Decomposition of Rational Discrete Hyperplanes [*]

Tristan Roussillon

July 11, 2025

Abstract

This paper is a contribution to the study of rational discrete hyperplanes, i.e., sets of points with integer coordinates lying between two parallel planes. Up to translation and symmetry, they are completely determined by a nonzero normal vector $\mathbf{a} \in \mathbb{N}^d$. If $\|\mathbf{a}\|_1 > 2^{d-1}$, there are two approximations $\mathbf{b}, \mathbf{c} \in \mathbb{N}^d$ of $\mathbf{a}$, satisfying $\mathbf{a} = \mathbf{b}+\mathbf{c}$, such that the discrete hyperplane plane of normal $\mathbf{a}$ can be partitioned into two disjoint sets having respectively the combinatorial structure of discrete hyperplanes of normal $\mathbf{b}$ and $\mathbf{c}$. The result is based on explicit geometrical mappings described by unimodular $d \times d$ matrices derived from $\mathbf{a}$ and its approximations. It may have practical interest in discrete geometry for the generation and recognition of discrete hyperplanes as well as for the decomposition of boundaries of discrete sets into planar patches.

1 Introduction

Discrete geometry mainly deals with sets of points of integer coordinates considered to be discretized versions of Euclidean objects. Very basic objects of interest are discrete hyperplanes [3, 2]. They are notably used to decompose boundaries of finite discrete sets into planar parts.

In 2d, the set of maximal discrete straight segments along the boundary of a discrete set, also called *tangential cover* in [11], can be computed very efficiently [19, 7, 12]. It provides a multigrid-convergent estimator of length and tangents [4, 21], a way of identifying convex and concave parts [6, 8, 27] as well as a way of computing compact polygonal representations [13, 23, 27]. In addition, asymptotic properties of maximal discrete straight segments can be used to estimate the local amount of noise [18]. See [20] for a summary of possible applications.

Almost all the above-mentionned results are based on a very fundamental property: any discrete straight segment large enough can be decomposed into two smaller discrete straight segments and there is a canonical way of doing so. This result can be obtained from the splitting formula [31, pp. 153–157] or the standard factorization of Christoffel words [1, pp. 19–22].

We focus in this paper on the extension of such decomposition to dimension $d \geq 2$. The main existing framework for that is based on a representation of discrete hyperplanes as unions of $(d-1)$-dimensional faces and on a geometrical extension of subsitutions, i.e., rules that replace faces by sets of faces. We can cite, among other, the pioneering work of Ito [16], as well as the works done by Fernique [9, 10], and more recently [25]. We propose in this paper another approach, which has several interesting features compared to the above framework. A detailed comparison is provided in the last section.

Before describing our approach, let us introduce some notations and definitions. Let $\{\mathbf{e}_1, \dots, \mathbf{e}_d\}$ be the canonical basis of $\mathbb{R}^d$. We denote by $\mathbf{0}$ the origin and by $\mathbf{1} = \sum_{i=1}^d \mathbf{e}_i$ the vector with all coordinates equal to 1. The j-th coordinate of a vector $\mathbf{x} \in \mathbb{R}^d$ is denoted by x_j. We focus on rational discrete hyperplanes, i.e., sets of points with integer coordinates lying between two parallel planes with rational coefficients. We use the standard arithmetical model introduced in [24]:

[*] This work has been funded by PARADIS ANR-18-CE23-0007-01 research grant.

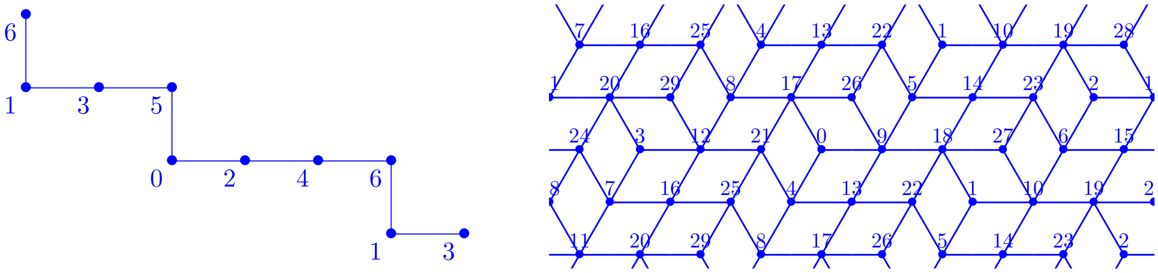
Definition 1. *Let* $\mathbf{a} \in \mathbb{N}^d \setminus \{\mathbf{0}\}$ *be such that* $\gcd(\mathbf{a}) = 1$. *The standard arithmetical discrete hyperplane* $\mathcal{P}(\mathbf{a})$ *is defined as*

$$\mathcal{P}(\mathbf{a}) := \{\mathbf{x} \in \mathbb{Z}^d \mid 0 \leq \mathbf{x} \cdot \mathbf{a} < \|\mathbf{a}\|_1\}. \tag{1}$$

Note that we assume without loss of generality that the coordinates of $\mathbf{a}$ are nonnegative integers. The case of negative coordinates can be bypassed by symmetry, the case of rational coordinates, by multiplying all coordinates by their least common multiple. In addition, we assume that all discrete hyperplanes pass by the origin because translations do not change the relative position of points.

It is very easy to determine whether a given point $\mathbf{x} \in \mathbb{Z}^d$ belongs to $\mathcal{P}(\mathbf{a})$ or not: the scalar product $\mathbf{x} \cdot \mathbf{a}$, called the *height* of $\mathbf{x}$, must fall between 0 and $\|\mathbf{a}\|_1 - 1$.

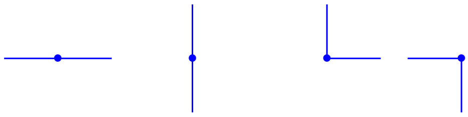
The adjacency graph associated to $\mathcal{P}(\mathbf{a})$ is a graph whose vertices are the points of $\mathcal{P}(\mathbf{a})$ and that has an edge between two distinct points $\mathbf{x}$ and $\mathbf{y}$ if and only if $\|\mathbf{x} - \mathbf{y}\|_1 = 1$. A discrete line and its adjacency graph are illustrated in Fig. 1 (a), while a discrete plane and its adjacency graph are illustrated in Fig. 1 (b). Note that this two-dimensional representation is obtained by projecting the discrete plane along $\mathbf{1}$, the squares thus appear as rhombi.



(a) (b)

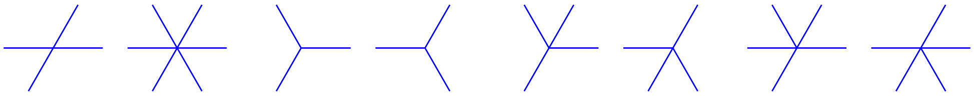
Figure 1: (Finite parts of) $\mathcal{P}(2, 5)$ (a) and $\mathcal{P}(4, 9, 17)$ (b). The number displayed close to a point is its height.

The set of edges incident to a given vertex $\mathbf{x}$ is determined by its height. The arrangement of edges incident to points of same height is thus the same. In 2d, there are only four different arrangements of incident edges in all discrete lines and at most three in a given one (Fig. 2). In 3d, there are only eight different arrangements of incident edges in all discrete planes and at most seven in a given one [14] (Fig. 3).



(a) (b) (c) (d)

Figure 2: All arrangements of incident edges in 2d – (a) and (b) cannot be in the same discrete line.



(a) (b) (c) (d) (e) (f) (g) (h)

Figure 3: All arrangements of incident edges in 3d – (a) and (b) cannot be in the same discrete plane. This is close to a vertex-atlas in tiling theory [30, section 5.3].

This paper is an extension of [26]. We show that, for any $\mathbf{a}$ large enough, there are two approximations $\mathbf{b}, \mathbf{c}$ of $\mathbf{a}$, such that $\mathbf{a} = \mathbf{b} + \mathbf{c}$ and $\mathcal{P}(\mathbf{a})$ can be partitioned into two disjoint sets having respectively the combinatorial structure of $\mathcal{P}(\mathbf{b})$ and $\mathcal{P}(\mathbf{c})$. More precisely, we prove the following

Theorem 1. *Let* $\mathbf{a} \in \mathbb{N}^d \setminus \{\mathbf{0}\}$ *be such that* $\gcd(\mathbf{a}) = 1$ *and* $\|\mathbf{a}\|_1 > 2^{d-1}$*. There exist two approximations* $\mathbf{b}, \mathbf{c}$ *of* $\mathbf{a}$*, two subsets* $\mathcal{S}_b, \mathcal{S}_c \subset \mathcal{P}(\mathbf{a})$ *and two bijective functions* g_b, g_c *such that* $\mathbf{a} = \mathbf{b} + \mathbf{c}$*,* $\mathcal{P}(\mathbf{a}) = \mathcal{S}_b \cup \mathcal{S}_c$*,* $\emptyset = \mathcal{S}_b \cap \mathcal{S}_c$*,* $g_b(\mathcal{S}_b) = \mathcal{P}(\mathbf{b})$*,* $g_c(\mathcal{S}_c) = \mathcal{P}(\mathbf{c})$*, and* $\forall j \in [\![1, d]\!]$*,*

$$\mathbf{x} \in \mathcal{S}_b \textit{ and } \mathbf{x} \pm \mathbf{e}_j \in \mathcal{P}(\mathbf{a}) \Leftrightarrow \; g_b(\mathbf{x}), g_b(\mathbf{x}) \pm \mathbf{e}_j \in \mathcal{P}(\mathbf{b}),$$
$$\mathbf{x} \in \mathcal{S}_c \textit{ and } \mathbf{x} \pm \mathbf{e}_j \in \mathcal{P}(\mathbf{a}) \Leftrightarrow \; g_c(\mathbf{x}), g_c(\mathbf{x}) \pm \mathbf{e}_j \in \mathcal{P}(\mathbf{c}).$$

The last part of the theorem means that the arrangement of edges incident to a vertex of $\mathcal{S}_b$ (resp. $\mathcal{S}_c$) is exactly the same as the arrangement of edges incident to $g_b(\mathbf{x})$ (resp. $g_c(\mathbf{x})$). An elementary three-dimensional example is given in Fig. 4. Another example is shown in Fig. 5.

The paper is organized as follows. In Section 2, we introduce the approximations of $\mathbf{a}$. In Section 3, instead of focusing on the points of $\mathcal{P}(\mathbf{a})$, we focus on their heights, interpreted as projections on a 1-dimensional subspace determined by $\mathbf{a}$. We derived several results mainly based on the Euclidean division and relate them to approximations. These two sections generalize the whole theoretical content of [26].

In addition, we provide a geometric and explicit construction of the decomposition in the two following sections by taking into account the $(d-1)$-dimensional subspace orthogonal to $\mathbf{a}$. In Section 4, we show how both 1- and $(d-1)$-dimensional subspaces are described by unimodular matrices of size $d \times d$. Slightly different matrices are also used to measure how far a vector is from $\mathbf{a}$ and thus to decide whether it is an approximation of $\mathbf{a}$ or not. With these tools in hand, we prove Theorem 1 in Section 5 and explicitely give the bijective functions g_b, g_c.

2 Approximations

The main theorem presented in the introduction involves vectors that approximate a given nonzero vector accurately enough. More precisely, we use the following

Definition 2. *Let* $\mathbf{a} \in \mathbb{N}^d \setminus \{\mathbf{0}\}$ *be such that* $\gcd(\mathbf{a}) = 1$*. A vector* $\mathbf{b} \in \mathbb{N}^d \setminus \{\mathbf{0}\}$ *is an* approximation *of* $\mathbf{a}$ *if and only if* $\mathbf{a} - \mathbf{b} \in \mathbb{N}^d \setminus \{\mathbf{0}\}$*,* $\gcd(\mathbf{b}) = 1$ *and*

$$\left\| \|\mathbf{a}\|_1 \mathbf{b} - \|\mathbf{b}\|_1 \mathbf{a} \right\|_\infty < \|\mathbf{a}\|_1 / 2. \tag{2}$$

As explained in [26, Section 4], this definition is closely related to the simultaneous approximation of fractions (see also, e.g., [15, Section 5.2], [28, Section 6.3]). We prove below that an approximation always exists provided that $\mathbf{a}$ is large enough.

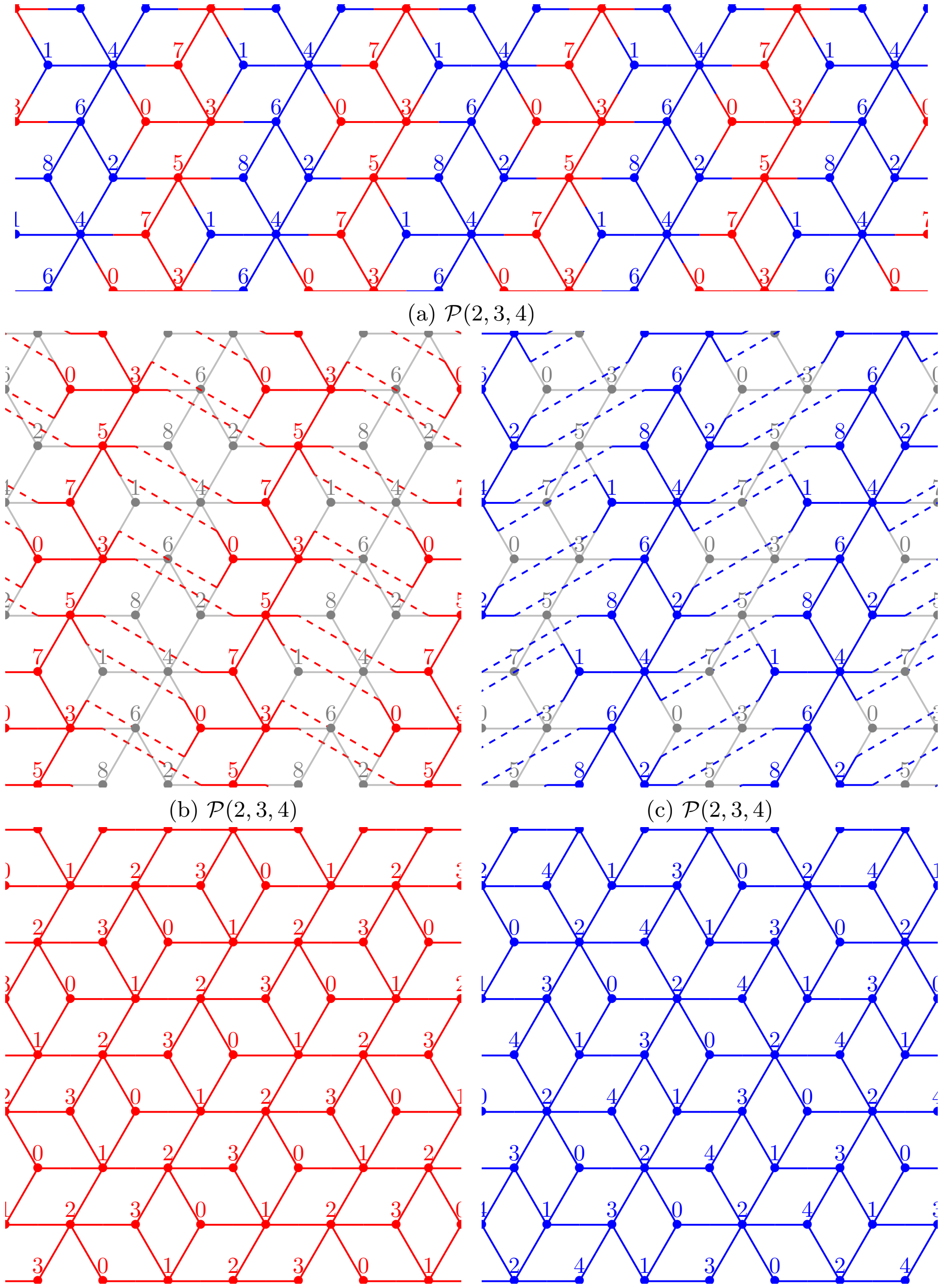
Lemma 2. *Let* $\mathbf{a} \in \mathbb{N}^d \setminus \{\mathbf{0}\}$ *be such that* $\gcd(\mathbf{a}) = 1$*. If* $\|\mathbf{a}\|_1 > 2^{d-1}$*, then an approximation of* $\mathbf{a}$ *as defined in Definition 2 exists.*

