arXiv:1602.00344v3 [math.OC] 6 Jan 2017

SPARSE SOLUTIONS OF LINEAR DIOPHANTINE EQUATIONS

ISKANDER ALIEV, JESÚS A. DE LOERA, TIMM OERTEL, AND CHRISTOPHER O'NEILL

Abstract. We present structural results on solutions to the Diophantine system $A\boldsymbol{y} = \boldsymbol{b}$, $\boldsymbol{y} \in \mathbb{Z}^t_{\geq 0}$ with the smallest number of non-zero entries. Our tools are algebraic and number theoretic in nature and include Siegel's Lemma, generating functions, and commutative algebra. These results have some interesting consequences in discrete optimization.

1. Introduction

Let A be an integer $d \times t$ matrix and let $\boldsymbol{b}$ be an integer d-dimensional vector. The purpose of this work is to study structural properties of the solutions to the non-linear integer optimization problem

$$\min\{\|\boldsymbol{y}\|_0 : A\boldsymbol{y} = \boldsymbol{b}, \boldsymbol{y} \in \mathbb{Z}^t_{\geq 0}\}. \tag{1}$$

Here, $\|\cdot\|_0$ denotes the 0-norm, which counts the cardinality of the *support* of $\boldsymbol{y}$, i.e. $\operatorname{supp}(\boldsymbol{y}) = \{i : y_i \neq 0\}$. In other words, the value of $\|\boldsymbol{y}\|_0$ equals the number of non-zero entries in the vector $\boldsymbol{y}$. Problem (1) aims to find the vector of minimal support.

Before we present our results and state prior work we introduce some basic notation. In this paper, $\log(a)$ refers to the base two logarithm used to measure bit-size. Let $A = (\boldsymbol{x}_1, \ldots, \boldsymbol{x}_t) \in \mathbb{Z}^{d\times t}$ be a matrix (defining Problem (1)), where the columns come from a finite set of vectors $X = \{\boldsymbol{x}_1, \ldots, \boldsymbol{x}_t\}$. In what follows we sometimes use A and X interchangeably.

The *conic hull* of X is the set

$$\operatorname{cone}(X) = \{\lambda_1\boldsymbol{x}_1 + \cdots + \lambda_t\boldsymbol{x}_t : \boldsymbol{x}_1, \ldots, \boldsymbol{x}_t \in X, \lambda_1, \ldots, \lambda_t \in \mathbb{R}_{\geq 0}\},$$

and the *semigroup* of X or the *integer conic hull* of X is the set

$$\operatorname{Sg}(X) = \{\lambda_1\boldsymbol{x}_1 + \cdots + \lambda_t\boldsymbol{x}_t : \boldsymbol{x}_1, \ldots, \boldsymbol{x}_t \in X, \lambda_1, \ldots, \lambda_t \in \mathbb{Z}_{\geq 0}\}.$$

For each $\boldsymbol{b} \in \operatorname{Sg}(X)$, we let

$$\mathsf{P}_X(\boldsymbol{b}) = \{\boldsymbol{\lambda} \in \mathbb{Z}^t_{\geq 0} : \lambda_1\boldsymbol{x}_1 + \cdots + \lambda_t\boldsymbol{x}_t = \boldsymbol{b}\}$$

denote the solution set for $\boldsymbol{b}$. We are interested in the asymptotic behavior of the function

$$\mathsf{m}_0(\boldsymbol{b}) = \min\{\|\boldsymbol{\lambda}\|_0 : \boldsymbol{\lambda} \in \mathsf{P}_X(\boldsymbol{b})\},$$

as well as methods of estimating the function

$$\mathsf{M}_0(X) = \max\{\mathsf{m}_0(\boldsymbol{b}) : \boldsymbol{b} \in \operatorname{Sg}(X)\}.$$

Finding the sparsest solution of a system of linear equations has many applications and there is a rich literature about this problem. For real variables, the 0-norm minimization problem has become quite popular in signal processing through the theory of *compressed*

Date: January 9, 2017.

sensing. It is known that a linear programming relaxation provides a guaranteed approximation [10, 11]. Moreover, many nice properties for the size of the solution are known for the case of random matrices [8, 11].

In this paper, we consider *integer* solutions, which have various applications as well. Integer sparsity appears in the setting of linear codes over finite fields, where the 0-norm is the *Hamming distance*, and the problem is closely related to the *nearest codeword problem* as well as to the problem of finding shortest cycles on graphs and matroids; see [4, 12, 26, 43] and references therein. Sparse integer solutions also appear in the context of finding guarantees for bin-packing problems via the Gilmore-Gomory formulation [22], as first suggested in [24]. More generally, upper bounds given for the size of the sparsest integer solution indicate that if there exists an optimal solution to such an integer program, then there exists one which is polynomial in the number of equations and the maximum binary encoding length among integers in the objective function vector and the constraint matrix (see [16, Section 3]). The problem of estimating $\mathsf{M}_0(X)$ goes back to classical results on the integer Carathéodory problem. Cook, Fonlupt, and Schrijver [13] showed that $\mathsf{M}_0(X) \leq 2d-1$ if $C = \operatorname{cone}(X)$ is pointed and X forms a Hilbert basis of C. This result was later improved by Sebő [36] to $\mathsf{M}_0(X) \leq 2d-2$. It remains an open question to determine a sharp upper bound in the Hilbert basis setting, in [9] an example is provided where $\mathsf{M}_0(X) = \lfloor \frac{7}{6}d \rfloor$. For an arbitrary finite set $X \subset \mathbb{Z}^d$, Eisenbrand and Shmonin [16] obtained the bound

$$\mathsf{M}_0(X) \leq 2d \log(4d\|X\|_\infty), \tag{2}$$

where $\|X\|_\infty = \max_{\boldsymbol{x}\in X} \|\boldsymbol{x}\|_\infty$ (recall that for a vector $\boldsymbol{x}$, one defines $\|\boldsymbol{x}\|_\infty = \max |x_i|$).

For linearly independent vectors $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_r$ in $\mathbb{R}^t$, the set $\Lambda = \{\sum_{i=1}^r z_i \boldsymbol{v}_i,\ z_i \in \mathbb{Z}\}$ is a r-dimensional *lattice* with *basis* $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_r$ and *determinant* $\det(\Lambda) = (\det(\boldsymbol{v}_i \cdot \boldsymbol{v}_j)_{1\leq i,j\leq r})^{1/2}$, where $\boldsymbol{v}_i \cdot \boldsymbol{v}_j$ is the standard inner product of the basis vectors $\boldsymbol{v}_i$ and $\boldsymbol{v}_j$. In what follows, we denote $X = \{\boldsymbol{x}_1, \ldots, \boldsymbol{x}_t\} \subset \mathbb{Z}^d$, and let $W = W(X)$ be the $t \times d$ matrix with rows $\boldsymbol{x}_1^T, \ldots, \boldsymbol{x}_t^T$ and let $r = r(X)$ be the column rank of the matrix W. We will denote by $\Lambda(X)$ the r-dimensional sublattice of $\mathbb{Z}^t$ formed by all integer points in the linear subspace $\operatorname{span}_{\mathbb{R}}(W)$ spanned by the columns of W, that is

$$\Lambda(X) = \operatorname{span}_{\mathbb{R}}(W) \cap \mathbb{Z}^t\,. \tag{3}$$

Similar, we let

$$H(X) = \det(\Lambda(X))$$

be the determinant of the lattice $\Lambda(X)$. Note that

$$H(X) = g^{-1}\sqrt{\det(V^T V)}\,, \tag{4}$$

where V is a matrix formed by any r linearly independent columns of W and g is the greatest common divisor of the determinants of all submatrices of V of order r (see [38, Chapter 1, §1] and [39]).

