Optimization Letters
https://doi.org/10.1007/s11590-022-01927-0

ORIGINAL PAPER

On unique recovery of finite-valued integer signals and admissible lattices of sparse hypercubes

Abdullah Alasmari[1] · **Iskander Aliev**[1]

Received: 16 March 2022 / Accepted: 20 August 2022

Abstract
The paper considers the problem of unique recovery of sparse finite-valued integer signals using a single linear integer measurement. For l-sparse signals in $\mathbb{Z}^n$, $2l < n$, with absolute entries bounded by r, we construct an $1 \times n$ measurement matrix with maximum absolute entry $\Delta = O(r^{2l-1})$. Here the implicit constant depends on l and n and the exponent $2l - 1$ is optimal. Additionally, we show that, in the above setting, a single measurement can be replaced by several measurements with absolute entries sub-linear in Δ. The proofs make use of results on admissible $(n-1)$-dimensional integer lattices for m-sparse n-cubes that are of independent interest.

Keywords Sparse recovery · Finite-valued signals · Admissible lattices · Sparse hypercubes

1 Unique recovery of sparse bounded integer signals

Fix a set $S \subset \mathbb{Z}^n$ which will be referred to as a *signal space*. We will consider the problem of unique recovery of a signal $\boldsymbol{x}_0 \in S$ from a relatively small number of noisy linear integer measurements, in the form introduced by Fukshansky et al. [9]. Specifically, given a number of measurements m with $m < n$, we aim to construct an integer *measurement matrix* $A \in \mathbb{Z}^{m \times n}$ such that any signal $\boldsymbol{x}_0 \in S$ can be uniquely recovered from m measurements represented by the vector $\boldsymbol{b} \in \mathbb{R}^m$ of the form

$$\boldsymbol{b} = A\boldsymbol{x}_0 + \boldsymbol{e}$$

with an unknown *noise vector* $\boldsymbol{e} \in \mathbb{R}^m$. To allow unique recovery we assume that

✉ Iskander Aliev
alievi@cardiff.ac.uk

Abdullah Alasmari
alasmariaa@cardiff.ac.uk

[1] Mathematics Institute, Cardiff University, Cardiff, Wales, UK

Published online: 13 September 2022

$$\|\boldsymbol{e}\|_2 < c\,,$$

where $\|\cdot\|_2$ denotes the ℓ_2-norm and c is a suitably chosen constant.

Based on [9], we will use the following recovery approach. For a set $Q \subset \mathbb{Z}^n$ we denote by $\mathcal{R}(Q)$ the set of all matrices $A \in \mathbb{Z}^{k\times n}$ with $k < n$, such that

$$\|A\boldsymbol{y}\|_2 \geq 1 \text{ for any nonzero } \boldsymbol{y} \in Q\,. \tag{1}$$

Recall that the *difference set* $D(X)$ of a set $X \in \mathbb{R}^n$ consists of all points $\boldsymbol{x} - \boldsymbol{y}$ with $\boldsymbol{x}, \boldsymbol{y} \in X$. We set $c = 1/2$ and consider $m \times n$ measurement matrices $A \in \mathcal{R}(Q)$ with $Q = D(S)$. In this case, for any $\boldsymbol{e} \in \mathbb{R}^m$ with $\|\boldsymbol{e}\|_2 < c = 1/2$, the signal $\boldsymbol{x}_0$ is the unique point of S satisfying the bound

$$\|A\boldsymbol{x} - \boldsymbol{b}\|_2 \leq \frac{1}{2}\,. \tag{2}$$

Indeed, for any $\boldsymbol{x} \in S$, $\boldsymbol{x} \neq \boldsymbol{x}_0$, satisfying (2), we would have

$$\begin{aligned}\|A(\boldsymbol{x} - \boldsymbol{x}_0)\|_2 &= \|A\boldsymbol{x} - \boldsymbol{b} - (A\boldsymbol{x}_0 - \boldsymbol{b})\|_2\\ &= \|A\boldsymbol{x} - \boldsymbol{b} + \boldsymbol{e}\|_2\\ &\leq \|A\boldsymbol{x} - \boldsymbol{b}\|_2 + \|\boldsymbol{e}\|_2 < 1\,,\end{aligned}$$

contradicting (1). Therefore, $\boldsymbol{x}_0$ can be recovered by any algorithm that, given input $\boldsymbol{b} \in \mathbb{R}^m$ computes a vector $\boldsymbol{x} \in S$ satisfying (2).

We will now introduce some basic notation needed for stating our results. Given $\boldsymbol{x} = (x_1, \ldots, x_n)^T \in \mathbb{R}^n$, we will denote by $\|\boldsymbol{x}\|_0 = |\{i : x_i \neq 0\}|$ the 0-"norm", widely used in the theory of *compressed sensing* [5, 6], which counts the cardinality of the support of $\boldsymbol{x}$. A vector $\boldsymbol{x} \in \mathbb{R}^n$ is called *l-sparse* if $\|\boldsymbol{x}\|_0 \leq l$. By $\mathbb{Z}_l^n$ we denote the set of l-sparse n-dimensional integer vectors:

$$\mathbb{Z}_l^n = \{z \in \mathbb{Z}^n : \|z\|_0 \leq l\}\,.$$

Given positive integers n, r, we denote by $C^n(r)$ the n-dimensional cube defined as $C^n(r) = \{\boldsymbol{x} \in \mathbb{R}^n : \|\boldsymbol{x}\|_\infty \leq r\}$, where $\|\cdot\|_\infty$ stands for the ℓ_∞-norm.