Proof. Let us consider the open unit d-cube $\mathcal{B} := \{\mathbf{x} \in \mathbb{R}^d \mid \|\mathbf{x}\|_\infty < 1/2\}$ and the images $\mathcal{B}_1$ and $\mathcal{B}_1^\star$ of $\mathcal{B}$ under the orthogonal projection onto the vector $\mathbf{1}$ and onto the supplementary subspace, respectively. An illustration in low dimensions is provided in Fig. 6 (a), where $\mathbf{1}$ points to the right in the case $d = 2$ and out of the plane of the paper in the case $d = 3$. According to a result about unit d-cubes, $\mathcal{B}_1$ and $\mathcal{B}_1^\star$ have the same volume [22]. Since the volume of $\mathcal{B}_1$ is equal to the unit d-cube's longest diagonal, one has $vol(\mathcal{B}_1^\star) = vol(\mathcal{B}_1) = \sqrt{d}$.

Let us consider the open line segment $\mathcal{S} := \{\lambda \mathbf{a} \mid \lambda \in (-1, 1)\}$ and the image $\mathcal{S}_1$ of $\mathcal{S}$ under the orthogonal projection onto $\mathbf{1}$. Since the scalar projection of $\pm\mathbf{a}$ onto $\mathbf{1}$ is $\pm\frac{\mathbf{a}\cdot\mathbf{1}}{\sqrt{d}}$, one has $vol(\mathcal{S}_1) = \frac{2}{\sqrt{d}}\|\mathbf{a}\|_1$.

Finally, let us consider the dilation of $\mathcal{S}$ by $\mathcal{B}_1^\star$, i.e., $\mathcal{D} := \mathcal{S} \oplus \mathcal{B}_1^\star$. It is a symmetric and convex region. An illustration for $d = 2$ is provided in Fig. 6 (b), where $\mathcal{S}$ and $\mathcal{S}_1$ are solid line segments, while $\mathcal{D}$ is the gray area.

In addition, there is a shear mapping between $\mathcal{S} \oplus \mathcal{B}_1^\star$ and $\mathcal{S}_1 \oplus \mathcal{B}_1^\star$, where the points are displaced within hyperplanes of normal vector $\mathbf{1}$. Since this transformation preserves the



(a) $\mathcal{P}(2,3,4)$

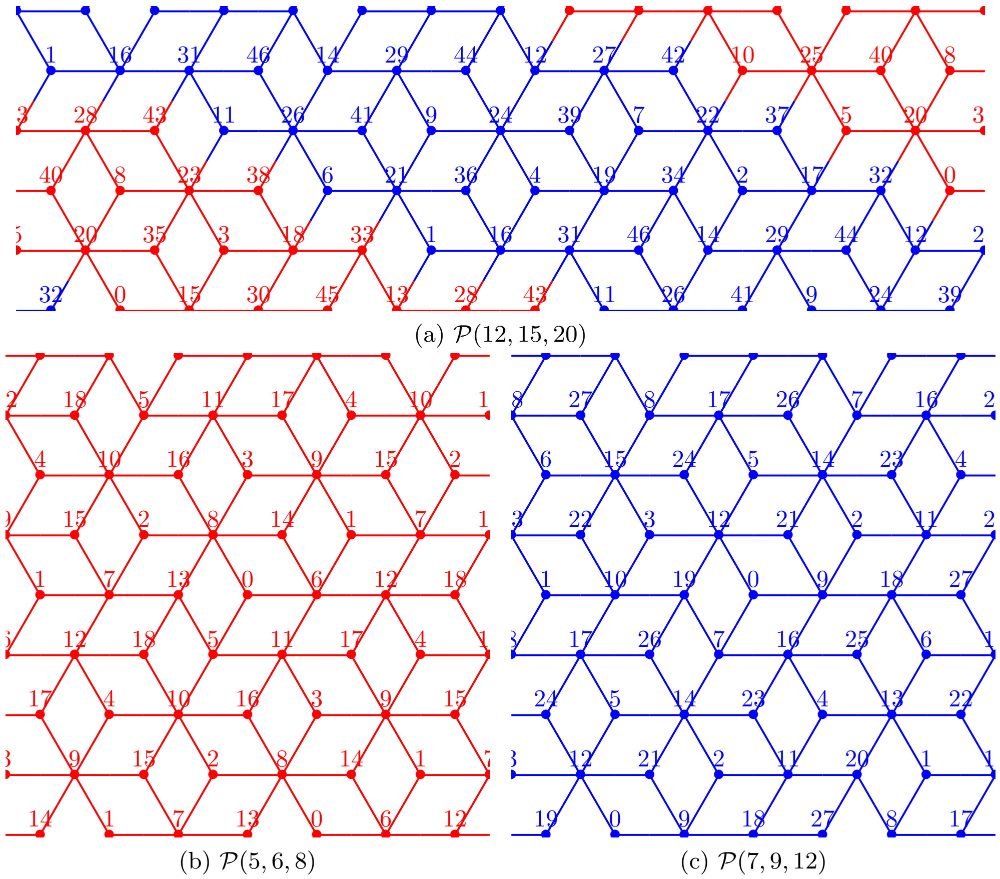
(b) $\mathcal{P}(2,3,4)$

(c) $\mathcal{P}(2,3,4)$

(d) $\mathcal{P}(1,1,2)$

(e) $\mathcal{P}(1,2,2)$

Figure 4: $\mathcal{P}(2,3,4)$ is partitioned into two sets (red and blue), each looking like a collection of strips (a). When the strips are combined together in (b) and (c), respectively, two discrete hyperplanes are obtained, namely $\mathcal{P}(1,1,2)$ (d) and $\mathcal{P}(1,2,2)$ (e), respectively. The arrangements of edges in the red (resp. blue) set match those of $\mathcal{P}(1,1,2)$ (resp. $\mathcal{P}(1,2,2)$).


(a) $\mathcal{P}(12, 15, 20)$

(b) $\mathcal{P}(5, 6, 8)$

(c) $\mathcal{P}(7, 9, 12)$

Figure 5: Decomposition of $\mathcal{P}(12, 15, 20)$ using the approximations $(5, 6, 8)$ and $(7, 9, 12)$. The arrangements of edges in the red (resp. blue) set match those of $\mathcal{P}(5, 6, 8)$ (resp. $\mathcal{P}(7, 9, 12)$).

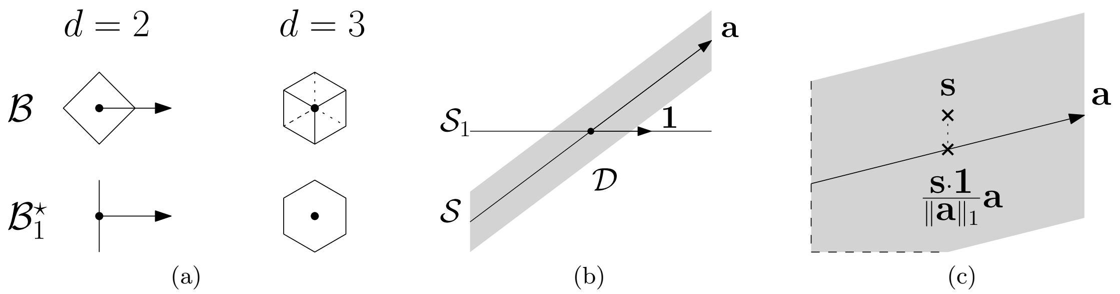


Figure 6: Illustration of the proof of Lemma 2.

volume, one has,

$$\begin{aligned} vol(\mathcal{D}) &= vol\big(\mathcal{S} \oplus \mathcal{B}_1^\star\big) \\ &= vol\big(\mathcal{S}_1 \oplus \mathcal{B}_1^\star\big) \\ &= vol\big(\mathcal{B}_1^\star\big) vol(\mathcal{S}_1) \\ &= \sqrt{d}\frac{2}{\sqrt{d}}\|\mathbf{a}\|_1 \\ &= 2\|\mathbf{a}\|_1 \\ &> 2 \cdot 2^{d-1} = 2^d \quad \text{(by hypothesis).} \end{aligned}$$

By Minkowski's theorem, since the volume of $\mathcal{D}$ is strictly greater than 2^d, $\mathcal{D}$ contains at least a nonzero integer point $\mathbf{s}$. By construction, the scalar projection of $\mathbf{s}$ onto $\mathbf{1}$ belongs to $\mathcal{S}_1$, which means that $-\frac{\mathbf{a}\cdot\mathbf{1}}{\sqrt{d}} < \frac{\mathbf{s}\cdot\mathbf{1}}{\sqrt{d}} < \frac{\mathbf{a}\cdot\mathbf{1}}{\sqrt{d}}$. Multiplying everything by $\sqrt{d}$, one has $-\mathbf{a}\cdot\mathbf{1} < \mathbf{s}\cdot\mathbf{1} < \mathbf{a}\cdot\mathbf{1}$.

Note that $\mathbf{s}\cdot\mathbf{1} \neq 0$. Indeed, the only way for $\mathbf{s}$ to have its coordinates sum to 0, would be for it to belong to $\{\mathbf{0}\} \oplus \mathcal{B}_1^\star \subset \{\mathbf{0}\} \oplus \mathcal{B}$, but the unit d-cube centered at $\mathbf{0}$ contains no integer points other than $\mathbf{0}$.

Due to the symmetry, one can assume without loss of generality that $0 < \mathbf{s}\cdot\mathbf{1}$. Furthermore, as illustrated in Fig. 6 (c), $\frac{\mathbf{s}\cdot\mathbf{1}}{\|\mathbf{a}\|_1}\mathbf{a}$ is the projection of $\mathbf{s}$ onto $\mathcal{S}$ along projecting lines orthogonal to $\mathbf{1}$. Since both $\mathbf{s}$ and its projection are in $\mathcal{D}$ by definition, we have

$$\left\|\frac{\mathbf{s}\cdot\mathbf{1}}{\|\mathbf{a}\|_1}\mathbf{a} - \mathbf{s}\right\|_\infty < \frac{1}{2} \quad \text{which implies} \quad \big\|\big(\mathbf{s}\cdot\mathbf{1}\big)\mathbf{a} - \big(\|\mathbf{a}\|_1\big)\mathbf{s}\big\|_\infty < \frac{\|\mathbf{a}\|_1}{2}.$$

Now, let us define $\mathbf{b} := \mathbf{s}/\gcd(\mathbf{s})$. It is clear that $\mathbf{b}\cdot\mathbf{1} = (\mathbf{s}\cdot\mathbf{1})/\gcd(\mathbf{s})$, which implies $0 < \mathbf{b}\cdot\mathbf{1} \leq \mathbf{s}\cdot\mathbf{1} < \mathbf{a}\cdot\mathbf{1}$ and

$$\big\|\big(\mathbf{b}\cdot\mathbf{1}\big)\mathbf{a} - \big(\|\mathbf{a}\|_1\big)\mathbf{b}\big\|_\infty = \frac{1}{\gcd(\mathbf{s})}\big\|\big(\mathbf{s}\cdot\mathbf{1}\big)\mathbf{a} - \big(\|\mathbf{a}\|_1\big)\mathbf{s}\big\|_\infty < \frac{\|\mathbf{a}\|_1}{2\gcd(\mathbf{s})} \leq \frac{\|\mathbf{a}\|_1}{2}. \tag{3}$$

From (3), the coordinates of $\mathbf{b}$ can be bounded from below and above. Indeed, (3) reads

$$\forall j \in [\![1,d]\!], -\frac{\|\mathbf{a}\|_1}{2} < \big(\mathbf{b}\cdot\mathbf{1}\big)a_j - \big(\|\mathbf{a}\|_1\big)b_j < \frac{\|\mathbf{a}\|_1}{2}.$$

Rearranging the terms of the right inequality, we obtain $\frac{(\mathbf{b}\cdot\mathbf{1})}{\|\mathbf{a}\|_1}a_j - \frac{1}{2} < b_j$. Since $a_j \geq 0$ and $b_j \in \mathbb{Z}$, it follows that $b_j \geq 0$ and, as a by-product, $\mathbf{b}\cdot\mathbf{1} = \|\mathbf{b}\|_1$. In addition, since $0 < \|\mathbf{b}\|_1$, $\mathbf{b} \neq \mathbf{0}$ and we conclude that $\mathbf{b} \in \mathbb{N}^d \setminus \{\mathbf{0}\}$.

Similarly, rearranging the terms of the left inequality, we obtain $b_j < \frac{\|\mathbf{b}\|_1}{\|\mathbf{a}\|_1}a_j + \frac{1}{2}$. Since $\|\mathbf{b}\|_1 < \|\mathbf{a}\|_1$, we have $\frac{\|\mathbf{b}\|_1}{\|\mathbf{a}\|_1}a_j + \frac{1}{2} < a_j + \frac{1}{2}$, which implies $b_j < a_j + \frac{1}{2}$, hence $b_j \leq a_j$. In addition, $\|\mathbf{b}\|_1 < \|\mathbf{a}\|_1$ also implies $\mathbf{b} \neq \mathbf{a}$ and we conclude that $\mathbf{a} - \mathbf{b} \in \mathbb{N}^d \setminus \{\mathbf{0}\}$.