1.1. **Our contributions.**

In this paper, we study two questions:

1. What are the best bounds we can give for $\mathsf{M}_0(X)$ in terms of the generating set X?

   Our first main result is Theorem 1. There, for general X, we obtain two new upper bounds for $\mathsf{M}_0(X)$ that improve upon (2) in two distinct ways.

   Theorem 1. *Let $X \subset \mathbb{Z}^d$ be a finite set of nonzero integer vectors. Then*
   (i) $\mathsf{M}_0(X) \leq r(X) + \lfloor \log(H(X)) \rfloor$, *and*
   (ii) $\mathsf{M}_0(X) \leq \lfloor 2d \log(2\sqrt{d}\|X\|_\infty) \rfloor$.

It should be pointed out here that the bound in Theorem 1 (i) depends only on the rank and $H(X)$, the height of a rational subspace S spanned by $W(X)$ and remains the same for any finite set of nonzero integer vectors X' with $S = \mathrm{span}_{\mathbb{R}}(W(X'))$. Hence the bound in Theorem 1 (i) becomes arbitrarily smaller than the bound (2) provided $\|X\|_\infty$ is sufficiently large.

The second result is Theorem 2 below, which refines Theorem 1 for knapsack problems with positive entries (that is, when $X \subset \mathbb{Z}_{>0}$ is a list of positive integers).

Theorem 2. *Let $X \subset \mathbb{Z}_{>0}$ be a finite set of positive integers. Then*

$$\mathsf{M}_0(X) \leq 1 + \lfloor \log(\|X\|_\infty) \rfloor . \tag{5}$$

Both theorems are proved in Section 2.

2. What is the asymptotic behavior of the univariate function $\mathsf{m}_0(\lambda \boldsymbol{b})$ obtained from successive dilations of the vector $\boldsymbol{b}$?

   We prove the somewhat surprising result that this function of λ is eventually a *periodic* function. The precise statement (Theorem 11) is reminiscent of the behavior of Ehrhart and volume functions of polyhedra; see [6] for more on polyhedral combinatorics. We also present Theorem 12, which is a much sharper result for knapsacks problems. The details of these results are discussed in Section 3.

In order to stress the applicability of our results in discrete optimization, we conclude this introduction with the following immediate corollary of Theorem 1, which gives an interesting bound on the sparsity of optimal solutions in integer and mixed integer linear programs.

Corollary 3. *Fix a matrix $A \in \mathbb{Z}^{d\times t}$ with columns $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_t$ and objective function $\boldsymbol{c} \in \mathbb{Z}^t$. If the integer program*

$$\min\{\boldsymbol{c}^T\boldsymbol{x} : A\boldsymbol{x} = \boldsymbol{b},\ \boldsymbol{x} \geq 0,\ \boldsymbol{x} \in \mathbb{Z}^t\}$$

has a finite optimum, then there exists an optimal solution $\boldsymbol{x}^*$ with at most

$$(d+1) + \lfloor \log(H(X)) \rfloor$$

non-zero components, where X is given by the enlarged column vectors

$$\left\{ \begin{pmatrix} \boldsymbol{a}_1 \\ c_1 \end{pmatrix}, \ldots, \begin{pmatrix} \boldsymbol{a}_1 \\ c_1 \end{pmatrix} \right\}.$$

More generally, if A and B are $d \times t_1$, $d \times t_2$ matrices, and an optimum exists for the mixed integer program

$$\min\{\boldsymbol{c}^T\boldsymbol{x} + \boldsymbol{v}^T\boldsymbol{y} : A\boldsymbol{x} + B\boldsymbol{y} = \boldsymbol{b},\ \boldsymbol{x} \geq 0,\ \boldsymbol{y} \geq 0,\ \boldsymbol{x} \in \mathbb{Z}^{t_1},\ \boldsymbol{y} \in \mathbb{R}^{t_2}\},$$

then there is an optimal solution with at most

$$(d+1) + \lfloor \log(H(X)) \rfloor + \mathrm{rank}(B)$$

non-zero components, where X is as before.

2. Bounds for sparsity in solutions through Siegel's Lemma

The proof of (2), and some of the proofs in [36], make use of equal sub-sums of the set of vectors X to decrease the number of elements needed to represent a given vector $\boldsymbol{b} \in \mathrm{Sg}(X)$. In this section, we use Siegel's Lemma and the geometry of numbers to refine (2). We now review some useful results.

2.1. **An application of Siegel's Lemma.** Given an integer matrix $A \in \mathbb{Z}^{m\times n}$, $m < n$, with m linearly independent rows, the system $A\boldsymbol{y} = \boldsymbol{0}$ has a nontrivial integer solution. If the coefficients are small integers, then there will be a solution in small integers. Thue was the first to use this principle in [40], Siegel was the first to state this idea formally ([37], Bd. I, p. 213, Hilfssatz). Bombieri and Vaaler [7] obtained the following general result.

Theorem 4 (Bombieri and Vaaler, 1983)**.** *Fix an $m \times n$ integer matrix A, $m < n$, with m linearly independent rows. To the system of equations $A\boldsymbol{y} = \boldsymbol{0}$, there are $n - m$ linearly independent integral solutions $\boldsymbol{y}_1, \dots, \boldsymbol{y}_{n-m}$ satisfying*

$$\prod_{l=1}^{n-m} ||\boldsymbol{y}_l||_\infty \le g^{-1}\sqrt{\det(AA^T)}\,, \tag{6}$$

where g is the greatest common divisor of the determinants of all $m \times m$ submatrices of A.

Note that (6) is optimal up to a constant multiple depending only on n and m [41]. Siegel's Lemma plays the key role in the proof of the following result.

Lemma 5. *Let $X \subset \mathbb{Z}^d$ be a finite set of nonzero integer vectors and let $\boldsymbol{b} \in \mathrm{Sg}(X)$. If*

$$|X| > r(X) + \log(H(X)) \tag{7}$$

then there exists a proper subset $Y \subset X$ such that $\boldsymbol{b} \in \mathrm{Sg}(Y)$.

Proof of Lemma 5. We will use Theorem 4. Suppose that

$$|X| = t > r(X) + \log(H(X))\,. \tag{8}$$

We need to show that there exists a proper subset Y of X such that $\boldsymbol{b} \in \mathrm{Sg}(Y)$.

The inequality (8) implies

$$H(X) < 2^{t-r}\,,$$

where $r = r(X)$. Let V be a matrix formed by r linearly independent columns of the matrix $W(X)$. Then $H(X) = g^{-1}\sqrt{\det(V^TV)}$, where g is the greatest common divisor of the determinants of all submatrices of V of order r. Applying Theorem 4 to the matrix V^T, there exists a nonzero vector $\boldsymbol{y} \in \mathbb{Z}^t$ such that

$$V^T\boldsymbol{y} = \boldsymbol{0} \tag{9}$$

and

$$||\boldsymbol{y}||_\infty \le H(X)^{1/(t-r)} < 2\,,$$

so $\boldsymbol{y} = (y_1, \dots, y_t)^T$ has entries $y_i \in \{-1, 0, 1\}$. By (9) we also have $W(X)^T\boldsymbol{y} = \boldsymbol{0}$, so that

$$y_1\boldsymbol{x}_1 + \cdots + y_t\boldsymbol{x}_t = \boldsymbol{0}.$$

We will show that $\boldsymbol{b} = \mu_1\boldsymbol{x}_1 + \cdots + \mu_t\boldsymbol{x}_t$, $\mu_i \in \mathbb{Z}_{\ge 0}$ with $\mu_i = 0$ for at least one i. Indeed, this means there exists a proper subset Y of X such that $\boldsymbol{b} \in \mathrm{Sg}(Y)$.