We will be interested in unique recovery of l-sparse signals with entries from a finite integer alphabet $[-r, r] \cap \mathbb{Z}$. Specifically, we will work with the signal space

$$S_l^n(r) = C^n(r) \cap \mathbb{Z}_l^n\,,$$

where $2l < n$.

The signal space $S_l^n(r)$ is finite and hence allows using a single measurement for unique recovery of its signals. From the computational and error-correcting perspectives (see [9] for more details), the measurement should have as small as possible absolute integer entries. Hence, given $l, n \in \mathbb{Z}$ with $1 \leq l < n/2$, $r \in \mathbb{Z}_{>0}$ and letting $Q = D(S_l^n(r))$, we face the optimisation problem

$$\min\{\|H\|_\infty : H \in \mathbb{Z}^{1\times n},\ H \in \mathcal{R}(Q)\}\,. \tag{3}$$

In this paper, we will obtain general estimates for the minimum in (3). Using condition (1), to get an upper bound for (3), it is sufficient to find an $1 \times n$ measurement matrix H such that its kernel space does not share any nonzero integer points with the convex hull of $D(S_l^n(r))$. This straightforward approach, however, results in the estimate

$$\|H\|_\infty = O(r^{n-1}), \tag{4}$$

where the implicit constant depends on l and n.

The first result of this paper shows that the exponent $n-1$ in (4) can be replaced with $2l-1$. Let

$$p_{m,n}(r) = (m\Delta(m,n)r+1)^{m-1} + \Delta(m,n)\sum_{i=0}^{m-2}(m\Delta(m,n)r+1)^i,$$

where $\Delta(m,n) = \min(n-1, \lceil (2n)^{(m-1)/m} \rceil)$.

Theorem 1 *For any $l, n \in \mathbb{Z}$ with $1 \le l < n/2$ and $r \in \mathbb{Z}_{>0}$ there exists an $1 \times n$ integer matrix H such that $H \in \mathcal{R}(Q)$ with $Q = D(S_l^n(r))$ and*

$$\|H\|_\infty \le p_{2l,n}(2r). \tag{5}$$

The proof of Theorem 1 is constructive. To obtain the bound (5) we combine known results on unique recovery over $\mathbb{Z}_l^n$, outlined in Sect. 2, with aggregation techniques, outlined in Sect. 4.

The second result gives a lower bound for the minimum in (3). Notably, it shows that the polynomial $p_{2l,n}(2r)$ in (5) cannot be replaced by a polynomial in r with degree smaller than $2l-1$.

Theorem 2 *For any $l, n \in \mathbb{Z}$ with $1 \le l < n/2$, $r \in \mathbb{Z}_{>0}$ and $1 \times n$ integer matrix $H \in \mathcal{R}(Q)$ with $Q = D(S_l^n(r))$ the bound*

$$\|H\|_\infty > \frac{r^{2l-1}}{\sqrt{2l}} \tag{6}$$

holds.

Based on Theorems 1 and 2 we pose the following question. Let us fix the sparsity level l and dimension n. In this setting, it would be interesting to find optimal upper bounds for minimal $\|H\|_\infty / r^{2l-1}$ when r tends to infinity. Specifically, given $l, n \in \mathbb{Z}_{>0}$ with $1 \le l < n/2$, to estimate

$$c_1(l,n) = \limsup \inf \frac{\|H\|_\infty}{r^{2l-1}}, \tag{7}$$

where the supremum limit is taken over all positive integers r and the infimum is taken over all $1 \times n$ integer matrices $H \in \mathcal{R}(Q)$ with $Q = D(S_l^n(r))$. Theorems 1 and 2 give a large interval for values of this quantity

$$\frac{1}{\sqrt{2l}} \leq c_1(l,n) \leq (4l\Delta(2l,n))^{2l-1}.$$

Although for finite signal spaces a single measurement is sufficient for unique recovery, one can ask whether allowing extra measurements would result in reducing measurements' entries. In this vein, we obtain the following general result. Let $Q \subset \mathbb{Z}^n$ be an arbitrary set. Suppose that we have an $1 \times n$ matrix $H \in \mathcal{R}(Q)$. We show that, for any integer m with $1 < m < n$, there exists an $m \times n$ matrix $A = (a_{ij})$ such that $A \in \mathcal{R}(Q)$ and the maximum absolute entry $\|A\|_\infty = \max_{i,j} |a_{ij}|$ is sub-linear in $\|H\|_\infty$.

