ALGEBRAIC ASPECTS OF DISCRETE TOMOGRAPHY

L. Hajdu and R. Tijdeman

Let A be a finite subset of $\mathbb{Z}^l$. We consider the problem of reconstructing a function $f: A \to \{0,1\}$ if all the line sums in finitely many directions are given. In Theorem 1 we give a complete characterization of the switching components, the functions $g: A \to \mathbb{Z}$ having zero line sums in these directions. Theorem 2 provides an algorithm for finding a function $g: A \to \mathbb{Z}$ having the same line sums as f in these directions such that $|f(x)-g(x)|$ is bounded on average by a number depending only on the number of directions.

1. Introduction

Discrete tomography is a subject of current interest (see [6] for the most recent progress). The main problem is to reconstruct a function $f: A \to \{0,1\}$ where A is a finite subset of $\mathbb{Z}^l$ ($l \geq 2$), if the sums of the function values along all the lines in a finite number of directions are given (the so-called X-rays). For the convenience of the reader we restrict ourselves to the case $l = 2$, but the developed theory can be extended without trouble to any dimension. For $l = 2$ a typical problem is as follows.

Problem 1. *Let k, m, n be integers greater than 1. Let $A = \{(i,j) \in \mathbb{Z}^2 : 0 \leq i < m, 0 \leq j < n\}$ and $f: A \to \{0,1\}$. Let $\{(a_d, b_d)\}_{d=1}^k$ be a set of pairs of coprime integers. Suppose f is unknown, but all the line sums $\sum_{a_d j = b_d i + t} f(i,j)$ (taken over $(i,j) \in A$) are given for $d = 1, \ldots, k$ and $t \in \mathbb{Z}$. Construct a function $g: A \to \{0,1\}$ such that*

$$\sum_{a_d j = b_d i + t} f(i,j) = \sum_{a_d j = b_d i + t} g(i,j) \quad \text{for } d = 1, \ldots, k \text{ and } t \in \mathbb{Z}. \tag{1}$$

For $k > 2$ the problem is NP-equivalent (see [5]). One way of dealing with the problem is to impose extra conditions on the set $A_1 = \{(i,j) \in A : f(i,j) = 1\}$, e.g. connectedness or convexity. Results of this kind are for example given in [1] and [4]. Another way of modifying the problem is to look for functions g which are good approximations to f in some sense. So Gritzmann (oral communication) asked for an algorithm which determines a function $g: A \to \mathbb{Z}$ satisfying (1) such

Mathematics Subject Classification: 92C55 (15A36).

The research of the first author was supported in part by the Hungarian Academy of Sciences and by Grants 023800 and T29330 from the Hungarian National Foundation for Scientific Research.

that $|f(i,j)-g(i,j)|$ is bounded by a number depending only on k for all $(i,j)\in A$. In Corollary 3 we provide an algorithm which does so at least in average.

In the present paper we shall analyze the structure of the set of solutions g satisfying (1). It is easy to construct functions $f:\ A\to\{0,1\}$ which are uniquely determined by their line sums in one direction, but there are also sets of line sums for which the number of solutions $g:\ A\to\{0,1\}$ satisfying (1) grows exponentially in m and n. In the literature there is the notion of switching component which under suitable conditions enables one to change one solution of Problem 1 to another. To understand the structure of switching components, it is useful to consider the following more general problem.

Problem 2. *Let $m,n,A,\{(a_d,b_d)\}_{d=1}^k$ be as in Problem 1. Suppose $f:\ A\to\mathbb{Z}$ is unknown, but all the line sums $\sum_{\substack{a_dj=b_di+t\\(i,j)\in A}} f(i,j)$ are given for $d=1,\dots,k$ and $t\in\mathbb{Z}$.*
Construct a function $g:\ A\to\mathbb{Z}$ such that (1) *holds and*

$$\sum_{(i,j)\in A} g(i,j)^2 \quad \textit{is minimal.}$$

Suppose $f:\ A\to\{0,1\}$. Then

$$\sum_{(i,j)\in A} f(i,j)^2=\sum_{(i,j)\in A} f(i,j)=\sum_{(i,j)\in A} g(i,j)\le \sum_{(i,j)\in A} g(i,j)^2$$

with equality if and only if $g:\ A\to\{0,1\}$. Hence the minimum is realized if and only if g is a solution to Problem 1. Therefore Problem 2 is a generalization of Problem 1.