Suppose that $\boldsymbol{b} = \lambda_1\boldsymbol{x}_1 + \cdots + \lambda_t\boldsymbol{x}_t$, $\lambda_i \in \mathbb{Z}_{>0}$. Writing $\lambda = \min_{i:y_i\neq 0}\lambda_i$ and replacing, if necessary, the vector $\boldsymbol{y}$ by $-\boldsymbol{y}$, we have

$$\boldsymbol{b} = \lambda_1\boldsymbol{x}_1 + \cdots + \lambda_t\boldsymbol{x}_t - \lambda(y_1\boldsymbol{x}_1 + \cdots + y_t\boldsymbol{x}_t) = \sum_{i=1}^{t}(\lambda_i - \lambda y_i)\boldsymbol{x}_i\,,$$

where all coefficients $\mu_i := \lambda_i - \lambda y_i$ are nonnegative and at least one of them is zero, as desired. □

The second ingredient for the proof of Theorem 1 is the following technical result.

Lemma 6. *Let $X \subset \mathbb{Z}^d$ be a finite set of nonzero integer vectors and Y be a subset of X. Then $H(Y) \leq H(X)$.*

Proof of Lemma 6. For $m \in \mathbb{Z}_{\geq 1}$ we denote by $[m]$ the set $\{1, 2, \ldots, m\}$. Given a matrix $V \in \mathbb{Z}^{m\times n}$ and a set $I \subset [m]$ we denote by V_I the matrix with rows $i \in I$ of V.

Assume without loss of generality that Y consists of the first s elements of X. Let $V \in \mathbb{Z}^{t\times r}$ be a matrix with $r = r(X)$ columns that form a basis of the lattice $\Lambda = \Lambda(X) = V\mathbb{Z}^r$. Let Γ denote the projection of Λ onto the first s coordinates, i.e., $\Gamma = V_{[s]}\mathbb{Z}^r$. We have $\mathrm{span}_{\mathbb{R}}(W(Y)) = \mathrm{span}_{\mathbb{R}}(W(X)_{[s]}) = \mathrm{span}_{\mathbb{R}}(V_{[s]})$ and, consequently, $\Gamma \subset \Lambda(Y)$. Thus, $H(Y) \leq \det(\Gamma)$. Since $H(X) = \det(\Lambda)$, it is sufficient to show that

$$\det(\Gamma) \leq \det(\Lambda)\,. \tag{10}$$

We have that

$$\det(\Lambda) = \sqrt{\det(V^T V)} = \sqrt{\sum_{I\subset[t] \text{ s.t. } |I|=r} \det(V_I)^2}$$

(see e.g. [25], Chapter 16, Theorem 18.) Note that by the choice of V, we have $g = 1$ in (4).

We denote $B = V_{[s]}$ and $k = \mathrm{rank}(B)$. Further, let $C = V_{[k]}$ and $D = V_{[s+r-k]\setminus[s]}$. By permutation of the rows of V we may assume without loss of generality that $\mathrm{rank}(B) = \mathrm{rank}(C) = k$ and $\mathrm{rank}((C^T\, D^T)) = r$

Now let $U \in \mathbb{Z}^{r\times r}$ be unimodular such that the matrix $(C^T\, D^T)^T U$ is in the Hermite normal form (see [35, Section 4.1]). In particular $((C^T\, D^T)^T U)_{ij} = 0$ for $i < j$.

Let $V' = VU$, $B' = BU$, $C' = CU$ and $D' = DU$. Observe that $V'\mathbb{Z}^r = VU\mathbb{Z}^r = \Lambda$ and $B'\mathbb{Z}^r = BU\mathbb{Z}^r = \Gamma$ and

$$\sum_{I\subset[t] \text{ s.t. } |I|=r} \det(V_I)^2 = \sum_{I\subset[t] \text{ s.t. } |I|=r} \det(V_I U)^2.$$

In particular $V'_{ij} = 0$ for $i = 1, \ldots, s$ and $j = 1, \ldots, r-k$, other wise $\mathrm{rank}(B) > k$.

Let $\bar{B}$ denote the k non-zero columns of B'. It holds that $\bar{B}\mathbb{Z}^k = \Gamma$. Let $J = \{s+1, \ldots, s+r-k\}$ and let Id_n denote the $n \times n$ identity matrix. Then

$$\begin{aligned}
(\det(\Gamma))^2 &= \textstyle\sum_{I\subset[s] \text{ s.t. } |I|=k} \det(\bar{B}_I)^2 \\
&= \textstyle\sum_{I\subset[s] \text{ s.t. } |I|=k} \det\left(\begin{pmatrix} 0 & \bar{B}_I \\ Id_{r-k} & 0 \end{pmatrix}\right)^2 \\
&\leq \textstyle\sum_{I\subset[s] \text{ s.t. } |I|=k} \det\left(\begin{pmatrix} B'_I \\ D' \end{pmatrix}\right)^2 \\
&= \textstyle\sum_{I\subset[s] \text{ s.t. } |I|=k} \det\left(V'_{I\cup J}\right)^2 \\
&\leq \textstyle\sum_{I\subset[t] \text{ s.t. } |I|=r} \det(V'_I)^2 = (\det(\Lambda))^2.
\end{aligned}$$

Hence (10) holds and the lemma is proved.

□

Now we are ready to prove Theorem 1.

Proof of Theorem 1. It is sufficient to show that

$$\mathsf{M}_0(X) \leq r(X) + \log(H(X))\,. \tag{11}$$

Suppose, to derive a contradiction, that $\mathsf{M}_0(X) > r(X) + \log(H(X))$. Then there exists $\boldsymbol{b} \in \mathrm{Sg}(X)$ such that

$$\mathsf{m}_0(\boldsymbol{b}) > r(X) + \log(H(X)).$$

Let Y be a subset of X such that $\boldsymbol{b} \in \mathrm{Sg}(Y)$ and $\mathsf{m}_0(\boldsymbol{b}) = |Y|$. Observe that $|Y| > r(X) + \log(H(X))$ implies $|Y| > r(Y) + \log(H(Y))$. Indeed, we clearly have $r(Y) \leq r(X)$ and the inequality $\log(H(Y)) \leq \log(H(X))$ follows from Lemma 6. Therefore, by Lemma 5, $\mathsf{m}_0(\boldsymbol{b}) < |Y|$. The obtained contradiction implies (11) and completes the proof of part (i).

Similarly, to prove part (ii) it suffices to show that for any subset Y of X the inequality $|Y| > 2d\log(2\sqrt{d}||X||_\infty)$ implies

$$|Y| > r(Y) + \log(H(Y)).$$

First, observe that

$$r(Y) \leq d \text{ and } H(Y) \leq (\sqrt{|Y|}||X||_\infty)^d. \tag{12}$$

Suppose that $|Y| > 2d\log(2\sqrt{d}||X||_\infty)$, that is,

$$||X||_\infty < \frac{1}{\sqrt{2d}} 2^{\frac{|Y|-d}{2d}}.$$

By (12), we see that

$$\begin{aligned} r(Y) + \log(H(Y)) &\leq d + d\log(\sqrt{|Y|}||X||_\infty) \\ &< d + d\log\left(\sqrt{|Y|}\tfrac{1}{\sqrt{2d}} 2^{\frac{|Y|-d}{2d}}\right) \\ &= \tfrac{|Y|}{2} + \tfrac{d}{2}\log(\tfrac{|Y|}{d}) < |Y|, \end{aligned}$$

which completes the proof of part (ii). □

2.2. **Knapsack case ($d = 1$) and sum-distinct sets.** In this section we prove Theorem 2 and propose a conjecture on the bounds for $\mathsf{M}_0(X)$ in terms of $\|X\|_\infty$ in the knapsack case.