Let $\gamma_{r,s}$ be the generalised Hermite constant, as defined by Rankin [14], that is the least number such that every lattice Λ of rank r in $\mathbb{R}^r$ has a sublattice Γ of rank s and determinant

$$\det(\Gamma) \leq \gamma_{r,s}^{1/2}(\det(\Lambda))^{s/r}.$$

Here $\gamma_{r,1} = \gamma_{r,r-1} = \gamma_r$ is the ordinary Hermite constant. For known results on the Rankin constant we refer the reader to the papers [14, 17, 19].

Theorem 3 *Let $Q \subset \mathbb{Z}^n$ and let H be an $1 \times n$ matrix such that $H \in \mathcal{R}(Q)$. For any integer m with $1 < m < n$, there exists an $m \times n$ matrix A such that $A \in \mathcal{R}(Q)$ and*

$$\|A\|_\infty \leq c_2(m,n)\|H\|_\infty^{\frac{n-m}{n-1}}, \tag{8}$$

where $c_2(m,n) = \gamma_{n-1,n-m}^{1/2} n^{(n-m)/(2(n-1))}$.

The proof of Theorem 3 makes use of results on rational subspaces obtained in [2]. Note that (8) improves the immediate bound $\|A\|_\infty \leq \|H\|_\infty$ when $\|H\|_\infty > c_2(m,n)^{(n-1)/(m-1)}$.

2 Unique recovery over $\mathbb{Z}_l^n$

The papers [8, 9, 11, 12] consider the problem of unique recovery over the signal space $\mathbb{Z}_l^n$, where l is a positive integer with $2l < n$. In this setting, the difference set $D(\mathbb{Z}_l^n)$ consists of $2l$-sparse integer vectors, $D(\mathbb{Z}_l^n) = \mathbb{Z}_{2l}^n$. The unique recovery of signals from $\mathbb{Z}_l^n$ involves constructing matrices $A \in \mathbb{Z}^{m \times n}$ with $m = 2l$ and as large as possible n, that belong to $\mathcal{R}(\mathbb{Z}_m^n)$. From the computational and error-correcting perspectives (see [9] for more details), it is also desirable to fix or bound the maximum absolute entry $\|A\|_\infty$ of the matrix A.

Konyagin [12, Theorem 3] proved the following theorem.

Theorem 4 *For integers $k, m \geq 2$, and integer n with*

$$m < n \le \frac{c^{-m} k^{m/(m-1)}}{\log(k)}$$

there exists an integer $m \times n$ matrix $A \in \mathcal{R}(\mathbb{Z}_m^n)$ such that $\|A\|_\infty = k$, where c is an absolute constant.

The proof of Theorem 4 employs probabilistic arguments to show existence of the desired measurement matrices. Subsequently, Konyagin and Sudakov [11, Theorem 1.3] (see also Ryutin [16]) proved the following result using an explicit and easily computable construction.

Theorem 5 *Let $k \in \mathbb{Z}_{>0}$, $m \in \mathbb{Z}_{>0}$, $m \ge 2$, and*

$$m < n \le \max(k+1, k^{m/(m-1)}/2)\,. \tag{9}$$

Then there is an $m \times n$ integer matrix $A \in \mathcal{R}(\mathbb{Z}_m^n)$ such that $\|A\|_\infty \le k$.

Theorem 5 implies the following corollary.

Corollary 6 *For any given $m, n \in \mathbb{Z}_{>0}$, $2 \le m < n$ there exists an $m \times n$ integer matrix $A \in \mathcal{R}(\mathbb{Z}_m^n)$ with*

$$\|A\|_\infty \le \Delta(m,n) = \min(n-1, \lceil (2n)^{(m-1)/m} \rceil)\,.$$

3 Admissible lattices of *m*-sparse *n*-cubes

By a *rational subspace* of $\mathbb{R}^n$ we understand a subspace generated by integer vectors. A rational hyperplane can be written as $P = \{\boldsymbol{x} \in \mathbb{R}^n : H\boldsymbol{x} = 0\}$, where $H = (H_{11}, \ldots, H_{1n})$ is an $1 \times n$ integer matrix with $\gcd(H) := \gcd(H_{11}, \ldots, H_{1n}) = 1$. We say that P has *height* $h(P) = \|H\|_\infty$.

For linearly independent $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_l$ in $\mathbb{R}^d$, the set $\Lambda = \{\sum_{i=1}^l x_i \boldsymbol{b}_i,\ x_i \in \mathbb{Z}\}$ is an l-dimensional *lattice* with *basis* $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_l$. Denoting by B the matrix with columns $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_l$, the *determinant* of Λ is defined as $\det(\Lambda) = \sqrt{\det(B^T B)}$. A lattice $\Lambda \subset \mathbb{R}^d$ is *(strictly) admissible* for a set $X \subset \mathbb{R}^d$ if Λ does not contain any nonzero point of X, that is $\Lambda \cap X \subset \{\boldsymbol{0}\}$. For a comprehensive introduction to the theory of lattices we refer the reader to [7, 10].