To sum up,

- $\mathbf{b}, \mathbf{a} - \mathbf{b} \in \mathbb{N}^d \setminus \{\mathbf{0}\}$,
- $\gcd(\mathbf{b}) = 1$ by definition of $\mathbf{b}$,
- $\big\|\big(\|\mathbf{b}\|_1\big)\mathbf{a} - \big(\|\mathbf{a}\|_1\big)\mathbf{b}\big\|_\infty < \frac{\|\mathbf{a}\|_1}{2}$ by (3) and $\mathbf{b}\cdot\mathbf{1} = \|\mathbf{b}\|_1$,

which means that $\mathbf{b}$ is an approximation of $\mathbf{a}$ according to Definition 2. □

Before ending the section, let us consider a vector $\mathbf{a} \in \mathbb{N}^d \setminus \{\mathbf{0}\}$ such that $\gcd(\mathbf{a}) = 1$ and an approximation $\mathbf{b}$ of $\mathbf{a}$. Let us consider the discrete hyperplanes $\mathcal{P}(\mathbf{a})$ and $\mathcal{P}(\mathbf{b})$. A crucial part of Theorem 1 involves a subset $\mathcal{S} \subset \mathcal{P}(\mathbf{a})$ and a bijective function $g : \mathbb{Z}^d \mapsto \mathbb{Z}^d$ such that, for all $\mathbf{x} \in \mathcal{S}$, there exists an edge between $\mathbf{x}$ and $\mathbf{x} + \mathbf{e}_j$ in the adjacency graph associated to $\mathcal{P}(\mathbf{a})$ if and only if there exists an edge between $g(\mathbf{x})$ and $g(\mathbf{x}) + \mathbf{e}_j$ in the adjacency graph associated to $\mathcal{P}(\mathbf{b})$:

$$\mathbf{x}, \mathbf{x} + \mathbf{e}_j \in \mathcal{P}(\mathbf{a}) \Leftrightarrow g(\mathbf{x}), g(\mathbf{x}) + \mathbf{e}_j \in \mathcal{P}(\mathbf{b}).$$

By considering a function $f : \mathbb{Z} \mapsto \mathbb{Z}$ acting on heights, instead of points, and using the definition of discrete hyperplanes (Definition 1), the above equivalence translates into:

$$h, h + a_j \in \{0, \dots, \|\mathbf{a}\|_1 - 1\} \Leftrightarrow f(h), f(h) + b_j \in \{0, \dots, \|\mathbf{b}\|_1 - 1\}.$$

In the following section, we show how to define the subset $\mathcal{S}$ (Definition 3) and the function f (Definition 4) using only $\|\mathbf{a}\|_1, \|\mathbf{b}\|_1$ and arithmetical properties. Since, most of the results are independant, $\|\mathbf{a}\|_1$ and $\|\mathbf{b}\|_1$ are denoted by two positive integers A and B, respectively. These preliminary results will be completed in Section 5 with the explicit construction of the function g.

3 Arithmetical Results

The heights of the points of a discrete hyperplane form a range of consecutive integers (Definition 1). That is why we gather in this section useful results about such ranges. Given two integers $i, j \in \mathbb{Z}$, $[\![i, j]\!]$ denotes the set of all integers ranging from i to j (the set is empty if $i > j$).

Definition 3. *Let $A, B \in \mathbb{N} \setminus \{0\}$ be two positive integers such that $B < A$. Let $D \in \mathbb{Z}$ be any integer. The set $\mathcal{H}(A, B, D)$ is defined as follows:*

$$\mathcal{H}(A, B, D) := \{h \in [\![0, A-1]\!] \mid (hB - D) \bmod A < B\}. \tag{4}$$

The above definition provides a way of partitioning the set $[\![0, A-1]\!]$ as shown in the following

Lemma 3. *Let $A, B \in \mathbb{N} \setminus \{0\}$ be two positive integers such that $B < A$. Let $D \in \mathbb{Z}$ be any integer. Let $\mathcal{H}$ be defined as in Definition 3. The sets $\mathcal{H}(A, B, D)$ and $\mathcal{H}(A, A-B, -D+1)$ partition $[\![0, A-1]\!]$.*

Proof. Obviously, $\forall h \in [\![0, A-1]\!]$, either $h \in \mathcal{H}(A, B, D)$ or $h \notin \mathcal{H}(A, B, D)$. The whole point is therefore to show that $h \notin \mathcal{H}(A, B, D)$ is equivalent to $h \in \mathcal{H}(A, A-B, -D+1)$.

By definition, $h \notin \mathcal{H}(A, B, D)$ means that $hB - D(\text{mod}A) \in [\![B, A-1]\!]$. However, by symmetry around 0, this is equivalent to $-(hB-D)(\bmod A) \in [\![1, A-B]\!]$ and by translation by -1, this is equivalent to $-(hB - D) - 1(\text{mod}A) \in [\![0, A-B-1]\!]$. See Fig. 7 for an illustration.

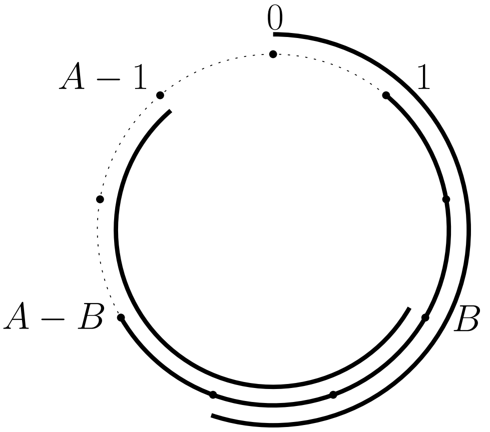


Figure 7: The intervals $[\![B, A-1]\!]$, $[\![1, A-B]\!]$ and $[\![0, A-B-1]\!]$ are depicted with a sequence of concentric circular arcs, starting with the innermost arc and going outward.

Furthermore, $-(hB - D) - 1(\text{mod}A) = h(A - B) - (-D + 1)(\text{mod}A)$. As a result, $h(A-B) - (-D+1)(\text{mod}A) \in [\![0, A-B-1]\!]$, which means that $h \in \mathcal{H}(A, A-B, -D+1)$ by definition. □

The largest (resp. smallest) integer less (resp. greater) than or equal to x is denoted by $\lfloor x \rfloor$ (resp. $\lceil x \rceil$). In the following definition, we introduce a function that bijectively map $\mathcal{H}(A, B, D)$ to $[\![0, B-1]\!]$ under certain conditions.

h	0	1	2	3	4	5	6	7	8
$(3h-1) \bmod 9 < 3$	8	2	5	8	2	5	8	2	5
$6h \bmod 9 < 6$	0	6	3	0	6	3	0	6	3
$\lfloor (3h-1)/9 \rfloor$	-1	0	0	0	1	1	1	2	2
$\lfloor 6h/9 \rfloor$	0	0	1	2	2	3	4	4	5

Table 1: In the top row, the range $\llbracket 0, 8 \rrbracket$ is partitioned into two subsets: $\mathcal{H}(9, 3, 1)$ in red and $\mathcal{H}(9, 6, 0)$ in blue. The two middle rows show how the subsets are computed according to Definition 3. The two last rows shows the functions mapping those subsets to the ranges $\llbracket 0, 2 \rrbracket$ and $\llbracket 0, 5 \rrbracket$ respectively.

Definition 4. *Let $A, B \in \mathbb{N} \setminus \{0\}$ be two positive integers such that $B < A$. Let $D \in \mathbb{Z}$ be any integer. Function $f(A, B, D) : \mathbb{Z} \mapsto \mathbb{Z}$ is defined such that:*

$$f(A, B, D)(h) := \left\lfloor \frac{hB - D}{A} \right\rfloor, \tag{5}$$

and function $f'(A, B, D) : \mathbb{Z} \mapsto \mathbb{Z}$ such that

$$f'(A, B, D)(h) := \left\lceil \frac{hA + D}{B} \right\rceil = -\left\lfloor \frac{-hA - D}{B} \right\rfloor. \tag{6}$$

The previous definition is illustrated in the two last rows of Table 1. We will show in Lemma 4 that $f(A, B, D)$ is indeed bijective on the range $\mathcal{H}(A, B, D)$ and that the inverse is $f'(A, B, D)$ whatever the value of D. Then, we will show in Lemma 5 that the image of $f(A, B, D)$ is $\llbracket 0, B - 1 \rrbracket$ for specific values of D.

To simplify the notation, we will write in this section $f(h)$ instead of $f(A, B, D)(h)$, using the full form only when the parameters differ from A, B, D.

Lemma 4. *Let $A, B \in \mathbb{N} \setminus \{0\}$ be two integers such that $B < A$. Let $D \in \mathbb{Z}$ be any integer. Let $\mathcal{H}, f, f'$ be defined as in Definitions 3 and 4. For all $h \in \mathcal{H}(A, B, D)$, $f'\big(f(h)\big) = h$ and $f\big(f'(h)\big) = h$.*

Proof. We first consider $f'\big(f(h)\big)$ and set r_h to be the remainder of the Euclidean division of $hB - D$ by A. We have $f(h)A = (hB - D) - r_h$. Thus,

$$\begin{aligned} f'\big(f(h)\big) &= -\left\lfloor \frac{-f(h)A - D}{B} \right\rfloor \\ &= -\left\lfloor \frac{-hB + D + r_h - D}{B} \right\rfloor \\ &= -\left\lfloor (-h) + \frac{r_h}{B} \right\rfloor \end{aligned}$$

However, h is an integer and $0 \leq r_h/B < 1$ because h is assumed to be in $\mathcal{H}(A, B, D)$ and therefore, r_h in $\llbracket 0, B - 1 \rrbracket$. Consequently, $f'\big(f(h)\big) = -(-h) = h$.

Simiarly, in order to simplify $f'\big(f(h)\big)$, we set r'_h to be the remainder of the Euclidean division of $-hA - D$ by B. We have $-f'(h)B = (-hA - D) - r'_h$. Thus,

$$\begin{aligned} f\big(f'(h)\big) &= \left\lfloor \frac{f'(h)B - D}{A} \right\rfloor \\ &= \left\lfloor \frac{hA + D + r'_h - D}{A} \right\rfloor \\ &= \left\lfloor h + \frac{r'_h}{A} \right\rfloor \end{aligned}$$

However, h is an integer and $0 \leq r'_h/A < 1$ because $r'_h \in \llbracket 0, B - 1 \rrbracket \subset \llbracket 0, A - 1 \rrbracket$. Consequently, $f\big(f'(h)\big) = h$. □

Lemma 5. *Let $A, B \in \mathbb{N} \setminus \{0\}$ be two positive integers such that $B < A$. Let $\mathcal{H}, f$ be defined as in Definitions 3 and 4. For all $D \in [\![-B+1, A-B]\!]$ and $h \in \mathcal{H}(A, B, D)$, $f(h) \in [\![0, B-1]\!]$.*

Proof. The proof is based on the equality $hB - D = f(h)A + r$, with $r \in [\![0, B-1]\!]$ (by Euclidean division, the restriction to $[\![0, B-1]\!]$ coming from the fact $h \in \mathcal{H}(A, B, D)$). We now separately consider the lower and upper bound.

We first bound $hB - D$ from below using $0 \leq h$ and $-A + B \leq -D$:

$$-A + B \leq hB - D.$$

Then, we replace $hB - D$ by $f(h)A + r$ to equivalently get:

$$-A + B \leq f(h)A + r.$$

Using $r \leq B - 1$, we finally get:

$$-A + B \leq f(h)A + B - 1. \text{ Therefore, } -1 + \frac{1}{A} \leq f(h),$$

which is equivalent to $0 \leq f(h)$ because A is positive and $f(h)$ is an integer.

We then bound $hB - D$ from above using $h \leq A - 1$ and $-D \leq B - 1$:

$$hB - D \leq AB - B + B - 1.$$

Then, we replace $hB - D$ by $f(h)A + r$ to equivalently get:

$$f(h)A + r \leq AB - 1.$$

Using $0 \leq r$, we finally get:

$$f(h)A \leq AB - 1. \text{ Therefore, } f(h) \leq B - \frac{1}{A},$$

which is equivalent to $f(h) \leq B - 1$ because A is positive and $B, f(h)$ are integers. □

We proceed with the following result, which is crucial for the rest of the paper (see, e.g., Corollary 7).

Lemma 6. *Let $A, B \in \mathbb{N} \setminus \{0\}$ be two positive integers such that $B < A$. Let $\mathcal{H}, f$ be defined as in Definitions 3 and 4. Let $a_j, b_j \in \mathbb{N}$ be two nonnegative integers such that $a_j \leq A$ and $b_j \leq B$. Let Q_j be set to $a_jB - b_jA$.*

For all $Q \geq |Q_j|$, $D \in [\![-B+1+Q, A-B-Q]\!]$ and $h \in \mathcal{H}(A, B, D)$,

$$a_j \leq h \Leftrightarrow b_j \leq f(h), \quad h \leq A - a_j - 1 \Leftrightarrow f(h) \leq B - b_j - 1.$$

Note that the subscript j has no particular signification in this lemma; a_j and b_j are plain labels just as u and v could be. We chose however those names to more easily use the lemma later, where a_j and b_j will be taken from the j-th coordinate of two vectors.

Proof. We use the same approach as in the proof of Lemma 5. In particular, we use the equality $hB - D = f(h)A + r$, with $r \in [\![0, B-1]\!]$.

For both bounds, we can separately show the forward implication for all $D \in [\![-B+1+Q_j, A-B-Q_j]\!]$ and the backward implication for all $D \in [\![-B+1-Q_j, A-B+Q_j]\!]$. The equivalence is then implied for all D in the intersection of the two previous ranges, i.e., for all $D \in [\![-B+1+|Q_j|, A-B-|Q_j|]\!]$. The final result follows because $[\![-B+1+Q, A-B-Q]\!]$ is included in $[\![-B+1+|Q_j|, A-B-|Q_j|]\!]$ for all $Q \geq |Q_j|$.

Now, we focus on the lower bound, the proof for the upper bound being similar is left to the reader.

For the forward implication, we first bound $hB - D$ from below using $a_j \leq h$ and $-A + B + Q_j \leq -D$:

$$a_jB - A + B + Q_j \leq hB - D.$$

Then, we replace Q_j by $b_jA - a_jB$ and $hB - D$ by $f(h)A + r$ to equivalently get

$$-A + B + b_jA \leq f(h)A + r.$$

Using $r \leq B-1$, we finally get:

$$-A+B+b_jA \leq f(h)A+B-1. \text{ Therefore, } b_j - 1 + \frac{1}{A} \leq f(h),$$

which is equivalent to $b_j \leq f(h)$.