In order to deal with Problem 2 we introduce the generating function $f(x,y)=\sum_{(i,j)\in A} f(i,j)x^iy^j$. Then the set of line sums in the direction (a,b) is determined by the remainder when $f(x,y)$ is divided by x^ay^b-1 if $a\ge 0,b>0$ and by x^a-y^{-b} if $a>0,b\le 0$. This fact enables us to describe a basis for the switching components. The description gives an answer to a problem posed by R. J. Gardner (oral communication) that switching components are linear combinations of projections of polytopes. Theorem 1 gives a complete characterization of the functions $g:\ A\to\mathbb{Z}$ having zero line sums in the directions $\{(a_d,b_d)\}_{d=1}^k$. In Corollary 1 we precisely indicate the freedom which is left to be able to construct a function $g:\ A\to\mathbb{Z}$ which has the same line sums in these directions as some given $f:\ A\to\mathbb{Z}$. In Corollary 2 we give the degree of freedom as a simple expression of the numbers a_d,b_d. As an illustration of the theory, we explicitly compute the seven dependencies for the standard case of directions $\{(1,0),(0,1),(1,1),(1,-1)\}$.

Finally we use the theory to obtain a polynomial-time algorithm for finding an approximation to f having the required line sums. We first compute a function $q:\ A\to\mathbb{Q}$ having the same line sums as f in the given directions by solving a system of linear equations. Subsequently we use the structure of switching components to find a function $g:\ A\to\mathbb{Z}$ which is not far from q and f. The general result is given in Theorem 2. It follows from Corollary 3 that the algorithm provides a solution $g:\ A\to\mathbb{Z}$ satisfying (1) with $|g(i,j)|\le 2^{k-1}+1$ on average. We expect that the function obtained by replacing all function values of q which are greater than $1/2$ by 1 and all others by 0 provides a good first approximation to f in practice.

2. Definitions and notation

Let $a, b \in \mathbb{Z}$ with $\gcd(a,b) = 1$ and $a \geq 0$. We call (a,b) a direction. Put

$$f_{(a,b)}(x,y) = \begin{cases} x^a y^b - 1, & \text{if } a > 0,\ b > 0, \\ x^a - y^{-b}, & \text{if } a > 0,\ b < 0, \\ x - 1, & \text{if } a = 1,\ b = 0, \\ y - 1, & \text{if } a = 0,\ b = 1. \end{cases}$$

By lines with direction (a,b) we mean lines of the form $ay = bx + t$ ($t \in \mathbb{Z}$) in the (x,y) plane.

Let $m, n \in \mathbb{N}$ and $A = \{(i,j) \in \mathbb{Z}^2 \ : \ 0 \leq i < m, 0 \leq j < n\}$. We call the elements of A squares. From now on let R denote a commutative ring. If $g : A \to R$ is a function, then the line sum of g along the line $ay = bx + t$ is defined as $\sum_{\substack{aj = bi + t \\ (i,j) \in A}} g(i,j)$.

It is clear that a function v defined on A can be considered as a vector (an mn-tuple). If we want to emphasize this, we write $\vec{v}$ instead of v. We always assume that the entries of these vectors are arranged according to squares of A in lexicographical order. If $R \subseteq \mathbb{R}$, the length of $\vec{v}$ (or v) is $|v| = |\vec{v}| = \sqrt{\sum_{(i,j) \in A} v(i,j)^2}$.