Let r be a positive integer and m be a positive integer with $1 < m < n$. We will consider an m-sparse n-dimensional cube

$$C_m^n(r) = \{\boldsymbol{x} \in C^n(r) : \|\boldsymbol{x}\|_0 \le m\}\,.$$

Constructing single measurements for unique recovery of sparse integer signals is closely linked to constructing admissible $(n-1)$-dimensional lattices for $C_m^n(r)$. From the unique recovery perspective, it is desirable to find a rational hyperplane P of smallest possible height such that the lattice $P \cap \mathbb{Z}^n$ is admissible for $C_m^n(r)$.

Similarly to (3), we consider the following optimisation problem. Given $m, n \in \mathbb{Z}$ with $1 < m < n$ and $r \in \mathbb{Z}_{>0}$, find

$$\min\{h(P) : P \text{ is a rational hyperplane in } \mathbb{R}^n \text{ such that the lattice } P \cap \mathbb{Z}^n \text{ is admissible for } C_m^n(r))\}. \tag{10}$$

The proofs of Theorems 1 and 2 will be based on the following estimates for the minimum in (10) that are of independent interest.

Proposition 7 *For any $m, n \in \mathbb{Z}$ with $1 < m < n$ and $r \in \mathbb{Z}_{>0}$ there exists a rational hyperplane P in $\mathbb{R}^n$ such that the lattice $P \cap \mathbb{Z}^n$ is admissible for $C_m^n(r)$ and*

$$h(P) \le p_{m,n}(r). \tag{11}$$

To prove Proposition 7 we combine constructions from the proof of Theorem 5 with aggregation techniques outlined in Sect. 4. The next result shows that the polynomial $p_{m,n}(r)$ in (11) cannot be replaced by a polynomial in r of degree smaller than $m - 1$.

Proposition 8 *For any $m, n \in \mathbb{Z}$ with $1 < m < n$, any $r \in \mathbb{Z}_{>0}$ and any rational hyperplane P in $\mathbb{R}^n$ such that the lattice $P \cap \mathbb{Z}^n$ is admissible for $C_m^n(r)$ the bound*

$$h(P) > \frac{r^{m-1}}{\sqrt{m}} \tag{12}$$

holds.

Similarly to (7), for $m, n \in \mathbb{Z}$ with $1 < m < n$, it would be interesting to estimate

$$c_3(m, n) = \limsup \inf \frac{h(P)}{r^{m-1}},$$

where the supremum limit is taken over all positive integers r and the infimum is taken over rational hyperplanes P in $\mathbb{R}^n$ such that $P \cap \mathbb{Z}^n$ is admissible for $C_m^n(r)$. Propositions 7 and 8 imply the bounds

$$\frac{1}{\sqrt{m}} \le c_3(m, n) \le (m\Delta(m, n))^{m-1}.$$

4 Consolidation/aggregation of linear Diophantine equations

The proof of Proposition 7 is based on consolidation/aggregation of linear Diophantine equations. This topic has been extensively studied in the literature. We refer the reader to the papers [13, 15] and references within.

Let $D \subset \mathbb{Z}^n$ be a set of integer points, $A \in \mathbb{Z}^{m\times n}$, $2 \le m < n$, be a matrix of rank $\operatorname{rank}(A) = m$, and $\boldsymbol{b} \in \mathbb{Z}^m$.

Let $B \in \mathbb{Z}^{l\times m}$, $l < m$, be a matrix of rank l such that

$$\{\boldsymbol{x} \in D : (BA)\boldsymbol{x} - B\boldsymbol{b} = \boldsymbol{0}\} = \{\boldsymbol{x} \in D : A\boldsymbol{x} - \boldsymbol{b} = \boldsymbol{0}\}.$$

Following [15], we will call B an *m-into-l consolidating matrix* and $(BA)\boldsymbol{x} - B\boldsymbol{b} = \boldsymbol{0}$ an *m-into-l consolidation* of $A\boldsymbol{x} - \boldsymbol{b} = \boldsymbol{0}$ with respect to the set D.

Let further $C \in \mathbb{Z}^{m\times(m-l)}$ be an integer matrix of $\operatorname{rank}(C) = m - l$ such that, for some consolidating matrix B, the columns of C span the *kernel* $\ker(B) = \{\boldsymbol{x} \in \mathbb{R}^m : B\boldsymbol{x} = \boldsymbol{0}\}$. That is, denoting by $\operatorname{span}_{\mathbb{R}}(C)$ the subspace spanned by the columns of C, we have $\operatorname{span}_{\mathbb{R}}(C) = \ker(B)$. We will call C an *aggregating matrix* for $A\boldsymbol{x} - \boldsymbol{b} = \boldsymbol{0}$ with respect to the set D.

We will write

$$F(\boldsymbol{x}) = A\boldsymbol{x} - \boldsymbol{b},$$

and denote by $F_i(\boldsymbol{x})$ the ith entry of the vector $F(\boldsymbol{x})$, that is $F(\boldsymbol{x}) = (F_1(\boldsymbol{x}), \dots, F_m(\boldsymbol{x}))^\top$.