For the backward implication, we conversely first bound $f(h)A + r$ from $b_j \leq f(h)$ and $0 \leq r$:

$$b_jA \leq f(h)A + r.$$

Then, we replace $f(h)A + r$ by $hB - D$ to equivalently get

$$b_jA \leq hB - D \Leftrightarrow b_jA + D \leq hB.$$

From $-B + 1 - Q_j \leq D$ and replacing Q_j by $b_jA - a_jB$, we obtain

$$a_jB - B + 1 \leq hB. \text{ Therefore, } a_j - 1 + \frac{1}{B} \leq h,$$

which is equivalent to $a_j \leq h$. □

To end the section, we relate the above results, especially Lemma 6, to approximations. Let us consider a vector $\mathbf{a} \in \mathbb{N}^d \setminus \{\mathbf{0}\}$ such that $\gcd(\mathbf{a}) = 1$ and an approximation $\mathbf{b}$ of $\mathbf{a}$. Let us consider the quantities $A := \|\mathbf{a}\|_1$, $B := \|\mathbf{b}\|_1$. For all $j \in [\![1, d]\!]$, we have $0 \leq a_j \leq A$ and, since $\mathbf{b} \in \mathbb{N}^d \setminus \{\mathbf{0}\}$, $0 \leq b_j \leq B$. Since $\mathbf{a} - \mathbf{b} \in \mathbb{N}^d \setminus \{\mathbf{0}\}$, we also have $B < A$. In addition, $Q \geq \left\|\mathbf{a}\big(\|\mathbf{b}\|_1\big) - \mathbf{b}\big(\|\mathbf{a}\|_1\big)\right\|_\infty$ obviously implies $Q \geq |a_jB - b_jA|$ for all $j \in [\![1, d]\!]$. Therefore, we obtain the following corollary of Lemma 6.

Corollary 7. *Let $\mathbf{a} \in \mathbb{N}^d \setminus \{\mathbf{0}\}$ be such that* $\gcd(\mathbf{a}) = 1$. *Let $\mathbf{b}$ be an approximation of $\mathbf{a}$ according to Definition 2. Let $\mathcal{H}, f$ be defined as in Definitions 3 and 4.*

For all $Q \geq \left\|\mathbf{a}\big(\|\mathbf{b}\|_1\big) - \mathbf{b}\big(\|\mathbf{a}\|_1\big)\right\|_\infty$, $D \in [\![-\|\mathbf{b}\|_1 + 1 + Q, \|\mathbf{a}\|_1 - \|\mathbf{b}\|_1 - Q]\!]$, $h \in \mathcal{H}(\|\mathbf{a}\|_1, \|\mathbf{b}\|_1, D)$ and $j \in [\![1, d]\!]$,

$$a_j \leq h \Leftrightarrow b_j \leq f(\|\mathbf{a}\|_1, \|\mathbf{b}\|_1, D)(h), \tag{7}$$
$$h \leq \|\mathbf{a}\|_1 - a_j - 1 \Leftrightarrow f(\|\mathbf{a}\|_1, \|\mathbf{b}\|_1, D)(h) \leq \|\mathbf{b}\|_1 - b_j - 1. \tag{8}$$

Another corollary can be deduced by setting $Q := \left\|\mathbf{a}\big(\|\mathbf{b}\|_1\big) - \mathbf{b}\big(\|\mathbf{a}\|_1\big)\right\|_\infty$, because in that case D always lies in a non-empty set. Indeed, since $\mathbf{b}$ is an approximation of $\mathbf{a}$, we have by definition $2Q \leq \|\mathbf{a}\|_1 - 1$, which is equivalent to $-\|\mathbf{b}\|_1 + 1 + Q \leq \|\mathbf{a}\|_1 - \|\mathbf{b}\|_1 - Q$.

As a consequence, there exists a value for D such that, using $f = f(\|\mathbf{a}\|_1, \|\mathbf{b}\|_1, D)$, the following equivalence

$$h, h + a_j \in [\![0, \|\mathbf{a}\|_1 - 1]\!] \Leftrightarrow f(h), f(h) + b_j \in [\![0, \|\mathbf{b}\|_1 - 1]\!]$$

is true for all $h \in \mathcal{H}(\|\mathbf{a}\|_1, \|\mathbf{b}\|_1, D)$.

This result is illustrated in Fig. 8, where the heights of the points are listed in increasing order from left to right (top row for $\mathbf{a}$, bottom row for $\mathbf{b}$). For a vector $\mathbf{v} \in \{\mathbf{a}, \mathbf{b}\}$ and every height h, the segments at angle $4\pi/3$, 0, $2\pi/3$ respectively represent the edge between a point of height h and a neighbor of height $h + v_1$, $h + v_2$, $h + v_3$, where angles are measured counterclockwise with respect to the horizontal segment directed to the right. Symmetrically, the segments at angle $\pi/3$, π, $5\pi/3$ respectively represent the edge between a point of height h and a neighbor of height $h - v_1$, $h - v_2$, $h - v_3$.

Since $(1, 2, 3)$ is an approximation of $(2, 3, 4)$, there exists D such that $f(9, 6, D)$ maps $\mathcal{H}(9, 6, D)$ (the blue part of the top row) to $[\![0, 5]\!]$ (bottom row) and the arrangement of segments is the same around a given h and the corresponding $f(9, 6, D)(h)$. Note that D is equal to 0 in Fig. 8.

As a counter-example, let us consider $(1, 1, 3)$. It is a nonzero vector with nonnegative and coprime coordinates. Each of its coordinates is smaller that the corresponding coordinate of $(2, 3, 4)$. However, $(1, 1, 3)$ is not an approximation of $(2, 3, 4)$ because

$$\|5(2, 3, 4) - 9(1, 1, 3)\|_\infty = \|(1, 6, -7)\|_\infty = 7 > 9/2.$$

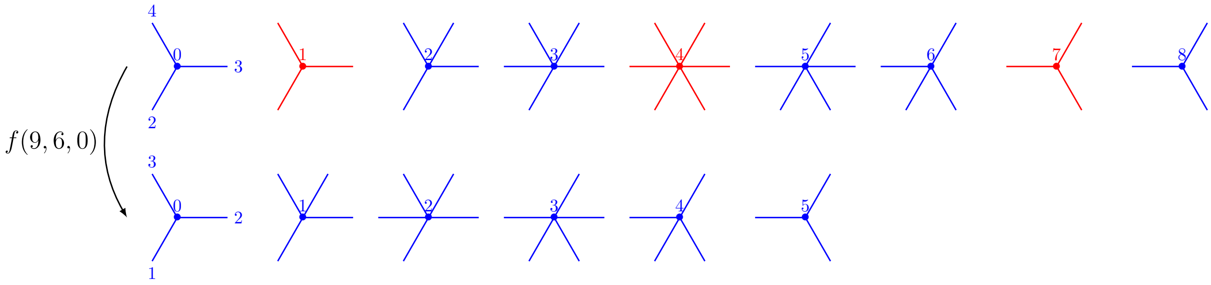


Figure 8: Lists of the arrangements of edges in the adjacency graph associated to $\mathcal{P}(2,3,4)$ (top) and $\mathcal{P}(1,2,3)$ (bottom) sorted by height. The blue part of the top row is combinatorially equivalent to the bottom row and there is a bijective function that maps the heights of one set to the other.

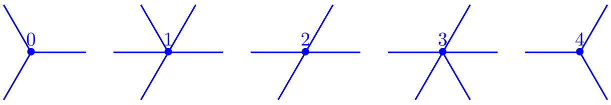


Figure 9: Lists of the arrangements of edges in the adjacency graph of $\mathcal{P}(1,1,3)$ sorted by height.

The combinatorial structure of $\mathcal{P}(1,1,3)$ is represented in Fig. 9. Three different arrangements of edges, around the points of height 1, 2 and 3, are not present in $\mathcal{P}(2,3,4)$ (Fig. 8, top row). It is thus not possible to retrieve $\mathcal{P}(1,1,3)$ from $\mathcal{P}(2,3,4)$.

With Corollary 7, we are close to be able to prove our main theorem. However, we lack geometrical results in order to deal with points instead of heights and explicitely construct the functions g_b and g_c involved in Theorem 1. The next two sections aim at filling that gap.

4 Matrix-Based Encoding of Approximations

In this section, we propose to use a unimodular matrix, i.e., of determinant ± 1, to store both $\mathbf{a}$ and at least one of its approximations, because we can derive from it orthogonal vectors and measures of how far the other column vectors are from $\mathbf{a}$.

We denote by $\mathbf{I}$ the identity matrix, by ${}^{t}\mathbf{M}$, the transpose of $\mathbf{M}$ and by ${}^{c}\mathbf{M}$, the cofactor matrix of $\mathbf{M}$. We recall below several well-known results: (9), (10) and (11), can be found respectively in [29, 4.35, 4.36, 4.37]).

$$ {}^{t}\mathbf{M}\,{}^{c}\mathbf{M} = {}^{c}\mathbf{M}\,{}^{t}\mathbf{M} = \det(\mathbf{M})\mathbf{I}, \tag{9}$$

$$ {}^{c}({}^{c}\mathbf{M}) = \det(\mathbf{M})^{d-2}\mathbf{M}, \tag{10}$$

$$ \det({}^{c}\mathbf{M}) = \det(\mathbf{M})^{d-1}. \tag{11}$$

We also use the notation $\mathbf{M} \overset{i}{\leftarrow} \mathbf{x}$ for the matrix obtained from $\mathbf{M}$ where its i-th column as been replaced by a vector $\mathbf{x}$, i.e.,

$$ \mathbf{M} \overset{i}{\leftarrow} \mathbf{x} = \mathbf{M}(\mathbf{I} - \mathbf{e}_i\,{}^{t}\mathbf{e}_i) + \mathbf{x}\,{}^{t}\mathbf{e}_i. $$

We gather below several results that will be discussed afterwards.

Proposition 8. *Let $\mathbf{U}$ be a unimodular matrix of size $d \times d$ such that the entries of the last column do not sum to zero, i.e., ${}^{t}\mathbf{1}\mathbf{U}\mathbf{e}_d \neq 0$. Let $\mathbf{V}$ be set to ${}^{c}\mathbf{U} \overset{d}{\leftarrow} \mathbf{1}$. We have the following results:*

$$ \mathbf{V} = {}^{c}\mathbf{U}\mathbf{W}, \textit{ where } \mathbf{W} := \mathbf{I} \overset{d}{\leftarrow} \det(\mathbf{U})\,{}^{t}\mathbf{U}\mathbf{1}, \tag{12}$$

$$ \det(\mathbf{V}) = \det(\mathbf{U})^{d}\left({}^{t}\mathbf{1}\mathbf{U}\mathbf{e}_d\right), \tag{13}$$

$$ \det({}^{c}\mathbf{V}) = \left({}^{t}\mathbf{1}\mathbf{U}\mathbf{e}_d\right)^{d-1}, \tag{14}$$

$$ {}^{t}\mathbf{1}\,{}^{c}\mathbf{V} = \det(\mathbf{V})\,{}^{t}\mathbf{e}_d, \tag{15}$$

$$ {}^{\mathrm{c}}\mathbf{V}\mathbf{e}_d = \det(\mathbf{U})^{d-2}\mathbf{U}\mathbf{e}_d, \tag{16} $$

$$ \forall i \in [\![1, d-1]\!],\ {}^{\mathrm{c}}\mathbf{V}\mathbf{e}_i = \det(\mathbf{U})^{d-1}\Big(\big({}^{\mathrm{t}}\mathbf{1}\mathbf{U}\mathbf{e}_d\big)\mathbf{U}\mathbf{e}_i - \big({}^{\mathrm{t}}\mathbf{1}\mathbf{U}\mathbf{e}_i\big)\mathbf{U}\mathbf{e}_d \Big). \tag{17} $$

Proof. First, (12) comes from (9), the unimodularity of $\mathbf{U}$ and the very definitions of $\mathbf{V}$ and $\mathbf{W}$:

$$
\begin{aligned}
{}^{\mathrm{c}}\mathbf{U}\mathbf{W} &= {}^{\mathrm{c}}\mathbf{U}\big(\mathbf{I} \overset{d}{\leftarrow} \det(\mathbf{U})\,{}^{\mathrm{t}}\mathbf{U}\mathbf{1}\big) \\
&= {}^{\mathrm{c}}\mathbf{U}\big(\mathbf{I} - \mathbf{e}_d\,{}^{\mathrm{t}}\mathbf{e}_d + \det(\mathbf{U})\,{}^{\mathrm{t}}\mathbf{U}\mathbf{1}\,{}^{\mathrm{t}}\mathbf{e}_d\big) \\
&= {}^{\mathrm{c}}\mathbf{U}\big(\mathbf{I} - \mathbf{e}_d\,{}^{\mathrm{t}}\mathbf{e}_d\big) + \underbrace{\det(\mathbf{U})\,{}^{\mathrm{c}}\mathbf{U}\,{}^{\mathrm{t}}\mathbf{U}}_{\det(\mathbf{U})^2=1}\mathbf{1}\,{}^{\mathrm{t}}\mathbf{e}_d \\
&= {}^{\mathrm{c}}\mathbf{U}\big(\mathbf{I} - \mathbf{e}_d\,{}^{\mathrm{t}}\mathbf{e}_d\big) + \mathbf{1}\,{}^{\mathrm{t}}\mathbf{e}_d \\
&= {}^{\mathrm{c}}\mathbf{U} \overset{d}{\leftarrow} \mathbf{1} = \mathbf{V}.
\end{aligned}
$$

The determinant of $\mathbf{W}$ can be computed by its cofactor expansion along the last row because the only nonzero entry in the last row is the very last one, equal to $\det(\mathbf{U})\,{}^{\mathrm{t}}\mathbf{1}\mathbf{U}\mathbf{e}_d$, and its corresponding cofactor is 1. As a result, $\det(\mathbf{W}) = \det(\mathbf{U})\,{}^{\mathrm{t}}\mathbf{1}\mathbf{U}\mathbf{e}_d$. Using (11) and (12), one can derive (13) as follows:

$$ \det(\mathbf{V}) = \underbrace{\det({}^{\mathrm{c}}\mathbf{U})}_{\det(\mathbf{U})^{d-1}}\ \underbrace{\det(\mathbf{W})}_{\det(\mathbf{U})\,{}^{\mathrm{t}}\mathbf{1}\mathbf{U}\mathbf{e}_d} = \det(\mathbf{U})^{d}\,{}^{\mathrm{t}}\mathbf{1}\mathbf{U}\mathbf{e}_d. $$

Then, using (11) and noticing that $\det(\mathbf{U})^{d(d-1)} = 1$, (14) follows. It is also possible to derive (15) from (9) and the very definition of $\mathbf{V}$:

$$ {}^{\mathrm{t}}\mathbf{1}\,{}^{\mathrm{c}}\mathbf{V} = {}^{\mathrm{t}}\mathbf{e}_d\,{}^{\mathrm{t}}\mathbf{V}\,{}^{\mathrm{c}}\mathbf{V} = \det(\mathbf{V})\,{}^{\mathrm{t}}\mathbf{e}_d. $$

Multiplying both sides of (12) by ${}^{\mathrm{t}}\mathbf{U}$ on the left and ${}^{\mathrm{t}}({}^{\mathrm{c}}\mathbf{V})$ on the right, then transposing both sides, we obtain

$$ \det(\mathbf{V})\mathbf{U} = \det(\mathbf{U})\,{}^{\mathrm{c}}\mathbf{V}\,{}^{\mathrm{t}}\mathbf{W}. $$

Using (13), the above equation simplifies into

$$ \det(\mathbf{U})^{d-1}\big({}^{\mathrm{t}}\mathbf{1}\mathbf{U}\mathbf{e}_d\big)\mathbf{U} = {}^{\mathrm{c}}\mathbf{V}\,{}^{\mathrm{t}}\mathbf{W} $$

and implies

$$ \forall i \in [\![1, d]\!],\ \det(\mathbf{U})^{d-1}\big({}^{\mathrm{t}}\mathbf{1}\mathbf{U}\mathbf{e}_d\big)\mathbf{U}\mathbf{e}_i = {}^{\mathrm{c}}\mathbf{V}\,{}^{\mathrm{t}}\mathbf{W}\mathbf{e}_i. $$

We now separately address the cases $i = d$ and $i \in [\![1, d-1]\!]$ in order to prove (16) and (17), respectively. We first replace ${}^{\mathrm{t}}\mathbf{W}\mathbf{e}_d$ by $\det(\mathbf{U})\big({}^{\mathrm{t}}\mathbf{1}\mathbf{U}\mathbf{e}_d\big)\mathbf{e}_d$ in the above equation to obtain

$$ \det(\mathbf{U})^{d-1}\big({}^{\mathrm{t}}\mathbf{1}\mathbf{U}\mathbf{e}_d\big)\mathbf{U}\mathbf{e}_d = \det(\mathbf{U})\big({}^{\mathrm{t}}\mathbf{1}\mathbf{U}\mathbf{e}_d\big)\,{}^{\mathrm{c}}\mathbf{V}\mathbf{e}_d. $$

Since ${}^{\mathrm{t}}\mathbf{1}\mathbf{U}\mathbf{e}_d \neq 0$ by hypothesis and $\det(\mathbf{U}) = \pm 1$, we divide both members by $\det(\mathbf{U})\big({}^{\mathrm{t}}\mathbf{1}\mathbf{U}\mathbf{e}_d\big)$ to obtain (16).