The proof of Theorem 2 will easily follow from the following lemma.

Lemma 7. *Let X be a finite set of positive integers and let $b \in \mathrm{Sg}(X)$. If*

$$|X| > 1 + \log(\|X\|_\infty) \tag{13}$$

then there exists a proper subset $Y \subset X$ such that $b \in \mathrm{Sg}(Y)$.

Proof of Lemma 7 . Let $X = \{x_1, \ldots, x_t\} \subset \mathbb{Z}^t_{>0}$ with $t \geq 2$. Consider the *knapsack polytope*

$$Q_X(b) = \{\boldsymbol{y} \in \mathbb{R}^t_{\geq 0} : W(X)^T \boldsymbol{y} = b\}.$$

The polytope $Q_X(b)$ is a $(t-1)$-dimensional simplex in $\mathbb{R}^t$ with vertices

$$(b/x_1, 0, \ldots, 0)^T, (0, b/x_2, \ldots, 0)^T, \ldots, (0, \ldots, 0, b/x_t)^T.$$

We will show that there exists an integer point point $\boldsymbol{\mu} = (\mu_1, \ldots, \mu_t)^T \in Q_X(b)$ with $\mu_i = 0$ for at least one i. Indeed, this means that there exists a proper subset Y of X such that $b \in \mathrm{Sg}(Y)$.

We will work with the $(t-1)$-dimensional simplex $S_X(b) = \pi_t(Q_X(b)) \subset \mathbb{R}^{t-1}$, where $\pi_t(\cdot) : \mathbb{R}^t \to \mathbb{R}^{t-1}$ is the projection that forgets the last coordinate. Observe that

$$S_X(b) = \left\{\boldsymbol{y} \in \mathbb{R}^{t-1}_{\geq 0} : y_1 x_1 + \cdots + y_{t-1} x_{t-1} \leq b\right\}$$

and, as all $x_i > 0$, the projection map $\pi_t(\cdot)$ establishes a bijection between $Q_X(b)$ and $S_X(b)$.

Let $\boldsymbol{\lambda}$ be any integer point in $Q_X(b)$. Suppose that $\boldsymbol{\lambda} \in \mathbb{Z}^t_{>0}$. Clearly, $\boldsymbol{\beta} = \pi_t(\boldsymbol{\lambda}) \in S_X(b)$. Consider the lattice

$$\Gamma = \{\boldsymbol{y} \in \mathbb{Z}^{t-1} : y_1x_1 + \cdots + y_{t-1}x_{t-1} \equiv 0 (\bmod x_t)\}\,.$$

The lattice Γ has determinant $\det(\Gamma) = x_t/g$, where $g = \gcd(x_1, \ldots, x_t)$ (see e.g. Corollary 3.2.20 in [15]).

By Minkowski's first fundamental theorem (see e.g. [23]), applied to Γ and the cube $[-1, 1]^{t-1}$, there exists a nonzero $\boldsymbol{u} \in \Gamma$ such that

$$\|\boldsymbol{u}\|_\infty \le (\det(\Gamma))^{1/(t-1)} \le x_t^{1/(t-1)}\,. \tag{14}$$

By (13), we have $x_t < 2^{t-1}$. Hence, together with (14), the point $\boldsymbol{u} = (u_1, \ldots, u_{t-1})^T$ has entries $u_i \in \{-1, 0, 1\}$. For some integer z, the point $\boldsymbol{p} = (u_1, \ldots, u_{n-1}, z)^T$ satisfies

$$W(X)^T\boldsymbol{p} = 0\,. \tag{15}$$

Suppose first that all nonzero entries of $\boldsymbol{u}$ are of the same sign. In this case we may assume without loss of generality that all nonzero entries of $\boldsymbol{u}$ are positive. Then for some integer k the point $\boldsymbol{\beta} - k\boldsymbol{u} \in S_X(b)$ will have less than $t-1$ nonzero entries. Therefore, the point $\boldsymbol{\mu} = \boldsymbol{\lambda} - k\boldsymbol{p}$ will have less than t nonzero entries. By construction, $\pi_t(\boldsymbol{\mu}) \in S_X(b)$. On the other hand, by (15), $W(X)^T\boldsymbol{\mu} = b$. This implies $\boldsymbol{\mu} \in Q_X(b)$. Hence this case is settled.

Suppose now that there are entries u_i and u_j with $u_iu_j < 0$. Then for some positive integers k, l the points $\boldsymbol{\beta} - k\boldsymbol{u}, \boldsymbol{\beta} + l\boldsymbol{u} \in \mathbb{Z}^{t-1}_{\ge 0}$ will have each less than $t-1$ nonzero entries. Clearly, at least one of these points is in the simplex $S_X(b)$. If $\boldsymbol{\beta} - k\boldsymbol{u} \in S_X(b)$ then set $\boldsymbol{\mu} = \boldsymbol{\lambda} - k\boldsymbol{p}$. Otherwise, set $\boldsymbol{\mu} = \boldsymbol{\lambda} + l\boldsymbol{p}$. Hence, as in the previous case, the point $\boldsymbol{\mu} \in Q_X(b)$ will have less than t nonzero entries. The lemma is proved.

□

Proof of Theorem 2 . It is sufficient to show that

$$\mathsf{M}_0(X) \le 1 + \log(\|X\|_\infty)\,. \tag{16}$$

Suppose, to derive a contradition, that $\mathsf{M}_0(X) > 1+\log(\|X\|_\infty)$. Then there exists $b \in \mathrm{Sg}(X)$ such that

$$\mathsf{m}_0(b) > 1 + \log(\|X\|_\infty). \tag{17}$$

Let Y be a subset of X such that $b \in \mathrm{Sg}(Y)$ and $\mathsf{m}_0(b) = |Y|$. By (17) we have $|Y| > 1 + \log(\|Y\|_\infty)$. Therefore, by Lemma 7, $\mathsf{m}_0(b) < |Y|$. The obtained contradiction implies (16). □

We now discuss the bounds for $\mathsf{M}_0(X)$ in terms of $\|X\|_\infty$ for the general knapsack problem. A minor improvement on part (ii) of Theorem 1 for $d = 1$ can be obtained by using a version of Siegel's Lemma that works with the maximum norm. Let $A \in \mathbb{Z}^{1\times n}$, $n \ge 2$, be a matrix with nonzero entries. Siegel's Lemma with respect to the maximum norm asks for the smallest possible constant $c_n > 0$ such that the equation $A\boldsymbol{y} = 0$ has a solution $\boldsymbol{y} \in \mathbb{Z}^n$ with

$$0 < ||\boldsymbol{y}||_\infty^{n-1} \le c_n||A||_\infty\,.$$

The only known exact values of c_n are $c_2 = 1$, $c_3 = 4/3$ and $c_4 = 27/19$ (see [34]). The upper bound $c_n \le \sqrt{n}$ immediately follows from Theorem 4. It was shown in [3] that $c_n \le \sigma_n^{-1}$, where σ_n denotes the *sinc* integral

$$\sigma_n = \frac{2}{\pi}\int_0^\infty \left(\frac{\sin x}{x}\right)^n dx\,.$$

Since $\sigma_n^{-1} \sim \sqrt{\frac{\pi n}{6}}$ as $n \to \infty$, the latter bound asymptotically improves the estimate $c_n \leq \sqrt{n}$. The sequences of numerators and denominators of $\sigma_n/2$ can be found in [1] as sequences A049330 and A049331, respectively. Using the bound $c_n \leq \sigma_n^{-1}$, we obtain the following version of Lemma 5 in terms of $\|X\|_\infty$.