Consider the set

$$F^o = \{F(\boldsymbol{x}) : \boldsymbol{x} \in D\} = \{A\boldsymbol{x} : \boldsymbol{x} \in D\} - \boldsymbol{b}.$$

This is the image of D under the linear mapping determined by the matrix A translated by the vector $-\boldsymbol{b}$. The following well-known lemma describes very important properties of the consolidation/aggregation.

Lemma 9 *Let $B \in \mathbb{Z}^{l\times m}$, $l < m$, be a matrix of rank l* and *$C \in \mathbb{Z}^{m\times(m-l)}$ be a matrix of rank $m - l$. Then*

(i) *B an m-into-l consolidating matrix for $A\boldsymbol{x} - \boldsymbol{b} = \boldsymbol{0}$ if and only if $F^o \cap \ker(B) \subset \{\boldsymbol{0}\}$.*
(ii) *C is an aggregating matrix of $A\boldsymbol{x} - \boldsymbol{b} = \boldsymbol{0}$ if and only if $F^o \cap \operatorname{span}_{\mathbb{R}}(C) \subset \{\boldsymbol{0}\}$.*

We will need the following lemma, given in [3, Theorem 6]. For completeness, we include a proof of this result as given in [15, Example 4.1].

Lemma 10 *Assume that $q_i \in \mathbb{Z}$ satisfy $|F_i(\boldsymbol{x})| < q_i$ for every $\boldsymbol{x} \in D$ such that $F_1(\boldsymbol{x}) = \cdots = F_{i-1}(\boldsymbol{x}) = 0$, $i = 1, \dots, m-1$. Then $F_1(\boldsymbol{x}) + q_1F_2(\boldsymbol{x}) + q_1q_2F_3(\boldsymbol{x}) + \cdots + q_1 \cdots q_{m-1}F_m(\boldsymbol{x}) = 0$ is an m-into-1 consolidation of $F(\boldsymbol{x}) = \boldsymbol{0}$ with respect to the set D.*

Proof We have to show that $B = (1, q_1, \dots, q_1 \cdots q_{m-1})$ is an m-into-1 consolidating matrix for $F(\boldsymbol{x}) = \boldsymbol{0}$. Let $C = (c_{ij}) \in \mathbb{Z}^{m\times(m-1)}$ be defined by $c_{1,k} = q_1\delta_{1,k}$ for $k = 1, \dots, m-1$ and $c_{ij} = q_i\delta_{i,j} - \delta_{i-1,j}$ for $i = 2, \dots, m$, $j = 1, \dots, m-1$. Here $\delta_{i,j}$ stands for the Kronecker delta. That is

$$C = \begin{pmatrix} q_1 & 0 & \cdots & 0 & 0 \\ -1 & q_2 & \cdots & 0 & 0 \\ 0 & -1 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & -1 & q_{m-1} \\ 0 & 0 & \cdots & 0 & -1 \end{pmatrix}.$$

We will show that C is an aggregating matrix for $F(\boldsymbol{x}) = \mathbf{0}$. It is sufficient to check that the inclusion $F^o \cap \mathrm{span}_{\mathbb{R}}(C) \subset \{\mathbf{0}\}$ in the part (ii) of Lemma 9 holds. Suppose

$$C\boldsymbol{v} = F(\boldsymbol{x}) \tag{13}$$

for some $\boldsymbol{v} \in \mathbb{R}^{m-1}$ and $\boldsymbol{x} \in D$.

Observe that the greatest common divisor of $(m-1) \times (m-1)$ subdeterminants of C is equal to one. It follows that the columns of C form a basis of the lattice $\mathrm{span}_{\mathbb{R}}(C) \cap \mathbb{Z}^m$. Next, by (13) we have $C\boldsymbol{v} \in \mathbb{Z}^m$. Therefore, $\boldsymbol{v} \in \mathbb{Z}^{m-1}$. The first coordinate of $C\boldsymbol{v}$ is $q_1 v_1$, hence $|q_1 v_1| = |F_1(\boldsymbol{x})| < |q_1|$ implies $v_1 = F_1(\boldsymbol{x}) = 0$. The second coordinate of $C\boldsymbol{v}$ is $q_2 v_2 - v_1 = q_2 v_2 = F_2(\boldsymbol{x})$. Now by definition of q_2 we have $|q_2 v_2| = |F_2(\boldsymbol{x})| < |q_2|$ and, consequently, $v_2 = 0$. Proceeding in this way we get $\boldsymbol{v} = \mathbf{0}$.

Finally, it is easy to see that the columns of C span $\ker(B)$. Hence B is an m-into-1 consolidating matrix for $F(\boldsymbol{x}) = \mathbf{0}$. □

5 Proofs of Proposition 7 and Theorem 1

We will begin with proving Proposition 7. The proof of Theorem 5 (Konyagin and Sudakov [11, Theorem 1.3]) gives two explicit constructions that can be used to obtain matrices $A \in \mathcal{R}(\mathbb{Z}_m^n)$ that satisfy conditions of Corollary 6. For completeness, we will outline these constructions here.