Similarly, for all $i \in [\![1, d-1]\!]$, ${}^{\mathrm{t}}\mathbf{W}\mathbf{e}_i$ is equal to $\mathbf{e}_i + \det(\mathbf{U})\big({}^{\mathrm{t}}\mathbf{1}\mathbf{U}\mathbf{e}_i\big)\mathbf{e}_d$, which leads to

$$ \det(\mathbf{U})^{d-1}\big({}^{\mathrm{t}}\mathbf{1}\mathbf{U}\mathbf{e}_d\big)\mathbf{U}\mathbf{e}_i = {}^{\mathrm{c}}\mathbf{V}\Big(\mathbf{e}_i + \det(\mathbf{U})\big({}^{\mathrm{t}}\mathbf{1}\mathbf{U}\mathbf{e}_i\big)\mathbf{e}_d\Big) $$

and, rearranging the terms, to

$$ {}^{\mathrm{c}}\mathbf{V}\mathbf{e}_i = \det(\mathbf{U})^{d-1}\big({}^{\mathrm{t}}\mathbf{1}\mathbf{U}\mathbf{e}_d\big)\mathbf{U}\mathbf{e}_i - \det(\mathbf{U})\big({}^{\mathrm{t}}\mathbf{1}\mathbf{U}\mathbf{e}_i\big)\,{}^{\mathrm{c}}\mathbf{V}\mathbf{e}_d. $$

Using (16), we then obtain (17). □

Proposition 8 is illustrated by numerical examples in Table 2 for $d = 2$ and $d = 3$. The reader can check the equations, especially

- (13) and (14) (the determinants are given in the table),

$\mathbf{U}$	${}^{c}\mathbf{U}$	$\mathbf{V}$	${}^{c}\mathbf{V}$
$\det(\mathbf{U})$	$\det({}^{c}\mathbf{U})$	$\det(\mathbf{V})$	$\det({}^{c}\mathbf{V})$
$\begin{pmatrix}1 & 2\\ 2 & 5\end{pmatrix}$	$\begin{pmatrix}5 & -2\\ -2 & 1\end{pmatrix}$	$\begin{pmatrix}5 & 1\\ -2 & 1\end{pmatrix}$	$\begin{pmatrix}1 & 2\\ -1 & 5\end{pmatrix}$
1	1	7	7
$\begin{pmatrix}0 & 1 & 2\\ 0 & 2 & 5\\ 1 & 3 & 7\end{pmatrix}$	$\begin{pmatrix}-1 & 5 & -2\\ -1 & -2 & 1\\ 1 & 0 & 0\end{pmatrix}$	$\begin{pmatrix}-1 & 5 & 1\\ -1 & -2 & 1\\ 1 & 0 & 1\end{pmatrix}$	$\begin{pmatrix}-2 & 2 & 2\\ -5 & -2 & 5\\ 7 & 0 & 7\end{pmatrix}$
1	1	14	14^2
$\begin{pmatrix}1 & 1 & 2\\ 1 & 1 & 3\\ 1 & 2 & 4\end{pmatrix}$	$\begin{pmatrix}-2 & -1 & 1\\ 0 & 2 & -1\\ 1 & -1 & 0\end{pmatrix}$	$\begin{pmatrix}-2 & -1 & 1\\ 0 & 2 & 1\\ 1 & -1 & 1\end{pmatrix}$	$\begin{pmatrix}3 & 1 & -2\\ 0 & -3 & -3\\ -3 & 2 & -4\end{pmatrix}$
-1	1	-9	9^2

Table 2: Illustration of Proposition 8 for $d = 2$ and $d = 3$.

- (15), which essentially states that, for the first $d-1$ columns of ${}^{c}\mathbf{V}$, the entries sum to zero,
- (16), which essentially states that the d-th column of $\mathbf{U}$ and ${}^{c}\mathbf{V}$ are equal (provided that $\det(\mathbf{U}) = 1$, otherwise they are opposites for any odd d).

Furthermore, the right term of (17) is very close to the left term of (2) when matching $\mathbf{Ue}_i$ and $\mathbf{Ue}_d$ with $\mathbf{b}$ and $\mathbf{a}$. Actually, ${}^{c}\mathbf{Ve}_i$ measures how far $\mathbf{Ue}_i$ is from $\mathbf{Ue}_d$. In particular, if $2\|\,{}^{c}\mathbf{Ve}_1\|_\infty < {}^{t}\mathbf{1}\mathbf{Ue}_d$, then $\mathbf{Ue}_i$ is an approximation of $\mathbf{Ue}_d$ provided that $\mathbf{Ue}_i, \mathbf{U}(\mathbf{e}_d - \mathbf{e}_i) \in \mathbb{N}^d \setminus \{\mathbf{0}\}$ is also true. By dividing both members of (17) by $\det(\mathbf{U})^{d-1}\left({}^{t}\mathbf{1}\mathbf{Ue}_d\right)$, we obtain

$$\forall i \in [\![1, d-1]\!], \frac{1}{\det(\mathbf{U})^{d-1}\left({}^{t}\mathbf{1}\mathbf{Ue}_d\right)}\,{}^{c}\mathbf{Ve}_i = \mathbf{Ue}_i - \frac{\left({}^{t}\mathbf{1}\mathbf{Ue}_i\right)}{\left({}^{t}\mathbf{1}\mathbf{Ue}_d\right)}\mathbf{Ue}_d.$$

The right member is the difference between $\mathbf{Ue}_i$ and its projection onto $\mathbf{Ue}_d$ done orthogonally to $\mathbf{1}$. This difference is actually equal to ${}^{c}\mathbf{Ve}_i$ up to a factor. Fig. 10 illustrates this relation. Note that the sign of the factor is negative if and only if $\det(\mathbf{U}) = -1$ and d is even.

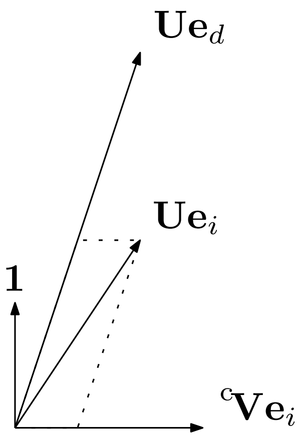


Figure 10: Geometrical interpretation of (17) and approximations.

The connection with approximations is also made explicit in the following existence result:

Lemma 9. *Let* $\mathbf{a} \in \mathbb{N}^d \setminus \{\mathbf{0}\}$ *be such that* $\gcd(\mathbf{a}) = 1$ *and* $\|\mathbf{a}\|_1 > 2^{d-1}$. *There exist an approximation* $\mathbf{b}$ *of* $\mathbf{a}$ *and a unimodular matrix* $\mathbf{U}$ *of size* $d \times d$ *such that* $\mathbf{Ue}_1 = \mathbf{b}$ *and* $\mathbf{Ue}_d = \mathbf{a}$.

Note that the two conditions involve specific columns of $\mathbf{U}$, namely the first and last one, but any other choice works as well by column permutation.

Proof. The set of all approximations of $\mathbf{a}$ is discrete, finite and, according to Lemma 2, not empty. In addition, by the very definition of approximation (Definition 2) and the hypothesis $\gcd(\mathbf{a}) = 1$, no approximation depends linearly on $\mathbf{a}$. Therefore, there must be an approximation $\mathbf{b}$ such that the convex hull of $\{\mathbf{0}, \mathbf{a}, \mathbf{b}\}$ does not contain any other approximations (see Fig. 11). Since every integer point lying in a certain convex region surrounding $\{\mathbf{0}, \mathbf{a}, \mathbf{b}\}$ is an approximation, the convex hull of these points does not contain any integer points other than $\mathbf{0}, \mathbf{a}$ and $\mathbf{b}$. By symmetry with respect to $\mathbf{a}/2$, the same is true for the convex hull of $\{\mathbf{0}, \mathbf{a}, \mathbf{a}-\mathbf{b}\}$ and the union of these two triangles, which together form the convex hull of $\{\mathbf{0}, \mathbf{a}, \mathbf{b}, \mathbf{a}-\mathbf{b}\}$, does not contain any integer points other than $\mathbf{0}, \mathbf{a}, \mathbf{b}$ and $\mathbf{a}-\mathbf{b}$. As a result, all integer points in the span of $\mathbf{a}$ and $\mathbf{b}$ are also in the 2-rank lattice generated by $\mathbf{a}$ and $\mathbf{b}$. Otherwise stated,

$$\forall(\alpha, \beta) \in \mathbb{R}^2,\ \alpha\mathbf{a} + \beta\mathbf{b} \in \mathbb{Z}^d \Rightarrow (\alpha, \beta) \in \mathbb{Z}^2.$$

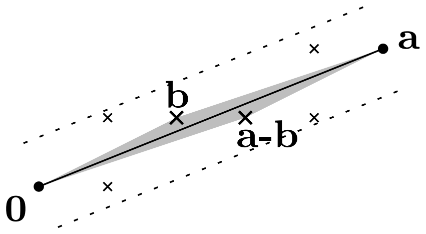


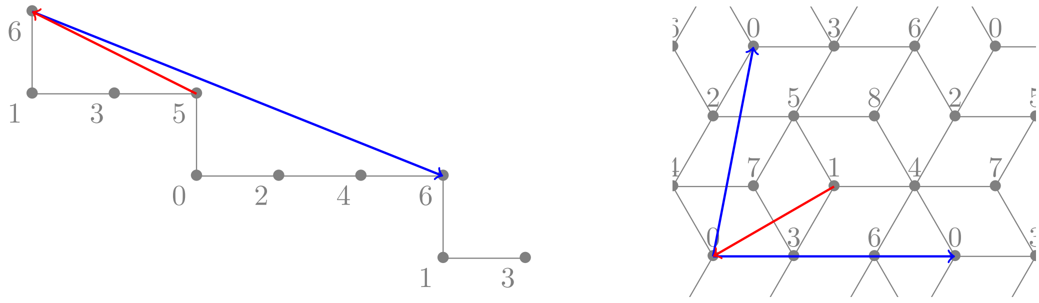
Figure 11: Two-dimensional illustration of the proof of Lemma 9. Approximations of $\mathbf{a}$, depicted with crosses, are integer points lying in a convex region, here bounded by dotted line segments. The convex hull of $\{\mathbf{0}, \mathbf{a}, \mathbf{b}, \mathbf{a}-\mathbf{b}\}$ does not contain any integer points other than its vertices.

By [28][Corollary 4.1.c and its proof], the above implies that there exists an $d \times d$ unimodular matrix $\mathbf{M}$ such that

$$\mathbf{M}[\mathbf{a}, \mathbf{b}] = \begin{pmatrix} \mathbf{I} \\ \mathbf{0} \end{pmatrix},$$

where the right member, known as the row-style Hermite Normal Form of $[\mathbf{a}, \mathbf{b}]$, is composed of a 2×2 identity matrix and zeros in the $d-2$ last rows. It follows that $\mathbf{M}^{-1}\mathbf{e}_1 = \mathbf{a}$, $\mathbf{M}^{-1}\mathbf{e}_2 = \mathbf{b}$ and $\mathbf{U}$ is obtained after two column permutations of $\mathbf{M}^{-1}$. □

To sum up, we use a unimodular matrix $\mathbf{U}$ whose last column is $\mathbf{a}$ and whose first column is $\mathbf{b}$, an approximation of $\mathbf{a}$. By the equality ${}^{t}\mathbf{U}\,{}^{c}\mathbf{U} = \pm\mathbf{I}$, the first $d-1$ columns of ${}^{c}\mathbf{U}$ are orthogonal to $\mathbf{a}$ and the d-th column of ${}^{c}\mathbf{U}$ has a scalar product equal to ± 1 with the vector $\mathbf{a}$, thus brings a point of height h to a point of height $h \pm 1$ (Fig. 12).



(a)

(b)

Figure 12: $\mathcal{P}(2,5)$ and $\mathcal{P}(2,3,4)$ are represented in (a) and (b) respectively, with the column vectors of ${}^{c}\mathbf{U}$ depicted with arrows. See the top and bottom rows of Table 2 to know what is ${}^{c}\mathbf{U}$ in (a) and (b) respectively.

In addition, by (15), the first $d-1$ columns of ${}^{c}\mathbf{V}$ are orthogonal to $\mathbf{1}$ and by (17), their l_∞-norms measure how far the first $d-1$ columns of $\mathbf{U}$ are from $\mathbf{a}$. Since the first column of $\mathbf{U}$ is an approximation of $\mathbf{a}$, the first column of ${}^{\mathrm{c}}\mathbf{V}$, i.e., ${}^{\mathrm{c}}\mathbf{V}\mathbf{e}_1$, is rather *short*, because its norm is bounded from above as follows: $2\| {}^{\mathrm{c}}\mathbf{V}\mathbf{e}_1\|_\infty < \|\mathbf{a}\|_1$.

5 Geometric Results

In this section, we propose a geometrical interpretation of the partitioning introduced in Section 3 (Definition 3), from which we can derive a bijective function acting on points.

To do so, we consider a unimodular matrix $\mathbf{U}$ and the associated matrix $\mathbf{V}$ defined as in the previous section. In order to simplify the notation, we denote by $\mathbf{b}, \mathbf{a}, \mathbf{t}_b, \mathbf{t}_a$ and $\mathbf{s}$, the column vectors $\mathbf{U}\mathbf{e}_1, \mathbf{U}\mathbf{e}_d, -{}^{\mathrm{c}}\mathbf{U}\mathbf{e}_1/\det(\mathbf{U}), {}^{\mathrm{c}}\mathbf{U}\mathbf{e}_d/\det(\mathbf{U})$ and $-{}^{\mathrm{c}}\mathbf{V}\mathbf{e}_1/\det(\mathbf{U})^{d-1}$, respectively. The factors are chosen so as to make positive all the scalar products involved in condition (22) below.