Lemma 8. *Let X be a finite set of integers and let $b \in \mathrm{Sg}(X)$. If*

$$|X| > 1 - \log(\sigma_{|X|}) + \log(||X||_\infty)\,. \tag{18}$$

then there exists a proper subset $Y \subset X$ such that $b \in \mathrm{Sg}(Y)$.

Proof of Lemma 8. Writing $t = |X|$, the inequality (18) implies that

$$||X||_\infty < \sigma_t 2^{t-1}.$$

By [3, Theorem 1], there exists a nonzero $\boldsymbol{y} \in \mathbb{Z}^t$ such that $y_1x_1 + \cdots + y_tx_t = 0$ and

$$||\boldsymbol{y}||_\infty \leq \left(\frac{||X||_\infty}{\sigma_t}\right)^{\frac{1}{t-1}} < 2\,. \tag{19}$$

As in the proof of Lemma 5 we now observe that $\boldsymbol{y} = (y_1, \ldots, y_t)^T$ has entries $y_i \in \{-1, 0, 1\}$, yielding the proper subset Y of X. □

Lemma 8 can be used to obtain a minor asymptotic improvement on part (ii) of Theorem 1 for $d = 1$.

It was observed by Schinzel (personal communication) that Siegel's Lemma is closely related to the following well known problem from additive number theory. A finite set $X = \{x_1, \ldots, x_t\} \subset \mathbb{Z}$ of integers is called *sum–distinct* if any two of its 2^t subsums differ by at least 1. We shall assume w.l.o.g. that $0 < x_1 < x_2 < \cdots < x_t$. In 1955, Erdős and Moser ([18], Problem 6) asked for an estimate on the least possible x_t of such a set, and Erdős conjectured that $x_t > c_0 2^t$ for some absolute constant $c_0 > 0$. It follows from [3, Theorem 1] that a sum-distinct set $X = \{x_1, \ldots, x_t\}$ satisfies $||X||_\infty > \sigma_t 2^{t-1}$ (cf. (19).) An unpublished result by Elkies and Gleason asymptotically improves this bound by a factor of $2/\sqrt{3}$.

Observe that the set X is not sum-distinct if and only if there exist $y_i \in \{-1, 0, 1\}$, not all zero, such that $y_1x_1 + \cdots + y_tx_t = 0$. Hence, an affirmative answer to Erdős-Moser conjecture would imply that (18) can be replaced by the inequality

$$|X| \geq -\log(c_0) + \log(||X||_\infty)\,.$$

Lemma 7 allows us to make such a replacement for sets of positive integers. Based on this, we conjecture that for $d = 1$ there exists a positive integer c such that

$$\mathsf{M}_0(X) \leq c + \lfloor \log(||X||_\infty)) \rfloor\,.$$

As a final remark for Section 2 we wish to discuss how tight are the bounds we have presented. The bound in part (i) of Theorem 1 is in fact attained for certain sets of generators in the cases $d = 2$ and $d = 3$. To see this, following [16], we consider the sets $X \subset \mathbb{Z}^d$ defined for $n \geq 2$ as

$$X = \{\boldsymbol{x}_{ij} : \boldsymbol{x}_{ij} = 2^i \boldsymbol{e}_j + \boldsymbol{e}_d\,, i = 0, \ldots, n-1\,, j = 1, \ldots, d-1\}\,,$$

where $\boldsymbol{e}_j$ is the jth standard basis vector.

For $\boldsymbol{b} = (2^n - 1)\sum_{j=1}^{d-1} \boldsymbol{e}_j + n(d-1)\boldsymbol{e}_d$ we clearly have $\mathsf{m}_0(\boldsymbol{b}) = n(d-1)$ and, consequently, $\mathsf{M}_0(X) = n(d-1)$. This value coincides with the upper bound (i) of Theorem 1 for $d = 2$ with $n = 2, 3$ and for $d = 3$ with $n = 2$.

3. Periodicity of the function m_0

In polyhedral combinatorics and combinatorial optimization it is well-known that there are interesting properties of dilation of polyhedra. For instance, the reader may be familiar with functions that behave well under dilation, such as the volume and the number of lattice points; their behaviour is captured by Ehrhart's Theorem (see [6] for an introduction). In this section we explain the asymptotic behavior of the norm-based function $\mathsf{m}_0(\mathbf{b})$, both in the most general setting (Theorem 11) and for knapsack problems (Theorem 12). We prove in particular that $\mathsf{m}_0 : \mathrm{Sg}(X) \to \mathbb{Z}_{\geq 0}$ is eventually periodic. Let us consider a motivating example, a simple knapsack problem.

Example 9. Let $X = \{4, 6, 15\} \subset \mathbb{Z}$, and let $S = \mathrm{Sg}(X)$. Depicted in Figure 1 are the polytopes $Q_X(25)$ and $Q_X(85)$. There is a single integer solution in $\mathsf{P}_X(85)$ that lies on a coordinate plane, namely $(10, 0, 3)^T$, so $\mathsf{m}_0(85) = 2$. On the other hand, the only integer solution in $\mathsf{P}_X(25)$ is $(1, 1, 1)^T$, so $\mathsf{m}_0(25) = 3$.

Notice that $85 - 25 = 60 = \mathrm{lcm}(X)$, so any integer solution in $\mathsf{P}_X(25)$ produces a solution in $\mathsf{P}_X(85)$ by sufficiently increasing any single component. Geometrically, the drop in 0-norm value occurs because the point $(10, 0, 3)^T \in \mathsf{P}_X(85)$ cannot be obtained in this way from a solution in $\mathsf{P}_X(25)$.

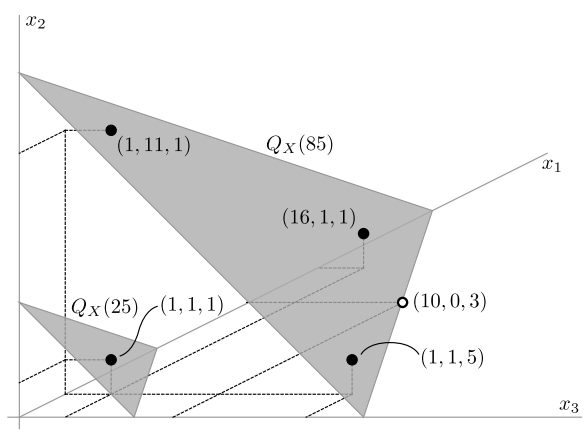

Figure 1. Polytopes $Q_X(25)$ and $Q_X(85)$, with $X = \{4, 6, 15\}$ as in Example 9.

Recall that a function $f : \mathbb{Z}_{\geq 0} \to \mathbb{Q}$ is a *quasipolynomial of degree k* if there exist periodic functions $a_0, \ldots, a_k : \mathbb{Z}_{\geq 0} \to \mathbb{Q}$ such that

$$f(b) = a_k(b)b^k + \cdots + a_1(b)b + a_0(b)$$

and a_k is not identically zero. The *period of f* is the minimal positive integer π such that $a_i(b + \pi) = a_i(b)$ for all $i \leq k$ and $b \in \mathbb{Z}_{\geq 0}$. The statement of Theorem 11 requires an appropriate multivariate analog.

Definition 10. Fix $f : \mathbb{Z}^d_{\geq 0} \to \mathbb{R}$, linearly independent $\mathbf{x}_1, \ldots, \mathbf{x}_t \in \mathbb{Z}^d_{\geq 0}$, and $\mathbf{b} \in \mathbb{Z}^d_{\geq 0}$.