Observe first that $A \in \mathcal{R}(\mathbb{Z}_m^n)$ if and only if all $m \times m$ subdeterminants of A are nonzero. Therefore, if for some d satisfying $m < n < d$ there exists an $m \times d$ matrix $A \in \mathcal{R}(\mathbb{Z}_m^d)$, then an $m \times n$ matrix in $\mathcal{R}(\mathbb{Z}_m^n)$ can be obtained by removing any $d - n$ columns from A. Set first $k = n - 1$. The first construction gives $A = (a_{ij}) \in \mathcal{R}(\mathbb{Z}_m^d)$ with $d \geq k + 1$. The dimension d is chosen as an odd prime number satisfying $k + 1 \leq d \leq 2k + 1$. Subsequently, the entries of the matrix A are defined as $a_{ij} \equiv j^{i-1} (\mathrm{mod}\ d)$ with $|a_{ij}| \leq (d-1)/2 \leq k$. In particular, for all j we have $a_{1j} = 1$. Next, set $k = \lceil (2n)^{(m-1)/m} \rceil$. The second construction gives $A = (a_{ij}) \in \mathcal{R}(\mathbb{Z}_m^d)$ with $d \geq k^{m/(m-1)}/2$. The dimension d is chosen as a prime number with $k^{m/(m-1)}/2 \leq d \leq k^{m/(m-1)}$. The entries of the matrix A satisfy $a_{ij} \equiv l_{ij} j^{i-1} (\mathrm{\ mod}\ d)$, where l_{ij} are certain integers not divisible by d chosen in a such way that $|a_{ij}| \leq k$. In particular, for all j one can take $l_{1j} = 1$, so that $a_{1j} = 1$.

In both constructions above, renumbering the rows of A, we may assume that $a_{mj} = 1$ for all j. Set $k = \Delta(m, n)$ and for $s = m\,k\,r + 1$ take

$$B = (1, s, \dots, s^{m-1})$$

and

$$H = BA\,.$$

We will show that the hyperplane $P = \ker(H)$ satisfies the conditions of Proposition 7.

Let $F(\boldsymbol{x}) = A\boldsymbol{x}$ and let $F_i(\boldsymbol{x})$ denote the ith entry of $F(\boldsymbol{x})$, that is

$$\begin{aligned} F_1(\boldsymbol{x}) &= a_{11}x_1 + \cdots + a_{1n}x_n\,, \\ &\vdots \\ F_m(\boldsymbol{x}) &= a_{m1}x_1 + \cdots + a_{mn}x_n\,. \end{aligned}$$

For any $\boldsymbol{x} \in C_m^n(r)$ and any $i \in \{1, \dots, m\}$, we have

$$F_i(\boldsymbol{x}) \le \|\boldsymbol{x}\|_0 \|A\|_\infty r \le m\,k\,r < s\,.$$

Lemma 10, applied with $D = C_m^n(r) \cap \mathbb{Z}^n$ and $q_i = s$ for $i = 1, \dots, m-1$, implies that

$$\{\boldsymbol{x} \in C_m^n(r) \cap \mathbb{Z}^n \,:\, H\boldsymbol{x} = \boldsymbol{0}\} = \{\boldsymbol{x} \in C_m^n(r) \cap \mathbb{Z}^n \,:\, A\boldsymbol{x} = \boldsymbol{0}\}\,. \tag{14}$$

Since $A \in \mathcal{R}(\mathbb{Z}_m^n)$ we have

$$\{\boldsymbol{x} \in C_m^n(r) \cap \mathbb{Z}^n \,:\, A\boldsymbol{x} = \boldsymbol{0}\} = \{\boldsymbol{0}\}\,. \tag{15}$$

Consequently, combining (14) and (15), the lattice $P \cap \mathbb{Z}^n$ is admissible for $C_m^n(r)$.

Finally, we obtain the bound

$$h(P) \le \|H\|_\infty \le s^{m-1} + k \sum_{i=0}^{m-2} s^i$$

that implies (11).

Remark 1 For given sparsity level m, dimension n and cube size r the set $\{F(\boldsymbol{x}) \,:\, \boldsymbol{x} \in D\}$ constructed in the proof will likely allow a more accurate choice of parameters q_i in Lemma 10, resulting in an improvement on the bound (11). Further, aggregation techniques can be also applied to the matrices in $\mathcal{R}(\mathbb{Z}_m^n)$ obtained using a probabilistic approach from the proof of Theorem 4 (Konyagin [12, Theorem 3]).

5.1 Proof of Theorem 1

Let $m = 2l$. By Proposition 7, there is a rational hyperplane P in $\mathbb{R}^n$ such that the lattice $P \cap \mathbb{Z}^n$ is admissible for $C_m^n(2r) \cap \mathbb{Z}^n$ and the bound

$$h(P) \le p_{m,n}(2r) \tag{16}$$

holds.