On one hand, (17) writes $\mathbf{s} = (\|\mathbf{b}\|_1\mathbf{a} - \|\mathbf{a}\|_1\mathbf{b})$ and on the other hand, using the relation (9), we have

$$\mathbf{a}\cdot\mathbf{t}_b = \big({}^{\mathrm{t}}\mathbf{e}_d\,{}^{\mathrm{t}}\mathbf{U}\,{}^{\mathrm{c}}\mathbf{U}\mathbf{e}_1\big)\big(-1/\det(\mathbf{U})\big) = 0, \tag{18}$$

$$\mathbf{b}\cdot\mathbf{t}_a = \big({}^{\mathrm{t}}\mathbf{e}_1\,{}^{\mathrm{t}}\mathbf{U}\,{}^{\mathrm{c}}\mathbf{U}\mathbf{e}_d\big)\big(1/\det(\mathbf{U})\big) = 0, \tag{19}$$

$$\mathbf{a}\cdot\mathbf{t}_a = \big({}^{\mathrm{t}}\mathbf{e}_d\,{}^{\mathrm{t}}\mathbf{U}\,{}^{\mathrm{c}}\mathbf{U}\mathbf{e}_d\big)\big(1/\det(\mathbf{U})\big) = 1, \tag{20}$$

$$\mathbf{b}\cdot\mathbf{t}_b = \big({}^{\mathrm{t}}\mathbf{e}_1\,{}^{\mathrm{t}}\mathbf{U}\,{}^{\mathrm{c}}\mathbf{U}\mathbf{e}_1\big)\big(-1/\det(\mathbf{U})\big) = -1. \tag{21}$$

Combining all previous results, we obtain

$$\mathbf{s}\cdot\mathbf{t}_b = (\|\mathbf{b}\|_1\mathbf{a} - \|\mathbf{a}\|_1\mathbf{b})\cdot\mathbf{t}_b = \|\mathbf{a}\|_1,$$
$$\mathbf{s}\cdot\mathbf{t}_a = (\|\mathbf{b}\|_1\mathbf{a} - \|\mathbf{a}\|_1\mathbf{b})\cdot\mathbf{t}_a = \|\mathbf{b}\|_1.$$

Now, let us consider the set of points $\mathbf{x}\in\mathcal{P}(\mathbf{a})$ such that

$$(\mathbf{s}\cdot\mathbf{x}) \bmod (\mathbf{s}\cdot\mathbf{t}_b) < (\mathbf{s}\cdot\mathbf{t}_a). \tag{22}$$

They are located in regularly-spaced strips orthogonal to $\mathbf{s}$ as shown in Fig. 13. The width of the periods is determined by the projection of $\mathbf{t}_b$ onto $\mathbf{s}$ and is equal to $\|\mathbf{a}\|_1$, while the width of the strips is determined by the projection of $\mathbf{t}_a$ onto $\mathbf{s}$ and is equal to $\|\mathbf{b}\|_1$.

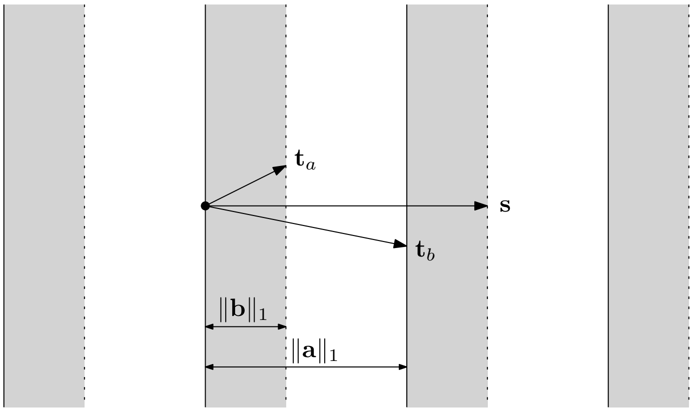


Figure 13: Geometrical interpretation of the partitioning, see (22).

Since $\mathbf{s}\cdot\mathbf{t}_b = \|\mathbf{a}\|_1$, $\mathbf{s}\cdot\mathbf{t}_a = \|\mathbf{b}\|_1$ and

$$\begin{aligned}\mathbf{s}\cdot\mathbf{x} \bmod \|\mathbf{a}\|_1 &= (\|\mathbf{b}\|_1\mathbf{a} - \|\mathbf{a}\|_1\mathbf{b})\cdot\mathbf{x} \bmod \|\mathbf{a}\|_1\\ &= (\mathbf{a}\cdot\mathbf{x})\|\mathbf{b}\|_1 \bmod \|\mathbf{a}\|_1,\end{aligned}$$

(22) is equivalent to $(\mathbf{a}\cdot\mathbf{x})\|\mathbf{b}\|_1 \bmod \|\mathbf{a}\|_1 < \|\mathbf{b}\|_1$, which is exactly the condition used in Definition 3, when matching $\mathbf{a}\cdot\mathbf{x}$, $\|\mathbf{b}\|_1$ and $\|\mathbf{a}\|_1$ with h, B and A, respectively. Fig. 13 therefore shows where are the points $\mathbf{x}\in\mathcal{P}(\mathbf{a})$ such that $\mathbf{a}\cdot\mathbf{x}$ belongs to $\mathcal{H}(\|\mathbf{a}\|_1, \|\mathbf{b}\|_1, 0)$. The use of a value distinct from 0 for parameter D in $\mathcal{H}(\|\mathbf{a}\|_1, \|\mathbf{b}\|_1, D)$, only adds an offset between the origin and the first strip.

Furthermore, we can derive a function that takes the strips as input and combines them together in order to cover the whole space as output. That geometrical function is based on a discrete function that numbers the periods. Then, the strips are translated by an amount that depends on the index of its period. More precisely, the strip of the k-th period is translated by $k(\mathbf{t}_a - \mathbf{t}_b)$: it is first translated by $-k\mathbf{t}_b$ to place it in the first period and it is then translated by $k\mathbf{t}_a$ to place it right after the first $k-1$ and previously-translated strips.

Note that we can number the periods by the following discrete function,

$$\left\lfloor \frac{\mathbf{s}\cdot\mathbf{x}}{\|\mathbf{a}\|_1} \right\rfloor = \left\lfloor \frac{(\mathbf{a}\cdot\mathbf{x})\|\mathbf{b}\|_1}{\|\mathbf{a}\|_1} - \mathbf{b}\cdot\mathbf{x} \right\rfloor = f(\|\mathbf{a}\|_1, \|\mathbf{b}\|_1, 0)\big(\mathbf{a}\cdot\mathbf{x}\big) - \mathbf{b}\cdot\mathbf{x},$$

where f is introduced in Definition 4. We thus propose the following

Definition 5. *Let $\mathbf{U}$ be a unimodular matrix of size $d \times d$ such that $\mathbf{a} := \mathbf{U}\mathbf{e}_1$ and $\mathbf{b} := \mathbf{U}\mathbf{e}_d$ are both in $\mathbb{N}^d \setminus \{\mathbf{0}\}$. Let $\mathbf{t}$ be equal to ${}^{c}\mathbf{U}(\mathbf{e}_1 + \mathbf{e}_d)/\det(\mathbf{U})$ and $D \in \mathbb{Z}$ be any integer. Let f, f' be defined as in Definition 4.*

Function $g(\mathbf{U}, D) : \mathbb{Z}^d \mapsto \mathbb{Z}^d$ is defined such that

$$g(\mathbf{U}, D)(\mathbf{x}) := \mathbf{x} + \mathbf{t}\big(f(\|\mathbf{a}\|_1, \|\mathbf{b}\|_1, D)(\mathbf{a}\cdot\mathbf{x}) - \mathbf{b}\cdot\mathbf{x}\big), \tag{23}$$

and function $g'(\mathbf{U}, D) : \mathbb{Z}^d \mapsto \mathbb{Z}^d$ such that

$$g'(\mathbf{U}, D)(\mathbf{x}) := \mathbf{x} + \mathbf{t}\big(f'(\|\mathbf{a}\|_1, \|\mathbf{b}\|_1, D)(\mathbf{b}\cdot\mathbf{x}) - \mathbf{a}\cdot\mathbf{x}\big). \tag{24}$$

To simplify the notation, we will write in the sequel $f(h)$ instead of $f(\|\mathbf{a}\|_1, \|\mathbf{b}\|_1, D)(h)$, $g(\mathbf{x})$ instead of $g(\mathbf{U}, D)(\mathbf{x})$ and similarly for f' and g'.

Using Lemma 4, we show below that g is indeed bijective and that the inverse is g'.

Lemma 10. *Let $\mathbf{U}$ be a unimodular matrix of size $d \times d$ such that $\mathbf{a} := \mathbf{U}\mathbf{e}_1$ and $\mathbf{b} := \mathbf{U}\mathbf{e}_d$ are both in $\mathbb{N}^d \setminus \{\mathbf{0}\}$. Let $D \in \mathbb{Z}$ be any integer. Let $\mathcal{H}, g, g'$ be defined as in Definitions 3 and 5. For all $\mathbf{x} \in \mathcal{P}(\mathbf{a})$ such that $\mathbf{a}\cdot\mathbf{x} \in \mathcal{H}(\|\mathbf{a}\|_1, \|\mathbf{b}\|_1, D)$, $g'\big(g(\mathbf{x})\big) = \mathbf{x}$ and $g\big(g'(\mathbf{x})\big) = \mathbf{x}$.*

Proof. As previously, we introduce the following notation: $\mathbf{t}_b := -{}^{c}\mathbf{U}\mathbf{e}_1/\det(\mathbf{U})$, $\mathbf{t}_a := {}^{c}\mathbf{U}\mathbf{e}_d/\det(\mathbf{U})$ and $\mathbf{t} := \mathbf{t}_a - \mathbf{t}_b = {}^{c}\mathbf{U}(\mathbf{e}_1 + \mathbf{e}_d)/\det(\mathbf{U})$.

By (18), (19), (20) and (21), we have $\mathbf{a}\cdot\mathbf{t} = \mathbf{b}\cdot\mathbf{t} = 1$, which leads to the following equalities:

$$\mathbf{b}\cdot g(\mathbf{x}) = (\mathbf{b}\cdot\mathbf{x}) + (\mathbf{b}\cdot\mathbf{t})\big(f(\mathbf{a}\cdot\mathbf{x}) - \mathbf{b}\cdot\mathbf{x}\big) = f(\mathbf{a}\cdot\mathbf{x}), \tag{25}$$

$$\mathbf{a}\cdot g'(\mathbf{x}) = (\mathbf{a}\cdot\mathbf{x}) + (\mathbf{a}\cdot\mathbf{t})\big(f'(\mathbf{b}\cdot\mathbf{x}) - \mathbf{a}\cdot\mathbf{x}\big) = f'(\mathbf{b}\cdot\mathbf{x}), \tag{26}$$

$$\mathbf{a}\cdot g(\mathbf{x}) = (\mathbf{a}\cdot\mathbf{x}) + (\mathbf{a}\cdot\mathbf{t})\big(f(\mathbf{a}\cdot\mathbf{x}) - \mathbf{b}\cdot\mathbf{x}\big) = f(\mathbf{a}\cdot\mathbf{x}) + \mathbf{a}\cdot\mathbf{x} - \mathbf{b}\cdot\mathbf{x}, \tag{27}$$

$$\mathbf{b}\cdot g'(\mathbf{x}) = (\mathbf{b}\cdot\mathbf{x}) + (\mathbf{b}\cdot\mathbf{t})\big(f'(\mathbf{b}\cdot\mathbf{x}) - \mathbf{a}\cdot\mathbf{x}\big) = f'(\mathbf{b}\cdot\mathbf{x}) + \mathbf{b}\cdot\mathbf{x} - \mathbf{a}\cdot\mathbf{x}. \tag{28}$$

From there, we simplify

$$g'\big(g(\mathbf{x})\big) = g(\mathbf{x}) + \mathbf{t}\big(f'\big(\mathbf{b}\cdot g(\mathbf{x})\big) - \mathbf{a}\cdot g(\mathbf{x})\big)$$

as follows:

- $g(\mathbf{x}) = \mathbf{x} + \mathbf{t}\big(f(\mathbf{a}\cdot\mathbf{x}) - \mathbf{b}\cdot\mathbf{x}\big)$ by definition,
- $f'\big(\mathbf{b}\cdot g(\mathbf{x})\big) = f'\big(f(\mathbf{a}\cdot\mathbf{x})\big) = \mathbf{a}\cdot\mathbf{x}$ by (25) and Lemma 4,
- $-\mathbf{a}\cdot g(\mathbf{x}) = -f(\mathbf{a}\cdot\mathbf{x}) - \mathbf{a}\cdot\mathbf{x} + \mathbf{b}\cdot\mathbf{x}$ by (27).

Putting all together, we obtain

$$g'\big(g(\mathbf{x})\big) = \mathbf{x} + \mathbf{t}\big(f(\mathbf{a}\cdot\mathbf{x}) - \mathbf{b}\cdot\mathbf{x}\big) + \mathbf{t}\big(\mathbf{a}\cdot\mathbf{x} - f(\mathbf{a}\cdot\mathbf{x}) - \mathbf{a}\cdot\mathbf{x} + \mathbf{b}\cdot\mathbf{x}\big) = \mathbf{x}.$$

Similarly, we have

$$g\big(g'(\mathbf{x})\big) = g'(\mathbf{x}) + \mathbf{t}\big(f\big(\mathbf{a}\cdot g'(\mathbf{x})\big) - \mathbf{b}\cdot g'(\mathbf{x})\big)$$

and

- $g'(\mathbf{x}) = \mathbf{x} + \mathbf{t}\big(f'(\mathbf{b}\cdot\mathbf{x}) - \mathbf{a}\cdot\mathbf{x}\big)$ by definition,

- $f\big(\mathbf{a} \cdot g'(\mathbf{x})\big) = f\big(f'(\mathbf{b} \cdot \mathbf{x})\big) = \mathbf{b} \cdot \mathbf{x}$ by (26) and Lemma 4,
- $-\mathbf{b} \cdot g'(\mathbf{x}) = -f'(\mathbf{b} \cdot \mathbf{x}) - \mathbf{b} \cdot \mathbf{x} + \mathbf{a} \cdot \mathbf{x}$ by (28).

Putting all together, we obtain

$$g'\big(g(\mathbf{x})\big) = \mathbf{x} + \mathbf{t}\big(f'(\mathbf{b} \cdot \mathbf{x}) - \mathbf{a} \cdot \mathbf{x}\big) + \mathbf{t}\big(\mathbf{b} \cdot \mathbf{x} - f'(\mathbf{b} \cdot \mathbf{x}) - \mathbf{b} \cdot \mathbf{x} + \mathbf{a} \cdot \mathbf{x}\big) = \mathbf{x}.$$

□

Using Lemma 5, we show below that the image of g is equal to $\mathcal{P}(\mathbf{b})$ for specific values of D.

