g\}$, as desired. Suppose now that we have a simplicial dense M, with $G=\{g\}$ and $\frac{1}{2}g \in \mathbb{Z}^n$. Applying Corollary 3.4 again, we get that $g+A_1=(|A|-1)B$. Suppose that $|A|$ were odd. Then each coordinate of $(|A|-1)B$ is even, as is each coordinate of g, and hence so is each coordinate of A_1. Considering the integers mod 2, we have $|A|=1$ but $A_1=0^n$, a contradiction. Therefore we must have that $|A|$ is even. We now consider the system $A(x_1,x_2,\ldots,x_n)^T=B$. We may apply Cramer's rule since $|A|\neq 0$ and $B\neq 0^n$; we find that, uniquely, $\det A^{\underline{i}}=x_i|A|$. We now consider the system reduced mod 2 (working in $\mathbb{Q}/2\mathbb{Q}$) and find that 1^n solves the reduced system, as $B=|A|B-g-A_1\equiv -A1^n\equiv A1^n \pmod 2$. Hence, each x_i is in fact an odd integer, and thus $\det A^{\underline{i}}$ is an even integer. Consequently, all $n\times n$ minors of M are even, which is violative of the denseness of M. $\square$

Our last result combines the two methods presented. It generalizes the one-dimensional theorem $g(a,a+c,a+2c,\ldots,a+kc)=a\lceil (a-1)/k\rceil+ac-a-c$, as proved in [Roberts 1956]. The following determines G, for M of a similarly special type.

Theorem 3.9. *Fix A and a vector $c\geq 0$. Set $C=c(1^n)^T$, a square matrix, and fix $k\in\mathbb{N}$. Set $M=[A|A+C|A+2C|\cdots|A+kC]$. Suppose that M is dense. Then $G(M)=\{Ax+|A|c-A_1-c : x\in\mathbb{N}_0^n,\ \|x\|_1=\lceil(|A|-1)/k\rceil\}$.*

Proof. We have

$$\begin{aligned}
M_{\mathbb{N}_0}&=\Big\{\sum_{i=0}^{k}(A+iC)x^i : x^i\in\mathbb{N}_0^n\Big\}=\Big\{A\sum_{i=0}^{k}x^i+C\sum_{i=0}^{k}ix^i : x^i\in\mathbb{N}_0^n\Big\}\\
&=\Big\{A\sum_{i=0}^{k}x^i+c\sum_{i=0}^{k}i\|x^i\|_1 : x^i\in\mathbb{N}_0^n\Big\}\\
&=\Big\{Ax+c\sum_{i=0}^{k}i\|x^i\|_1 : x^i\in\mathbb{N}_0^n;\ x=\sum_{i=0}^{k}x^i\Big\}.
\end{aligned}$$

Now, for a fixed $x\in\mathbb{N}_0^n$, as we vary the decomposition $x=\sum_{i=0}^{k}x^i$ (for $x^i\in\mathbb{N}_0^n$), we find that $\sum_{i=0}^{k}i\|x^i\|_1$ takes on all values from 0 to $k\|x\|_1$. Hence $M_{\mathbb{N}_0}=\{Ax+c\gamma : x\in\mathbb{N}_0^n,\ \gamma\in\mathbb{N}_0,\ \gamma\leq k\|x\|_1\}$.