We can write $P = \ker(H)$ for an $1 \times n$ integer matrix H with $h(P) = \|H\|_\infty$. The inclusion

$$D(S_l^n(r)) \subset S_m^n(2r) = C_m^n(2r) \cap \mathbb{Z}^n$$

implies the condition (1) with $A = H$ and $Q = D(S_l^n(r))$. Hence $H \in \mathcal{R}(Q)$. Finally, the bound (5) immediately follows from (16).

6 Proofs of Proposition 8 and Theorem 2

We will first prove Proposition 8. Let $A \in \mathbb{Z}^{m\times n}$, $m < n$, and let $\tau = \{i_1, \dots, i_k\} \subseteq \{1, \dots, n\}$ with $i_1 < i_2 < \cdots < i_k$. We will denote by A_τ the $m \times k$ submatrix of A with columns indexed by τ. In the same manner, given $\boldsymbol{x} \in \mathbb{R}^n$, we will denote by $\boldsymbol{x}_\tau$ the vector $(x_{i_1}, \dots, x_{i_k})^\top$. The complement of τ in $\{1, \dots, n\}$ will be denoted as $\bar{\tau}$. For matrices A of rank m, the notation $\gcd(A)$ will be used for the greatest common divisor of all $m \times m$ subdeterminants of A.

The proof makes use of the following version of Siegel's Lemma obtained by Bombieri and Vaaler [4, Theorem 2].

Theorem 11 *Let $M \in \mathbb{Z}^{m\times n}$, $m < n$, be a matrix of rank m. There exist $n - m$ linearly independent integer vectors $\boldsymbol{y}_1, \dots, \boldsymbol{y}_{n-m} \in \ker(M)$ satisfying*

$$\prod_{i=1}^{n-m} \|\boldsymbol{y}_i\|_\infty \le \frac{\sqrt{\det(MM^T)}}{\gcd(M)}\,.$$

Suppose, to derive a contradiction, that Proposition 8 does not hold. Then for some $m, n \in \mathbb{Z}_{>0}$ with $1 < m < n$, and $r \in \mathbb{Z}_{>0}$ there exists a rational hyperplane P in $\mathbb{R}^n$ such that $P \cap \mathbb{Z}^n$ is admissible for $C_m^n(r)$ and

$$h(P) \le \frac{r^{m-1}}{\sqrt{m}}\,. \tag{17}$$

There exists an $1 \times n$ integer matrix H such that $P = \ker(H)$ and $h(P) = \|H\|_\infty$. Take $\tau = \{1, \dots, m\}$. Observe that H cannot have zero entries, as otherwise its kernel P would contain the corresponding standard basis vectors. Hence, $H_\tau \neq \mathbf{0}$. By Theorem 11, applied with $M = H_\tau$, there exists an integer vector $\boldsymbol{x}_\tau \in \ker(H_\tau)$ such that

$$0 < \|\boldsymbol{x}_\tau\|_\infty^{m-1} \le \frac{\|H_\tau\|_2}{\gcd(H_\tau)} \le \sqrt{m}\|H_\tau\|_\infty \le \sqrt{m}\,h(P)\,. \tag{18}$$

By the upper bound (17) we have

$$\|\boldsymbol{x}_\tau\|_\infty \le r\,.$$

Consequently, the lifted vector

$$\begin{pmatrix} \boldsymbol{x}_\tau \\ \mathbf{0}_{\bar{\tau}} \end{pmatrix} \in C_m^n(r) \cap P \cap \mathbb{Z}^n,$$

contradicting the assumption that $P \cap \mathbb{Z}^n$ is admissible for $C_m^n(r)$. The obtained contradiction completes the proof of Proposition 8.

Remark 2 A minor improvement of (18) can be obtained using a refinement of Siegel's lemma proved in [1]. Further, the last inequality in (18) can be slightly strengthened using the following observation. Since $P \cap \mathbb{Z}^n$ is admissible for $C_m^n(1)$ and $m \geq 2$, we may assume that $H_{11} < H_{12} < \cdots < H_{1n}$. This allows choosing H_τ with $\|H_\tau\| \leq \|H\|_\infty - n + m$.

6.1 Proof of Theorem 2

Take any $l, n \in \mathbb{Z}_{>0}$ with $1 \leq l < n/2$, $r \in \mathbb{Z}_{>0}$ and any $1 \times n$ integer matrix $H \in \mathcal{R}(Q)$ with $Q = D(S_l^n(r))$. Consider the hyperplane $P = \ker(H)$. Set $m = 2l$ and observe that

$$C_m^n(r) \cap \mathbb{Z}^n \subset Q\,.$$

Therefore, the lattice $P \cap \mathbb{Z}^n$ is admissible for $C_m^n(r)$ and (12) implies (6).

7 Proof of Theorem 3

The proof of Theorem 3 is based on the following result, which is a special case of Proposition 1 (ii) in [2].