(a) The *cone generated by* $\mathbf{x}_1, \ldots, \mathbf{x}_t$ *translated by* $\mathbf{b}$ is the set

$$C = C(\mathbf{b}; \mathbf{x}_1, \ldots, \mathbf{x}_t) = \mathbf{b} + \mathrm{Sg}(\{\mathbf{x}_1, \ldots, \mathbf{x}_t\}) \subset \mathbb{Z}^d_{\geq 0}.$$

(b) The function f is a *simple quasipolynomial supported on the cone* C if (i) f vanishes outside of C and (ii) f coincides with a polynomial when restricted to C. The *degree of* f is the degree of the restriction of f to C.
(c) The function f is *eventually quasipolynomial* if it is a finite sum of simple quasipolynomials. The *degree* of f is the minimal integer k such that f can be written as a sum of simple quasipolynomials of degree at most k.

We are now ready to state the main result for this section (Theorem 11).

Theorem 11. *For any finite set of non-negative integer vectors* $X \subset \mathbb{Z}^d$, $\mathsf{m}_0 : \mathrm{Sg}(X) \to \mathbb{Z}_{\geq 0}$ *is eventually quasiconstant, i.e. a quasipolynomial of degree* 0.

Focusing our attention on the case of knapsack problems (that is, when $X \subset \mathbb{Z}_{>0}$), Theorem 11 implies that the function $\mathsf{m}_0(b)$ is eventually periodic. Our next main result, Theorem 12, gives a more direct proof of this fact; in doing so, a bound on the starting point of this periodic behavior and a precise value for the minimal period are achieved.

In what follows, for $X' \subset \mathbb{Z}_{>0}$, let

$$F(X') = \max(\mathrm{Sg}(\gcd(X')) \setminus \mathrm{Sg}(X')),$$

which coincides with the *Frobenius number* (see e.g. [32]) when $\gcd(X') = 1$.

Theorem 12. *Fix a set* X *of positive integers, let* $L = \mathrm{lcm}(X)$, *and let*

$$N_0 = \max\{F(X') : X' \subset X\}.$$

Each $b > N_0$ *satisfies*

$$\mathsf{m}_0(b + L) = \mathsf{m}_0(b).$$

Moreover, $\mathrm{lcm}(X)$ *is the minimal value of* L *for which the above statement holds.*

Example 13. Resuming notation from Example 9, Figure 2 depicts values of the function $\mathsf{m}_0 : \mathrm{Sg}(X) \to \mathbb{Z}_{\geq 0}$. The periodic behavior ensured by Theorems 11 and 12 is evident, as we can see that $\mathsf{m}_0(b + 60) = \mathsf{m}_0(b)$ for each $b \geq 42$.

Algebraically, this occur because $L = 60$ lies in every subsemigroup of $\mathrm{Sg}(X)$ generated by a proper subset of X, so adding L to any element of $\mathrm{Sg}(X)$ preserves membership in all such subsemigroups. We must require b be sufficiently large to ensure $b+60$ is not contained in any additional subsemigroups not already containing b (Figure 1 depicts this phenomenon for $b = 25$).

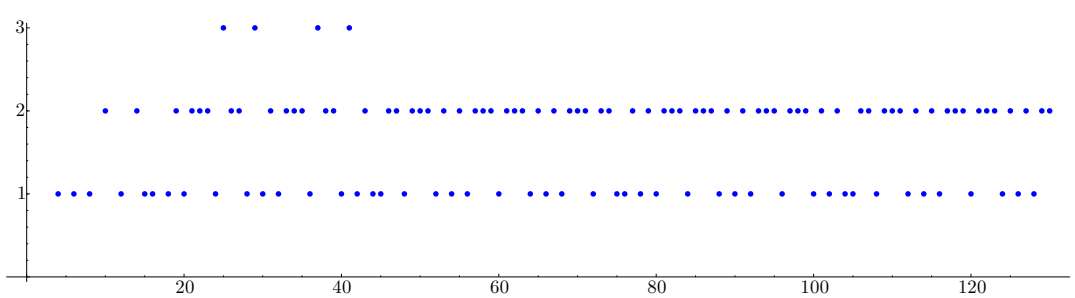

FIGURE 2. Plot of $\mathsf{m}_0 : \mathrm{Sg}(X) \to \mathbb{Z}_{\geq 0}$ for $X = \{4, 6, 15\}$ in Example 9.

Our study of the asymptotic behavior of $\mathsf{m}_0(\mathbf{b})$ was inspired by [30, Theorem 5.2], a result that appeared in [5] for knapsack problems, stating that the value of the maximal ℓ_1-norm is eventually quasilinear (Definition 10). In future work we will discuss the situation for other norms. The proof of Theorem 11, presented later in this section, uses generating functions and Hilbert's Theorem (Theorems 15 and 16).

3.1. **Proof of Theorems 11 and 12 through Commutative Algebra.** The following theorem, a consequence of the Hilbert Basis Theorem, characterizes the eventual behavior of Hilbert functions of certain $\mathbb{Z}_{\geq 0}$-graded modules. For more background on Hilbert functions and graded modules, see [28, 33].

Definition 14. Fix a field $\Bbbk$ (if the reader prefer, he/she can assume $\Bbbk = F_2$, but what follows works in full generality), let $R = \Bbbk[z_1, \ldots, z_t]$, and fix an R-module M. A $\mathbb{Z}^d_{\geq 0}$*-grading of* R is a function $\deg : \mathbb{Z}^t_{\geq 0} \to \mathbb{Z}^d_{\geq 0}$ satisfying

$$\deg(\mathbf{y} + \mathbf{y}') = \deg(\mathbf{y}) + \deg(\mathbf{y}')$$

for all $\mathbf{y}, \mathbf{y}' \in \mathbb{Z}^t_{\geq 0}$. Here, $\deg(z_1^{y_1} \cdots z_t^{y_t}) = \deg(\mathbf{y})$ represents the degree of the monomial $z_1^{y_1} \cdots z_t^{y_t}$ for $\mathbf{y} \in \mathbb{Z}^t_{\geq 0}$. Let $R_{\mathbf{b}}$ denote the $\Bbbk$-vector subspace of R spanned by those $\mathbf{y} \in \mathbb{Z}^t_{\geq 0}$ satisfying $\deg \mathbf{y} = \mathbf{b}$. An $\mathbb{Z}^d_{\geq 0}$*-grading of* M is an expression

$$M \cong \bigoplus_{\mathbf{b} \in \mathbb{Z}^d_{\geq 0}} M_{\mathbf{b}}$$

of M as a direct sum of finite dimensional $\Bbbk$-subspaces of M with $R_{\mathbf{b}} M_{\mathbf{b}'} \subset M_{\mathbf{b}+\mathbf{b}'}$ for all $\mathbf{b}, \mathbf{b}' \in \mathbb{Z}^d_{\geq 0}$. The *Hilbert function of* M is the function $\mathcal{H}(M; -) : \mathbb{Z}^d_{\geq 0} \to \mathbb{Z}_{\geq 0}$ given by

$$\mathcal{H}(M; \mathbf{b}) = \dim_{\Bbbk} M_{\mathbf{b}}$$

for each $\mathbf{b} \in \mathbb{Z}^d_{\geq 0}$.