Lemma 11. *Let $\mathbf{U}$ be a unimodular matrix of size $d \times d$ such that $\mathbf{a} := \mathbf{U}\mathbf{e}_1$ and $\mathbf{b} := \mathbf{U}\mathbf{e}_d$ are both in $\mathbb{N}^d \setminus \{\mathbf{0}\}$. Let $D \in \mathbb{Z}$ be any integer. Let $\mathcal{H}, g$ be defined as in Definitions 3 and 5. For all $D \in \llbracket -\|\mathbf{b}\|_1 + 1, \|\mathbf{a}\|_1 - \|\mathbf{b}\|_1 \rrbracket$ and for all $\mathbf{x} \in \mathcal{P}(\mathbf{a})$ such that $\mathbf{a} \cdot \mathbf{x} \in \mathcal{H}(\|\mathbf{a}\|_1, \|\mathbf{b}\|_1, D)$, $g(\mathbf{x}) \in \mathcal{P}(\mathbf{b})$.*

Proof. By Lemma 5, we have for all $\mathbf{x} \in \mathcal{P}(\mathbf{a})$ such that $\mathbf{a} \cdot \mathbf{x} \in \mathcal{H}(\|\mathbf{a}\|_1, \|\mathbf{b}\|_1, D)$,

$$0 \leq f(\mathbf{a} \cdot \mathbf{x}) \leq \|\mathbf{b}\|_1 - 1,$$

where f is introduced in Definition 4.

By (25) and the very definition of discrete planes, the conclusion follows:

$$0 \leq \mathbf{b} \cdot g(\mathbf{x}) \leq \|\mathbf{b}\|_1 - 1. \text{ Therefore, } g(\mathbf{x}) \in \mathcal{P}(\mathbf{b}).$$

□

To sum up, the bijective function g, which acts on points, is consistent, by projection, with the bijective function f, which acts on heights (Fig. 14).

$$\begin{tikzcd}
\boxed{\mathcal{H}(\|\mathbf{a}\|_1, \|\mathbf{b}\|_1, D)} \arrow[r, bend left, "f"] & \boxed{\llbracket 0, \|\mathbf{b}\|_1 - 1 \rrbracket} \arrow[l, bend left, "f' = f^{-1}"] \\
\boxed{\{\mathbf{x} \in \mathcal{P}(\mathbf{a}) \mid \mathbf{a} \cdot \mathbf{x} \in \mathcal{H}(\|\mathbf{a}\|_1, \|\mathbf{b}\|_1, D)\}} \arrow[u, "\text{projection}"] \arrow[r, bend right, "g"'] & \boxed{\mathcal{P}(\mathbf{b})} \arrow[u] \arrow[l, bend right, "g' = g^{-1}"']
\end{tikzcd}$$

Figure 14: Domain and image of f and g (see Definitions 4 and 5).

Before proving our main result, note that functions g, g' are naturally extended to sets of points: the image of a set of points under these functions is the set of the images of the individual points.

Let us recall Theorem 1:

Theorem 1. *Let $\mathbf{a} \in \mathbb{N}^d \setminus \{\mathbf{0}\}$ be such that $\gcd(\mathbf{a}) = 1$ and $\|\mathbf{a}\|_1 > 2^{d-1}$. There exist two approximations $\mathbf{b}, \mathbf{c} \in \mathbb{N}^d$ of $\mathbf{a}$, two subsets $\mathcal{S}_b, \mathcal{S}_c \subset \mathcal{P}(\mathbf{a})$ and two bijective functions g_b, g_c such that $\mathbf{a} = \mathbf{b} + \mathbf{c}$, $\mathcal{P}(\mathbf{a}) = \mathcal{S}_b \cup \mathcal{S}_c$, $\emptyset = \mathcal{S}_b \cap \mathcal{S}_c$, $g(\mathcal{S}_b) = \mathcal{P}(\mathbf{b})$, $g(\mathcal{S}_c) = \mathcal{P}(\mathbf{c})$, and $\forall j \in \llbracket 1, d \rrbracket$,*

$$\begin{aligned}
\mathbf{x} \in \mathcal{S}_b \textit{ and } \mathbf{x} \pm \mathbf{e}_j \in \mathcal{P}(\mathbf{a}) &\Leftrightarrow\ g_b(\mathbf{x}), g_b(\mathbf{x}) \pm \mathbf{e}_j \in \mathcal{P}(\mathbf{b}), \\
\mathbf{x} \in \mathcal{S}_c \textit{ and } \mathbf{x} \pm \mathbf{e}_j \in \mathcal{P}(\mathbf{a}) &\Leftrightarrow\ g_c(\mathbf{x}), g_c(\mathbf{x}) \pm \mathbf{e}_j \in \mathcal{P}(\mathbf{c}).
\end{aligned}$$

Proof. By Lemma 2, there exists an approximation $\mathbf{b}$ of $\mathbf{a}$ (Definition 2). We can partition $\mathcal{P}(\mathbf{a})$ using $\mathcal{H}$ (Definition 3) and a parameter $D \in \mathbb{Z}$ to determine later:

$$\begin{aligned}\mathcal{S}_b &:= \{\mathbf{x} \in \mathcal{P}(\mathbf{a}) \mid \mathbf{a} \cdot \mathbf{x} \in \mathcal{H}(\|\mathbf{a}\|_1, \|\mathbf{b}\|_1, D)\},\\ \mathcal{S}_c &:= \{\mathbf{x} \in \mathcal{P}(\mathbf{a}) \mid \mathbf{a} \cdot \mathbf{x} \in \mathcal{H}(\|\mathbf{a}\|_1, \|\mathbf{a}\|_1 - \|\mathbf{b}\|_1, -D+1)\}.\end{aligned}$$

The fact that $\mathcal{S}_b$ and $\mathcal{S}_c$ partition $\mathcal{P}(\mathbf{a})$, i.e., $\mathcal{P}(\mathbf{a}) = \mathcal{S}_b \cup \mathcal{S}_c$ and $\emptyset = \mathcal{S}_b \cap \mathcal{S}_c$, straigthforwardly comes from Lemma 3.

By Lemma 9, there exists a unimodular matrix $\mathbf{U}$ such that $\mathbf{U}\mathbf{e}_1 = \mathbf{b}$, $\mathbf{U}\mathbf{e}_d = \mathbf{a}$. Let us set g_b to $g(\mathbf{U}, D)$ (Definition 5). The domain of g_b is exactly $\mathcal{S}_b$ by definition. It is bijective (Lemma 10) and, if $D \in [\![-\|\mathbf{b}\|_1 + 1, \|\mathbf{a}\|_1 - \|\mathbf{b}\|_1]\!]$, its image is $\mathcal{P}(\mathbf{b})$ (Lemma 11). In that case, we have thus

$$\mathbf{x} \in \mathcal{S}_b \Leftrightarrow g_b(\mathbf{x}) \in \mathcal{P}(\mathbf{b})$$

and it remains to check that the arrangement of edges incident to $\mathbf{x} \in \mathcal{S}_b$ in the adjacency graph associated to $\mathcal{P}(\mathbf{a})$ is equal to the arrangement of edges incident to $g_b(\mathbf{x})$ in the adjacency graph associated to $\mathcal{P}(\mathbf{b})$, i.e., for all $\mathbf{x} \in \mathcal{S}_b$ and all $j \in [\![1, d]\!]$,

$$\mathbf{x} \pm \mathbf{e}_j \in \mathcal{P}(\mathbf{a}) \Leftrightarrow g_b(\mathbf{x}) \pm \mathbf{e}_j \in \mathcal{P}(\mathbf{b}).$$

Focusing on the case $+\mathbf{e}_j$ and using the definition of discrete hyperplanes (Definition 1), this amounts to showing that for all $\mathbf{x} \in \mathcal{S}_b$ and all $j \in [\![1, d]\!]$,

$$\mathbf{a} \cdot \mathbf{x} \leq \|\mathbf{a}\|_1 - a_j - 1 \Leftrightarrow \mathbf{b} \cdot g_b(\mathbf{x}) \leq \|\mathbf{b}\|_1 - b_j - 1.$$

Let Q be equal to $\big\|\mathbf{a}\big(\|\mathbf{b}\|_1\big) - \mathbf{b}\big(\|\mathbf{a}\|_1\big)\big\|_\infty$. By (8) and the discussion that follows Corollary 7, for all $D \in [\![-\|\mathbf{b}\|_1 + 1 + Q, \|\mathbf{a}\|_1 - \|\mathbf{b}\|_1 - Q]\!]$ (the set is not empty), for all $\mathbf{x} \in \mathcal{S}_b$ and all $j \in [\![1, d]\!]$,

$$\mathbf{a} \cdot \mathbf{x} \leq \|\mathbf{a}\|_1 - a_j - 1 \Leftrightarrow f(\|\mathbf{a}\|_1, \|\mathbf{b}\|_1, D)(\mathbf{a} \cdot \mathbf{x}) \leq \|\mathbf{b}\|_1 - b_j - 1,$$

where f is introducted in Definition 4. By (25), we can replace $f(\|\mathbf{a}\|_1, \|\mathbf{b}\|_1, D)(\mathbf{a} \cdot \mathbf{x})$ by $\mathbf{b} \cdot g_b(\mathbf{x})$ to get the result.

For the opposite edges, we can apply the same line of reasoning, using (7) and $-\mathbf{e}_j$ instead of (8) and $+\mathbf{e}_j$.

To complete the proof, we set g_c to $g(\mathbf{U}', D')$, where $D' \in \mathbb{Z}$ is an integer to determine later and $\mathbf{U}'$ is obtained from $\mathbf{U}$ by replacing its first column by $\mathbf{c} := \mathbf{a} - \mathbf{b}$. Note that $\mathbf{U}'$ is unimodular since it is obtained from $\mathbf{U}$ by elementary column operations. In addition, $\mathbf{c}$ is an approximation of $\mathbf{a}$:

- $\gcd(\mathbf{c}) = 1$ because $\mathbf{U}'$ is unimodular,
- $\mathbf{c} = \mathbf{a} - \mathbf{b}, \mathbf{a} - \mathbf{c} = \mathbf{b} \in \mathbb{N}^d \setminus \{\mathbf{0}\}$ because $\mathbf{b}$ is an approximation of $\mathbf{a}$,
- $\Big\|\big(\|\mathbf{c}\|_1\big)\mathbf{a} - \big(\|\mathbf{a}\|_1\big)\mathbf{c}\Big\|_\infty < \frac{1}{2}\|\mathbf{a}\|_1$ because

$$\begin{aligned}\big(\|\mathbf{c}\|_1\big)\mathbf{a} - \big(\|\mathbf{a}\|_1\big)\mathbf{c} &= \big(\|\mathbf{a}\|_1 - \|\mathbf{b}\|_1\big)\mathbf{a} - \|\mathbf{a}\|_1(\mathbf{a} - \mathbf{b})\\ &= \big(\|\mathbf{a}\|_1\big)\mathbf{a} - \big(\|\mathbf{a}\|_1\big)\mathbf{a} - \big(\|\mathbf{b}\|_1\big)\mathbf{a} + \big(\|\mathbf{a}\|_1\big)\mathbf{b}\\ &= -\Big(\big(\|\mathbf{b}\|_1\big)\mathbf{a} - \big(\|\mathbf{a}\|_1\big)\mathbf{b}\Big)\end{aligned}$$

and

$$\Big\| - \Big(\big(\|\mathbf{b}\|_1\big)\mathbf{a} - \big(\|\mathbf{a}\|_1\big)\mathbf{b}\Big)\Big\|_\infty = \Big\|\big(\|\mathbf{b}\|_1\big)\mathbf{a} - \big(\|\mathbf{a}\|_1\big)\mathbf{b}\Big\|_\infty < \tfrac{1}{2}\|\mathbf{a}\|_1,$$

where we used (2) for the upper bound.

To be able to do for g_c, what we did for g_b, it is enough to check that we can choose a value for D' that is consistent with the one of D. On one hand, the definition of $\mathcal{S}_c$ implies that $D' = -D + 1$. On the other hand, D must belong to $[\![-\|\mathbf{b}\|_1 + 1 + Q, \|\mathbf{a}\|_1 - \|\mathbf{b}\|_1 - Q]\!]$, while D' must belong to $[\![-\|\mathbf{c}\|_1 + 1 + Q', \|\mathbf{a}\|_1 - \|\mathbf{c}\|_1 - Q']\!]$, where

$$Q' := \Big\|\big(\|\mathbf{c}\|_1\big)\mathbf{a} - \big(\|\mathbf{a}\|_1\big)\mathbf{c}\Big\|_\infty = \Big\|\big(\|\mathbf{b}\|_1\big)\mathbf{a} - \big(\|\mathbf{a}\|_1\big)\mathbf{b}\Big\|_\infty = Q.$$

We can indeed check that

$$D' = -D + 1 \in [\![-\|\mathbf{a}\|_1 + \|\mathbf{b}\|_1 + Q + 1, \|\mathbf{b}\|_1 - Q]\!],$$

where the interval is also equal to $[\![-\|\mathbf{c}\|_1 + 1 + Q', \|\mathbf{a}\|_1 - \|\mathbf{c}\|_1 - Q']\!]$, which concludes. □

6 Conclusion, Discussion, Perspectives

We have shown in Theorem 1 that for any $\mathbf{a}$ large enough, there are two approximations $\mathbf{b}, \mathbf{c}$ of $\mathbf{a}$, such that $\mathbf{a} = \mathbf{b} + \mathbf{c}$ and $\mathcal{P}(\mathbf{a})$ can be partitioned into two disjoint sets having respectively the combinatorial structure of $\mathcal{P}(\mathbf{b})$ and $\mathcal{P}(\mathbf{c})$.

Note that such partition does not exist for all $\mathbf{a}$. In particular, it may not exist for a too small $\mathbf{a}$, i.e., if $\|\mathbf{a}\|_1 \leq 2^{d-1}$. By enumeration over the finite set of vectors $\mathbf{a} \in \mathbb{N}^d \setminus \{\mathbf{0}\}$ such that $\|\mathbf{a}\|_1 \leq 2^{d-1}$, the list of the vectors that has no approximation can be exhibited in small dimension: they are, up to a permutation of the coordinates, $(0,1)$, $(1,1)$ in 2d (Fig. 15) and $(0,0,1)$, $(0,1,1)$, $(1,1,1)$, $(1,1,2)$ in 3d (Fig. 16).

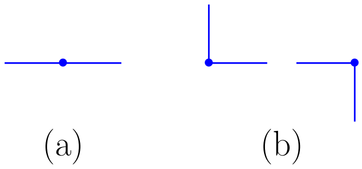


Figure 15: Arrangements of incident edges in the discrete lines of normal $(0,1)$ (a) and $(1,1)$ (b). Those discrete lines cannot be decomposed according to our criterion, because their arrangements of incident edges are not present in other discrete lines of shorter normal vectors.