Proposition 12 *Let S be an one-dimensional rational subspace of $\mathbb{R}^n$. When $1 < m < n$, there is a rational subspace $T \supset S$ of dimension m in $\mathbb{R}^n$ with*

$$\det(T \cap \mathbb{Z}^n) \leq \gamma_{n-1,n-m}^{1/2} \det(S \cap \mathbb{Z}^n)^{(n-m)/(n-1)}\,. \tag{19}$$

The constant $\gamma_{n-1,n-m}^{1/2}$ here is best possible.

Take any $Q \subset \mathbb{Z}^n$ and suppose that we are given an integer $1 \times n$ matrix $H \in \mathcal{R}(Q)$. Let m be an integer with $1 < m < n$ and let T be the subspace from Proposition 12, applied to the rational subspace S of $\mathbb{R}^n$ spanned by the row vector H.

By Theorem 11, applied with any $(n-m) \times n$ integer matrix M with $T = \ker(M)$, there exist m linearly independent integer vectors $\boldsymbol{g}_1, \ldots, \boldsymbol{g}_m \in T$ such that

$$\|\boldsymbol{g}_1\|_\infty \cdots \|\boldsymbol{g}_m\|_\infty \leq \frac{\sqrt{\det(MM^T)}}{\gcd(M)} = \det(T \cap \mathbb{Z}^n)\,. \tag{20}$$

For a proof of the last equality in (20) we refer the reader to [18, Corollaries 5I-J]. Now we can form a matrix A with rows $\boldsymbol{g}_1^\top, \ldots, \boldsymbol{g}_m^\top$, so that $S \subset \mathrm{span}_{\mathbb{R}}(A^\top)$. Observe that $\ker(A) \subset \ker(H)$ and hence, $A \in \mathcal{R}(Q)$.

Finally, combining (20), (19) and the bound $\det(S \cap \mathbb{Z}^n) \leq \sqrt{n}\|H\|_\infty$, we get the estimate (8):

$$\|A\|_\infty \le \gamma_{n-1,n-m}^{1/2} n^{(n-m)/(2(n-1))} \|H\|_\infty^{(n-m)/(n-1)}.$$

Declarations

Conflict of interests The authors have no competing interests to declare that are relevant to the content of this article. Data sharing not applicable to this article as no datasets were generated or analysed during the current study.

References

1. Aliev, I.: Siegel's lemma and sum-distinct sets. Discrete Comput. Geom. **39**(1–3), 59–66 (2008)
2. Aliev, I., Schinzel, A., Schmidt, W.M.: On vectors whose span contains a given linear subspace. Monatsh. Math. **144**(3), 177–191 (2005)
3. Anthonisse, J.M.: A note on equivalent systems of linear Diophantine equations. Z. Operations Res. Ser. A-B **17**, A167–A177 (1973)
4. Bombieri, E., Vaaler, J.: On Siegel's lemma. Invent. Math. **73**(1), 11–32 (1983)
5. Candès, E.J., Romberg, J.K., Tao, T.: Stable signal recovery from incomplete and inaccurate measurements. Common. Pure Appl. Math. **59**(8), 1207–1223 (2006)
6. Candès, E.J., Tao, T.: Decoding by linear programming. IEEE Trans. Inform. Theory **51**(12), 4203–4215 (2005)
7. Cassels, J.W.S.: An Introduction to the Geometry of Numbers. Springer, Berlin (1971)
8. Fukshansky, L., Hsu. A.: Covering point-sets with parallel hyperplanes and sparse signal recovery. Discrete and Computational Geometry (2022)
9. Fukshansky, L., Needell, D., Sudakov, B.: An algebraic perspective on integer sparse recovery. Appl. Math. Comput. **340**, 31–42 (2019)
10. Gruber, P.M., Lekkerkerker, C.G.: Geometry of Numbers. North-Holland Mathematical Library, vol. 37, 2nd edn. North-Holland Publishing Co, Amsterdam (1987)
11. Konyagin, S., Sudakov, B.: An extremal problem for integer sparse recovery. Linear Algebra Appl. **586**, 1–6 (2020)
12. Konyagin, S.V.: On the recovery of an integer vector from linear measurements. Mat. Zametki **104**(6), 863–871 (2018)
13. Poirion, P.-L.: Optimal constraints aggregation method for ILP. Discrete Appl. Math. **262**, 148–157 (2019)
14. Rankin, R.A.: On positive definite quadratic forms. J. Lond. Math. Soc. **28**, 309–314 (1953)
15. Rosenberg, I.G.: Aggregation of equations in integer programming. Discrete Math. **10**, 325–341 (1974)
16. Ryutin, K.S.: Recovering sparse integer vectors from linear measurements. Uspekhi Mat. Nauk **74**(6(450)), 167–168 (2019)
17. Sawatani, K., Watanabe, T., Okuda, K.: A note on the Hermite–Rankin constant. J. Théor. Nombres Bordeaux **22**(1), 209–217 (2010)
18. Schmidt, W.M.: Diophantine Approximations and Diophantine Equations. Lecture Notes in Mathematics. Springer, Berlin (1991)

19. Thunder, J.L.: Higher-dimensional analogs of Hermite's constant. Mich. Math. J. **45**(2), 301–314 (1998)