Theorem 15 ([33, Theorem I.2.3])**.** *Fix a $\mathbb{Z}_{\geq 0}$-graded polynomial ring R, and a finitely generated $\mathbb{Z}_{\geq 0}$-graded R-module M of Krull dimension d. The Hilbert function of M eventually equals a quasipolynomial of degree $d-1$ (called the* Hilbert quasipolynomial of M*). More specifically, there exist periodic functions $a_0, \ldots, a_{d-1} : \mathbb{Z}_{\geq 0} \to \mathbb{Q}$ such that $a_{d-1} \not\equiv 0$ and*

$$\mathcal{H}(M; b) = a_{d-1}(b) b^{d-1} + \cdots + a_1(b) b + a_0(b)$$

for sufficiently large b. Additionally, if $y_1, \ldots, y_d \in R$ is a homogeneous system of parameters for M, then the period of each a_i divides $\operatorname{lcm}(\deg(y_1), \ldots, \deg(y_d))$.

The proof of Theorem 11 uses a generalization of Theorem 15 to multigradings.

Theorem 16 ([30, Theorem 2.10])**.** *Fix a $\mathbb{Z}^d_{\geq 0}$-graded polynomial ring R, and a finitely generated $\mathbb{Z}^d_{\geq 0}$-graded R-module M. The Hilbert function of M is eventually quasipolynomial.*

We are now ready to prove Theorems 11 and 12.

Proof of Theorem 11. We will use Theorem 16. Multigrade the polynomial ring $\Bbbk[z_1, \ldots, z_t]$ by $\deg(z_i) = \mathbf{x}_i$ for $i \leq t$. The ideals

$$I_j = \left\langle \textstyle\prod_{i \in T} z_i : T \subset \{1, \ldots, t\}, |T| = j \right\rangle \subset \Bbbk[z_1, \ldots, z_t]$$

for $j \leq t$ and $I_{t+1} = 0$ form a descending chain

$$I_1 \supset I_2 \supset \cdots \supset I_t \supset I_{t+1} = 0$$

with the property that for $j \leq t$, $\mathcal{H}(I_j/I_{j+1}; \mathbf{b}) > 0$ if and only if $\mathbf{b} \in \mathrm{Sg}(X)$ has a solution $\mathbf{y} \in \mathsf{P}_X(\mathbf{b})$ with $\|\mathbf{y}\|_0 = j$. Indeed, each I_j is determined by the monomials it contains, and a solution $\mathbf{y} \in \mathsf{P}_X(\mathbf{b})$ satisfies $\|\mathbf{y}\|_0 = j$ if and only if $z_1^{y_1} \cdots z_t^{y_t} \in I_j \setminus I_{j+1}$.

Applying Theorem 16 to the quotient I_j/I_{j+1} proves that the characteristic function

$$\chi_j(\mathbf{b}) = \begin{cases} 1 & \text{if } \|\mathbf{y}\|_0 = j \text{ for some } \mathbf{y} \in \mathsf{P}_X(\mathbf{b}) \\ 0 & \text{otherwise} \end{cases}$$

is eventually quasiconstant for each $j \leq t$, and thus

$$\mathsf{m}_0(\mathbf{b}) = \max\{(t-j)\chi_j(\mathbf{b}) : j \leq t\}$$

is eventually quasiconstant as well. □

Proof of Theorem 12. First, fix $\mathbf{y} \in \mathsf{P}_X(b)$. Since $b > 0$, we have $y_j > 0$ for some $j \leq t$. Since $x_j \mid L$, the solution $\mathbf{y} + (L/x_j)\mathbf{e}_j \in \mathsf{P}_X(b+L)$ has support $\mathrm{supp}(\mathbf{y})$. This proves $\mathsf{m}_0(b+L) \leq \mathsf{m}_0(b)$. Next, fix $\mathbf{y} \in \mathsf{P}_X(b+L)$ with $|\mathrm{supp}(\mathbf{y})|$ minimal, and let $S' = \mathrm{Sg}(\mathrm{supp}(\mathbf{y}))$. Since $b > F(S')$, we have $b \in S'$ and thus $\mathsf{m}_0(b) \leq |\mathrm{supp}(\mathbf{y})|$. We conclude $\mathsf{m}_0(b+L) = \mathsf{m}_0(b)$.

For the final claim, consider the characteristic function χ_T of the set $T = \bigcup_{i \leq t} \mathrm{Sg}(x_i)$. Notice that $\chi_T(b)$ is nonzero precisely when $\mathsf{m}_0(b) = 1$. The result follows from the fact that χ_T has minimal period $\mathrm{lcm}(X)$. □

Remark 17. Notice that simply proving "$\supseteq$" in Theorem 12 is sufficient to prove eventual periodicity of m_0 if a precise lower bound on the start of periodicity is not desired. Indeed, it follows that for each $j < L$, the sequence $\{\mathsf{m}_0(kL+j)\}_{k \geq 1}$ is (eventually) a non-increasing sequence of positive integers, and thus eventually constant.

We conclude this section by considering the following problem: "Give a bound on $\mathsf{m}_0(b)$ that holds for all but finitely many $b \in \mathrm{Sg}(X)$." Proposition 18 gives an optimal answer in the knapsack setting.

Proposition 18. *If m is the minimal size of a relatively prime subset of $X \subset \mathbb{Z}_{\geq 0}$, then $\mathsf{m}_0(b) \leq m$ for all but finitely many $b \in \mathrm{Sg}(X)$. More specifically, let $X_1, \ldots, X_r$ denote the relatively prime subsets of X with cardinality m, and let*

$$N_0 = \max\left(\bigcap_{i=1}^r \mathbb{Z}_{\geq 0} \setminus \mathrm{Sg}(X_i)\right).$$

Then $\mathsf{m}_0(b) \leq m$ for all $b > N_0$, and $\mathsf{m}_0(b) = m$ for infinitely many $b > N_0$ (that is to say, the eventual bound m is sharp).

Proof. Every $b > N_0$ lies in $\langle X_i \rangle$ for some $i \leq r$, so $\mathsf{m}_0(b) \leq |X_i| = m$. By the minimality of m, we have $\mathrm{Sg}(X') \subset \mathrm{Sg}(\gcd(X')) \subsetneq \mathbb{Z}_{\geq 0}$ for any subset $X' \subset X$ with $|X'| < m$. In particular, the set

$$\mathrm{Sg}(X) \setminus \bigcup_{|X'|<m} \mathrm{Sg}(X')$$

has infinite cardinality, and is precisely the set of elements $b \in \mathrm{Sg}(X)$ with $\mathsf{m}_0(b) \geq m$. The second claim now follows from the first. □

Example 19. Return to $X = \{4, 6, 15\}$ as in Example 9. Proposition 18 ensures $\mathsf{m}(b) \leq 2$ for all $b \geq 42$, even though $M_0(X) = 3$ is achieved at four distinct values prior to $b = 42$. Algebraically, this is because $\gcd(4, 15) = 1$, so every $b \geq 42$ lies in $\mathrm{Sg}(4, 15)$ and thus satisfies $\mathsf{m}_0(b) \leq 2$. However, $\mathsf{m}_0(25) = 3$, since $(1, 1, 1)^T$ is the only solution in $\mathsf{P}_X(25)$.

Acknowledgements. The second author acknowledges support from NSF dms-grant 1522158. We are grateful to Lenny Fushansky, Martin Henk, Frédéric Meunier, and Daniele Micciancio for their very useful comments and references. We would also like to thank the referees for their valuable suggestions.

References

[1] The on-line encyclopedia of integer sequences, http://oeis.org.

[2] M. Ajtai, *The shortest vector problem in l_2 is NP-hard for randomized reductions*, Proceedings of the 30-th annual ACM symposium of the theory of computing 1998, 10–19.

[3] I. Aliev, *Siegel's lemma and sum-distinct sets*, Discrete and Comput. Geom. **39** (2008), 59–66.