Choose any $x\in\mathbb{N}_0^n$ satisfying $\|x\|_1=\lceil(|A|-1)/k\rceil$. Set $T=\{Ax+c\gamma\in M_{\mathbb{N}_0} : 0\leq\gamma\leq|A|-1\}$. By construction, we have $T\subseteq M_{\mathbb{N}_0}$. Further, the elements of T must be inequivalent mod A, since c is a generator of the cyclic group $\mathbb{Z}^n/A_{\mathbb{Z}}$. Set $h=\operatorname{lub}(T)-A_1=Ax+(|A|-1)c-A_1$. Note that each $t\in T$ either has $t\in V(h)$ or $t\leq t'$ (and $t\equiv t'$) for some $t'\in V(h)$; hence $V(h)\subseteq M_{\mathbb{N}_0}$ and h is complete. For any $i\in[1,n]$, $|A|-1>k\|x-e_i\|_1$, so $A(x-e_i)+(|A|-1)c\in C^i(h)$, and thus $h\in G(M)$. Now, let $g\in G(M)$. By Theorem 3.1, we have $g\geq Ax+(|A|-1)c-A_1$, for some $x\in\mathbb{N}_0^n$ with $|A|-1\leq k\|x\|_1$. By our earlier observation, $Ax+(|A|-1)c-A_1\in G(M)$, so we have equality by the minimality of g. $\square$

Example 3.10. Consider $M=\left(\begin{smallmatrix}5&0&7&2&9&4&11&6&13&8&15&10&17&12&19&14\\0&4&1&5&2&6&3&7&4&8&5&9&6&10&7&11\end{smallmatrix}\right)$. We see that $M=[A|A+C|A+2C|A+3C|A+4C|A+5C|A+6C|A+7C]$ for $A=\left(\begin{smallmatrix}5&0\\0&4\end{smallmatrix}\right)$ and

$C=\left(\begin{smallmatrix}2&2\\1&1\end{smallmatrix}\right)$. M is dense since $|A|=20$, $|A+C|=33$ and $\gcd(20,33)=1$. Applying Theorem 3.9, we get $G(M)=\left\{Ax+\left(\begin{smallmatrix}33\\15\end{smallmatrix}\right):x,\ \|x\|_1=3\right\}=\left\{\left(\begin{smallmatrix}48\\15\end{smallmatrix}\right),\left(\begin{smallmatrix}43\\19\end{smallmatrix}\right),\left(\begin{smallmatrix}38\\23\end{smallmatrix}\right),\left(\begin{smallmatrix}33\\27\end{smallmatrix}\right)\right\}$.

Acknowledgements

The authors would like to gratefully acknowledge the helpful comments of the anonymous referees.

References

[Brauer 1942] A. Brauer, "On a problem of partitions", *Amer. J. Math.* **64** (1942), 299–312. MR 3,270d Zbl 0061.06801

[Brauer and Shockley 1962] A. Brauer and J. E. Shockley, "On a problem of Frobenius", *J. Reine Angew. Math.* **211** (1962), 215–220. MR 26 #6113 Zbl 0108.04604

[Dedekind 1877] R. Dedekind, "Sur la théorie des nombres entiers algébriques", *Darboux Bull.* **9** (1877), 278. Translated as *Theory of algebraic integers*, Cambridge University Press, 1996.

[Frumkin 1981] M. A. Frumkin, "On the number of nonnegative integer solutions of a system of linear Diophantine equations", pp. 95–108 in *Studies on graphs and discrete programming* (Brussels, 1979), edited by P. Hansen, Ann. Discrete Math. **11**, North-Holland, Amsterdam, 1981. MR 83k:10028 Zbl 0477.90048

[Ivanov and Shevchenko 1975] N. N. Ivanov and V. N. Shevchenko, "The structure of a finitely generated semilattice", *Dokl. Akad. Nauk BSSR* **19**:9 (1975), 773–774. In Russian. MR 52 #8075 Zbl 0312.10009

[Johnson 1960] S. M. Johnson, "A linear diophantine problem", *Canad. J. Math.* **12** (1960), 390–398. MR 22 #12074 Zbl 0096.02803

[Knight 1980] M. J. Knight, "A generalization of a result of Sylvester's", *J. Number Theory* **12**:3 (1980), 364–366. MR 81j:10019 Zbl 0441.10010