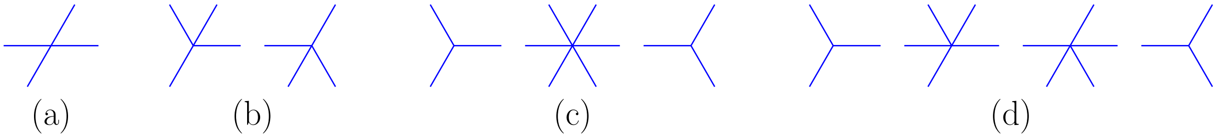
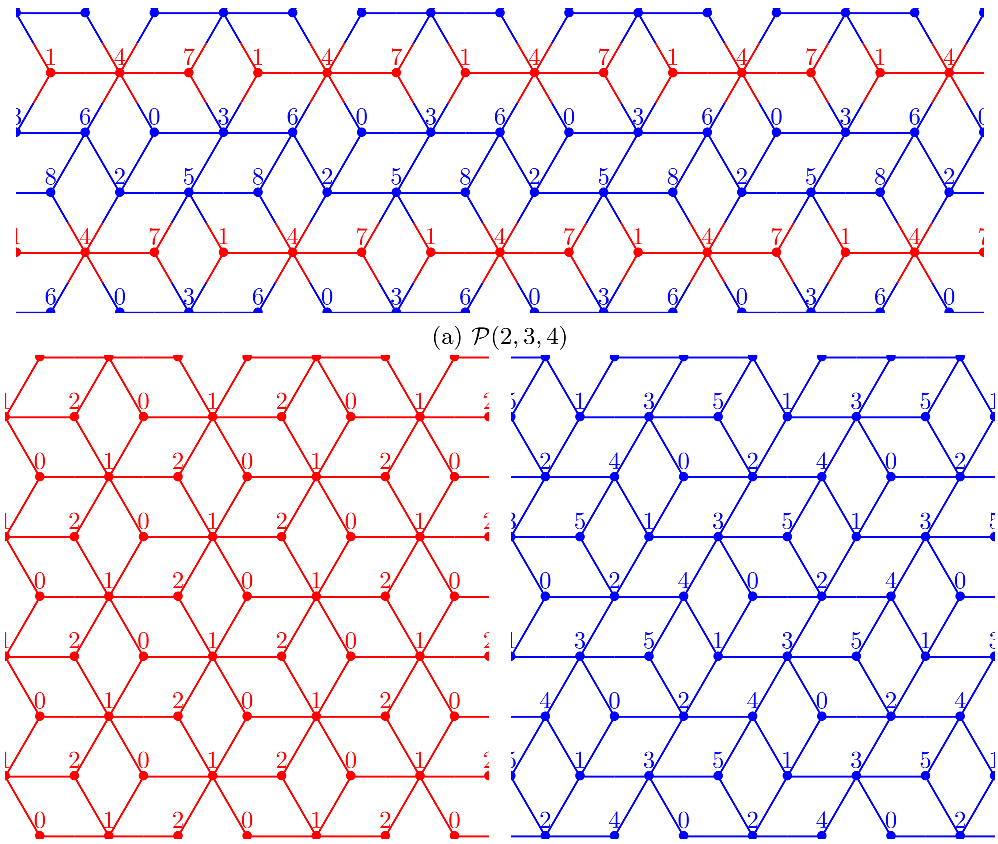


Figure 16: Arrangements of incident edges in the discrete planes of normal $(0,0,1)$ (a), $(0,1,1)$ (b), $(1,1,1)$ (c), $(1,1,2)$ (d). Those discrete planes cannot be decomposed according to our criterion, because their arrangements of incident edges are not present in other discrete planes of shorter normal vectors.

Note also that our partition is generally not unique for two main reasons. On one hand, there may be more than two approximations when $d \geq 3$. For example, $(1,1,1)$, $(1,1,2)$, $(1,2,2)$, $(1,2,3)$ are all approximations of $(2,3,4)$ (compare Fig. 4 with Fig. 17).

On the other hand, for each pair of approximations, there may be several possible values for the offset parameter D (Fig. 18).

Contrary to the previous works based on a geometrical extension of substitutions (see, e.g., [16, 9, 10, 25]), our approach has several interesting features. It is based on a representation of discrete hyperplanes as sets of points (Definition 1), instead of sets of $(d-1)$-dimensional faces, which is simpler and more common in discrete geometry. It relies on the notion of approximations (Definition 2) and does not depend on a multidimensional continued fraction algorithm such as Jacobi-Perron [16] or Brun [10]. Our approach also relies on an explicit and easily interpretable floor function (Definitions 4 and 5), instead of a discretization mechanism, which is implicitly described by a substitution and prone to fractal effects. Finally, it guarantees a strong combinatorial property involving the arrangements of edges incident to every nodes in the adjacency graphs. This explains why there are a few cases for which there is no decomposition in our approach, while a decomposition always exists with the substitution-based approach. For example, consider a straight line of normal $(1,1)$. It can be represented as an alternated sequence of horizontal and vertical unit straight segments. There are 90-degree corners between two consecutive unit straight segments. It can be decomposed into horizontal $(0,1)$ and vertical $(1,0)$ lines with the substitution-based approach. However, since there is no corner in the horizontal and vertical lines, this decomposition does not preserve the arrangements of incident edges as it is required in our approach (Fig. 15). It is not clear yet, if that requirement is an advantage or a disadvantage for the future applications, but in the latter case, it would be easy to remove the undesired constraints and adapt our results.

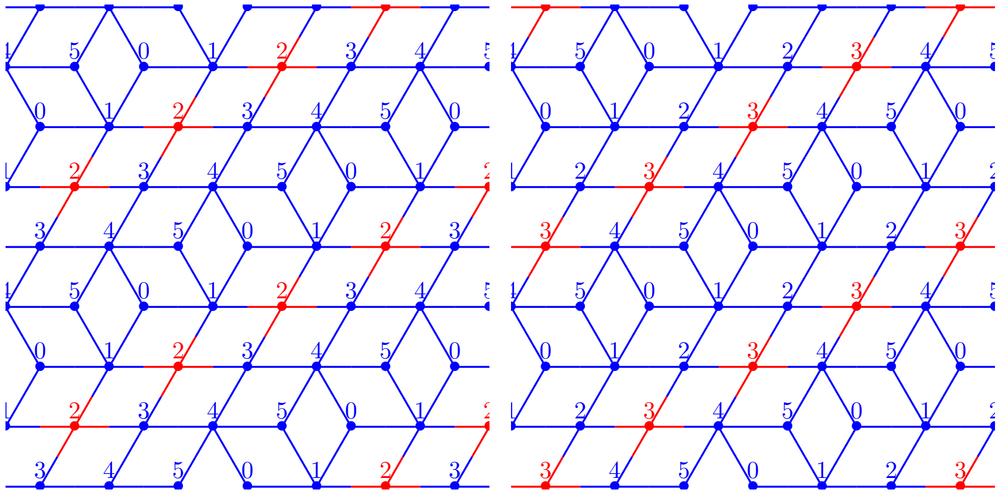


(a) $\mathcal{P}(2,3,4)$

(b) $\mathcal{P}(1,1,2)$

(c) $\mathcal{P}(1,2,2)$

Figure 17: Decomposition of $\mathcal{P}(2,3,4)$ using the approximations $(1,1,1)$ and $(1,2,3)$. The arrangements of edges in the red (resp. blue) set match those of $\mathcal{P}(1,1,1)$ (resp. $\mathcal{P}(1,2,3)$).



(a)

(b)

Figure 18: Two decompositions of $\mathcal{P}(1,1,4)$ using the approximations $(0,0,1)$ and $(1,1,3)$. The height of the points of the red set belongs to $\mathcal{H}(6,1,2)$ in (a), but $\mathcal{H}(6,1,3)$ in (b) (Definition 3).

A short-term perspective is to design an efficient algorithm to compute the required matrix from the input vector $\mathbf{a}$. Even if the proofs of Lemmas 2 and 9 are not totally constructive, they provide hints on how it can be done. A first approach consists in finding an approximation $\mathbf{b}$ by a brute-force search and then, computing the Hermite Normal Form of $[\mathbf{a}, \mathbf{b}]$ (see, e.g., [28, Section 5.3], [5, Algorithm 2.4.5]). Another approach consists in first computing a unimodular matrix $\mathbf{M}$ such that $\mathbf{M}\mathbf{e}_d = \mathbf{a}$ from the Hermite Normal Form of $\mathbf{a}$ only, then finding an approximation as a linear combination with integer coefficients of the first $d - 1$ columns of $\mathbf{M}$. For this task, one may use a lattice basis reduction in infinity norm (see the end of Section 4). This is not so easy in arbitrary dimension, but in dimension three, the lattice has rank two, and the lattice basis reduction can be done efficiently, even in the l_∞-norm [17]. The only challenge is to limit the size of the involved integers during the whole computation. However, it is certainly possible to work modulo a well-chosen integer.

Building on that, another perspective is to design algorithms that recursively decompose a given discrete plane into building blocks or, conversely, generate the discrete plane defined by a given normal vector from the same building blocks. That kind of algorithms can be translated into plane-probing algorithms, because a similar link has been shown with the substitution-based approach [25]. With these algorithmic tools in hand, it would then be possible to look at the problem of decomposing boundaries of 3d discrete sets into planar patches with fresh eyes.

References

[1] J. Berstel, A. Lauve, C. Reutenauer, and F. Saliola. *Combinatorics on Words: Christoffel Words and Repetition in Words.* American Mathematical Society, 2008.

[2] V. Brimkov, D. Coeurjolly, and R. Klette. Digital planarity – a review. *Discret. Appl. Math.*, 155(4):468–495, 2007.

[3] D. Coeurjolly and V. Brimkov. Computational aspects of digital plane and hyperplane recognition. In R. Reulke, U. Eckardt, B. Flach, U. Knauer, and K. Polthier, editors, *Combinatorial Image Analysis*, pages 291–306, Berlin, Heidelberg, 2006. Springer Berlin Heidelberg.

[4] D. Coeurjolly and R. Klette. A comparative evaluation of length estimators of digital curves. *IEEE Trans. Pattern Anal. Mach. Intell.*, 26(2):252–8, feb 2004.

[5] H. Cohen. *A Course in Computational Algebraic Number Theory.* Springer, 2010.

[6] I. Debled-Rennesson, J.-L. Rémy, and J. Rouyer-Degli. Detection of the Discrete Convexity of Polyominoes. *Discrete Applied Mathematics*, 125:115–133, 2003.

[7] I. Debled-Rennesson and J.-P. Reveillès. A linear algorithm for segmentation of digital curves. *International Journal of Pattern Recognition and Artificial Intelligence*, 9(4):635–662, 1995.

[8] H. Dorksen-Reiter and I. Debled-Rennesson. Convex and concave parts of digital curves. In *Geometric Properties from Incomplete Data*, volume 31 of *Computational Imaging and Vision*, pages 145–159. Springer, 2006.

[9] T. Fernique. Multidimensional Sturmian Sequences and Generalized Substitutions. *International Journal of Foundations of Computer Science*, 17:575–600, 2006.

[10] T. Fernique. Generation and recognition of digital planes using multi-dimensional continued fractions. *Pattern Recognition*, 42(10):2229–2238, 2009.

[11] F. Feschet. Canonical representations of discrete curves. *Pattern Analysis and Applications*, 8(1):84–94, 2005.

[12] F. Feschet and L. Tougne. Optimal time computation of the tangent of a discrete curve: Application to the curvature. In *8-th International Conference on Discrete Geometry for Computer Imagery*, volume 1568 of *Lecture Notes on Computer Science*, pages 31–40. Springer, 1999.

[13] F. Feschet and L. Tougne. On the Min DSS problem of closed discrete curves. *Discrete Applied Mathematics*, 151(1-3):138–153, 2005.

[14] J. Françon. Sur la topologie d'un plan arithmétique. *Theoretical Computer Science*, 156(1):159–176, 1996.

[15] M. Grötschel, L. Lovász, and A. Schrijver. *Geometric algorithms and combinatorial optimization.* Springer-Verlag, Berlin, 1993.

[16] S. Ito and M. Ohtsuki. Parallelogram tilings and Jacobi-Perron algorithm. *Tokyo Journal of Mathematics*, 17:33–58, 1994.

[17] M. Kaib and C. P. Schnorr. The generalized gauss reduction algorithm. *Journal of Algorithms*, 21(3):565–578, 1996.

[18] B. Kerautret and J.-O. Lachaud. Meaningful scales detection along digital contours for unsupervised local noise estimation. *IEEE Trans. Pattern Anal. Mach. Intell.*, 34(12):2379–2392, 2012.

[19] V. A. Kovalevsky. New definition and fast recognition of digital straight segments and arcs. In *Tenth International Conference on Pattern Analysis and Pattern Recognition*, pages 31–34, 1990.

[20] J.-O. Lachaud. Digital shape analysis with maximal segments. In *Applications of Discrete Geometry and Mathematical Morphology*, pages 14–27, 2012.

[21] J.-O. Lachaud, A. Vialard, and F. de Vieilleville. Fast, accurate and convergent tangent estimation on digital contours. *Image and Vision Computing*, 25(10):1572–1587, 2007.

[22] P. McMullen. Volumes of Projections of unit Cubes. *Bulletin of the London Mathematical Society*, 16(3):278–280, 1984.

[23] X. Provencal and J.-O. Lachaud. Two linear-time algorithms for computing the minimum length polygon of a digital contour. In *15-th IAPR International Conference on Discrete Geometry for Computer Imagery*, volume 5810 of *Lecture Notes on Computer Science*, pages 104–117. Springer, 2009.

[24] J.-P. Reveillès. *Géométrie Discrète, calculs en nombres entiers et algorithmique.* Thèse d'etat, Université Louis Pasteur, 1991.

[25] T. Roussillon. Combinatorial Generation of Planar Sets. *Journal of Mathematical Imaging and Vision*, 65(5):702–717, July 2023.

[26] T. Roussillon and S. Labbé. Decomposition of rational discrete planes. In S. Brunetti, A. Frosini, and S. Rinaldi, editors, *Discrete Geometry and Mathematical Morphology*, pages 54–66, Cham, 2024. Springer Nature Switzerland.

[27] T. Roussillon and I. Sivignon. Faithful polygonal representation of the convex and concave parts of a digital curve. *Pattern Recognition*, 44(10-11):2693–2700, oct 2011.

[28] A. Schrijver. *Theory of linear and integer programming.* John Wiley & Sons, Inc., USA, 1986.

[29] G. A. F. Seber. *A Matrix Handbook for Statisticians.* Wiley-Interscience, Hoboken, NJ, 2008.

[30] M. Senechal. *Quasicrystals and geometry.* Cambridge University Press, 1995.

[31] K. Voss. *Discrete Images, Objects, and Functions in Zn.* Springer-Verlag, 1993.