[4] N. Alon, R. Panigrahy, and S. Yekhanin, *Deterministic approximation algorithms for the nearest codeword problem* Approximation, Randomization, and Combinatorial Optimization. Algorithms and Techniques, Vol. 5687, Lecture Notes in Computer Science pp 339-351, Proceedings of 12th International Workshop, APPROX 2009, and 13th International Workshop, RANDOM 2009, Berkeley, CA, USA, August 21-23, 2009.

[5] T. Barron, C. O'Neill and R. Pelayo, *On the set of elasticities in numerical monoids*, Semigroup Forum, to appear. Available at arXiv: math.CO/1409.3425.

[6] A. I. Barvinok and J. Pommersheim, *An algorithmic theory of lattice points in polyhedra*, New Perspectives in Algebraic Combinatorics (Berkeley, CA, 1996-1997), 91–147, Math. Sci. Res. Inst. Publ. 38, Cambridge Univ. Press, Cambridge, 1999.

[7] E. Bombieri and J. Vaaler, *On Siegel's lemma*, Invent. math. **73** (1983), 11–32.

[8] A. Bruckstein, D. Donoho and M. Elad, *From sparse solutions of systems of equations to sparse modeling of signals and images*, SIAM Rev. **51** (2009), no. 1, 34–81.

[9] W. Bruns, J. Gubeladze, M. Henk, A. Martin, and R. Weismantel, *A counterexample to an integer analogue of Carathéodory's theorem.* J. Reine Angew. Math. 510 (1999), 179?185.

[10] E. Candes, J. K. Romberg and T. Tao, *Stable signal recovery from incomplete and inaccurate measurements*, Comm. Pure Appl. Math., **59** (2006), 1207–1223.

[11] E. Candes and T. Tao, *Decoding by linear programming*, IEEE Trans. Inform. Theory 51 (2005), no. 12, 4203–4215.

[12] J. J. Cho, Y. Chen, Y. Ding, *On the (co)girth of a connected matroid*, Discrete Applied Mathematics, Vol. 155, 18, 1 (2007), 2456–2470.

[13] W. Cook, J. Fonlupt and A. Schrijver, *An integer analogue of Carathéodory's theorem*, J. Comb. Theory B **40** (1986), 63–70.

[14] M. Delgado, P. García-Sánchez and J. Morais, *NumericalSgps, A package for numerical semigroups*, Version 0.980 dev (2013), (GAP package), `http://www.fc.up.pt/cmup/mdelgado/numericalsgps/`

[15] C. Dwork, *Lattices and their applications to cryptography*, Lecture Notes, Stanford University, 1998.

[16] F. Eisenbrand and G. Shmonin, *Carathéodory bounds for integer cones*, Oper. Res. Lett. **34** (2006), 564–568.

[17] N. D. Elkies, *An improved lower bound on the greatest element of a sum-distinct set of fixed order*, J. Comb. Theory A **41** (1986), no. 1, 89–94.

[18] P. Erdős, *Problems and results in additive number theory*, Colloque sur la Théorie des Nombres, Bruxelles, 1955, 127–137.

[19] B. Fields, *Length functions determined by killing powers of several ideals in a local ring*, Thesis (Ph.D.)-University of Michigan. 2000. 55 pp.

[20] J. García-García, M. Moreno-Frías and A. Vigneron-Tenorio, *Computation of delta sets of numerical monoids*, Montash. Math. **178** (2015), 457–472.

[21] P. García-Sánchez and J. Rosales, *Numerical semigroups*, vol. 20, Developments in Mathematics, Springer-Verlag, 2009.

[22] P.C. Gilmore and R.E. Gomory, *A linear programming approach to the cutting-stock problem*, Operations Res. **9** (1961), 849–859.

[23] P. M. Gruber and C. G. Lekkerkerker, *Geometry of numbers*, North–Holland, Amsterdam, 1987.

[24] N. Karmarkar and R. Karp, *An efficient approximation scheme for the one-dimensional bin-packing problem*, 23rd annual symposium on foundations of computer science (Chicago, Ill., 1982), 312–320, IEEE, New York, 1982.

[25] S. Mac Lane, G. Birkhoff, *Algebra*, Third edition. Chelsea Publishing Co., New York, 1988.

[26] D. Micciancio, *Locally dense codes* IEEE 29th Conference on Computational Complexity–CC 2014, 90–97, IEEE Computer Soc., Los Alamitos, CA, 2014.
[27] D. Micciancio, *Inapproximability of the shortest vector problem: toward a deterministic reduction*, Theory Comput. **8** (2012), 487–512.
[28] E. Miller and B. Sturmfels, *Combinatorial commutative algebra*, Graduate Texts in Mathematics, vol. 227, Springer-Verlag, New York, 2005.
[29] B.K. Natarajan, *Sparse approximate solutions to linear systems*, SIAM J. Comput., 24 (1995), pp. 227–234.
[30] C. O'Neill, *On factorization invariants and Hilbert functions*, preprint. Available at arXiv: math.AC/1503.08351.
[31] C. O'Neill and R. Pelayo, *On the linearity of ω-primality in numerical monoids*, J. Pure and Applied Algebra **218** (2014) 1620–1627.
[32] J. L. Ramírez Alfonsín, *The Diophantine Frobenius problem*, Oxford Lecture Series in Mathematics and Its Applications, Oxford University Press, New York, 2006.
[33] R. Stanley, *Combinatorics and commutative algebra, second edition*, Progress in Mathematics, 41. Birkhäuser Boston, Inc., Boston, MA, 1996. x+164 pp. ISBN: 0-8176-3836-9
[34] A. Schinzel, *A Property of polynomials with an application to Siegel's lemma*, Monatsh. Math. **137** (2002), 239–251.
[35] A. Schrijver, *Theory of linear and integer programming*, Wiley, Chichester, 1986.
[36] A. Sebő, *Hilbert bases, Carathéodory's theorem and combinatorial optimization*, Proceedings of the 1st International Conference in Integer Programming and Combinatorial Optimization, Waterloo, ON, Canada, 1990, 431–456.
[37] C. L. Siegel, *Über Einige Anwendungen Diophantischer Approximationen*, Abh. der Preus. Akad. der Wissenschaften. Phys.–math. Kl. 1929, Nr. 1 (=*Ges. Abh.*, I, 209–266)
[38] T. Skolem, *Diophantische Gleichungen. Ergebnisse der Mathematik*, Vol 5. Berlin: Springer 1938.
[39] H. J. S. Smith, *On systems of linear indeterminate equations and congruences*, Phil. Trans. Roy. Soc. London **151** (1861), 293 – 326 (=Coll. Math. Papers, I, 367–409)
[40] A. Thue, *Über Annäherungswerte Algebraischer Zahlen*, J. reine angew. Math. **135**(1909), 284–305.
[41] J. Vaaler, *The best constant in Siegel lemma*, Monatsh. Math. **140** (2003), 71–89.
[42] P. van Emde Boas, *Another NP-complete problem and the complexity of computing short vectors in a lattice*, Technical Report 81–04, Matematische Instituut, University of Amsterdam, 1981.
[43] A. Vardy, *The intractability of computing the minimum distance of a code*, IEEE Trans. Information Theory 43(6): 1757-1766 (1997)
[44] J. von zur Gathen and J. Gerhard, *Modern computer algebra*, Cambridge Univ. Press, Cambridge, 1999.

Cardiff University, UK
E-mail address: `alievi@cardiff.ac.uk`

University of California, Davis, USA
E-mail address: `deloera@math.ucdavis.edu`

Cardiff University, UK
E-mail address: `oertelt@cardiff.ac.uk`

University of California, Davis, USA
E-mail address: `coneill@math.ucdavis.edu`