[Novikov 1992] B. V. Novikov, "On the structure of subsets of a vector lattice that are closed with respect to addition", *Ukrain. Geom. Sb.* 35 (1992), 99–103. In Russian; translated in *J. Math. Sci.* **72**:4 (1994), 3223–3225. MR 95b:52027 Zbl 0850.06010

[Ramírez Alfonsín 2006] J. L. Ramírez Alfonsín, *The Diophantine Frobenius problem*, Oxford Lecture Series in Mathematics and its Applications **30**, Oxford University Press, Oxford, 2006. MR 2007i:11052 Zbl 1134.11012

[Roberts 1956] J. B. Roberts, "Note on linear forms", *Proc. Amer. Math. Soc.* **7** (1956), 465–469. MR 19,1038d Zbl 0071.03902

[Rosales et al. 2004] J. C. Rosales, P. A. García-Sánchez, and J. I. García-García, "Every positive integer is the Frobenius number of a numerical semigroup with three generators", *Math. Scand.* **94**:1 (2004), 5–12. MR 2004j:20117 Zbl 1077.20071

[Rycerz 2000] A. Rycerz, "The generalized residue classes and integral monoids with minimal sets", *Opuscula Math.* 20 (2000), 65–69. MR 2002k:11035

[Simpson and Tijdeman 2003] R. J. Simpson and R. Tijdeman, "Multi-dimensional versions of a theorem of Fine and Wilf and a formula of Sylvester", *Proc. Amer. Math. Soc.* **131**:6 (2003), 1661–1671. MR 2004k:11025 Zbl 1013.05087

[Vizvári 1987] B. Vizvári, "An application of Gomory cuts in number theory", *Period. Math. Hungar.* **18**:3 (1987), 213–228. MR 89d:11017 Zbl 0626.10013 [van der Waerden 1967] B. L. van der Waerden, *Algebra*, vol. 2, 5th ed., Heidelberger Taschenbücher **23**, Springer, Berlin, 1967. In German; translated as *Algebra*, vol. 2, Frederick Ungar, New York, 1970. MR 41 #8187b

Received: 2011-03-02 Revised: 2011-05-09 Accepted: 2011-05-09

jmamos1984@gmail.com *Department of Mathematics, Kansas State University, Manhattan, KS 66506, United States*

ipascu@wellesley.edu *Department of Economics, Massachusetts Institute of Technology, 50 Memorial Drive, Cambridge, MA 02142, United States*

vadim123@gmail.com *Department of Mathematics and Statistics, San Diego State University, 5500 Campanile Drive, San Diego CA 92182-7720, United States*
http://www-rohan.sdsu.edu/~vadim/

enrique.trevino@dartmouth.edu *Department of Mathematics, Dartmouth College, Hanover, NH 03755, United States*

yanzhang@fas.harvard.edu *Department of Mathematics, Massachusetts Institute of Technology, 50 Memorial Drive, 77 Massachusetts Avenue, Cambridge, MA 02139-4307, United States*

involve

pjm.math.berkeley.edu/involve

See inside back cover or http://pjm.math.berkeley.edu/involve for submission instructions.

The subscription price for 2011 is US $100/year for the electronic version, and $130/year (+$35 shipping outside the US) for print and electronic. Subscriptions, requests for back issues from the last three years and changes of subscribers address should be sent to Mathematical Sciences Publishers, Department of Mathematics, University of California, Berkeley, CA 94704-3840, USA.

Involve (ISSN 1944-4184 electronic, 1944-4176 printed) at Mathematical Sciences Publishers, Department of Mathematics, University of California, Berkeley, CA 94720-3840 is published continuously online. Periodical rate postage paid at Berkeley, CA 94704, and additional mailing offices.

Involve peer review and production are managed by EditFLOW™ from Mathematical Sciences Publishers.

PUBLISHED BY

mathematical sciences publishers

http://msp.org/

A NON-PROFIT CORPORATION

Typeset in LaTeX

involve

2011 vol. 4 no. 2