A set $S = \{(a_d, b_d)\}_{d=1}^k$ of directions is called valid for A, if $\sum_{d=1}^k a_d < m$ and $\sum_{d=1}^k |b_d| < n$. Suppose $S = \{(a_d, b_d)\}_{d=1}^k$ is a valid set of directions for A. Put $F_S(x,y) = \prod_{d=1}^k f_{(a_d,b_d)}(x,y)$ and $F_{(u,v;S)}(x,y) = x^u y^v F_S(x,y)$ for $0 \leq u < m - \sum_{d=1}^k a_d$ and $0 \leq v < n - \sum_{d=1}^k |b_d|$. For these values of u and v define the functions $m_{(u,v;S)} : A \to R$ by

$$m_{(u,v;S)}(i,j) = \text{coeff}(x^i y^j) \text{ in } F_{(u,v;S)}(x,y) \ \text{ for } (i,j) \in A.$$

The $m_{(u,v;S)}$'s are called the switching elements corresponding to the direction set S. By the bottom-left corner of the switching element $m_{(0,0;S)}$ we mean the square (i^*, j^*) for which $m_{(0,0;S)}(i^*, j^*) \neq 0$, but $m_{(0,0;S)}(i,j) = 0$, whenever $i < i^*$ or $i = i^*$, $j < j^*$. Observe that (i^*, j^*) is lexicographically the first square of A for which the function value of $m_{(0,0;S)}$ is nonzero. It follows from the definitions of $f_{(a,b)}$ and F_S that if $a_0 = \sum_{b_d < 0} a_d$, then

$$m_{(0,0;S)}(i^*, j^*) = \text{coeff}(x^{a_0}) \text{ in } F_S(x,y) = \pm 1.$$

Since it corresponds with the bottom-left corner of $m_{(0,0;S)}$, for every u and v we define the bottom-left corner of $m_{(u,v;S)}$ as $(i^* + u, j^* + v)$. Again, the bottom-left corner of $m_{(u,v;S)}$ is lexicographically the first square of A for which the function value of $m_{(u,v;S)}$ is nonzero, and we also have

$$m_{(u,v;S)}(i^* + u, j^* + v) = \pm 1.$$

3. New results

Theorem 1. *Let $m, n \in \mathbb{N}$, $A = \{(i,j) \in \mathbb{Z}^2 \ : \ 0 \le i < m, 0 \le j < n\}$ and $S = \{(a_d, b_d)\}_{d=1}^k$ a valid set of directions for A. Put $M = \sum_{d=1}^k a_d$, $N = \sum_{d=1}^k |b_d|$. Let R be an integral domain such that $R[x,y]$ is a unique factorization domain. Then any function $g : A \to R$ with zero line sums along the lines corresponding to S can be uniquely written in the form*

$$g = \sum_{u=0}^{m-1-M} \sum_{v=0}^{n-1-N} c_{uv} m_{(u,v;S)}$$

with $c_{uv} \in R$. Moreover, every such function g has zero line sums along the lines corresponding to S.

Remark 1. In Theorem 1, R can be chosen as $\mathbb{Z}$ or any field.

Remark 2. The functions g as in Theorem 1 correspond to the switching components from Definition 2.3.1 of [3]. Theorem 1 shows that every switching component is a linear combination of switching elements. R. J. Gardner (oral communication) posed the problem of understanding the structure of switching components. By the fact that F_S is the product of k binomials, we can consider $m_{(u,v;S)}$ as the projection of a k-dimensional hypercube such that every edge of it has a vertex with value 1 and a vertex with value -1, and that values are added if the projections of vertices coincide. In this sense Theorem 1 provides a solution to Gardner's problem.

The following results are consequences of Theorem 1.

Corollary 1. *Let A, S and R be as in Theorem 1. Let L be the set of those squares of A which are the bottom-left corners of the switching elements. Then for any $f : A \to R$ and for any prescribed values from R for the squares of L, there exists a unique $g : A \to R$ having the prescribed values at the squares of L and having the same line sums as f along the lines corresponding to S.*

Corollary 2. *Let A, S and R be as in Theorem 1. Then there are exactly*

$$\sum_{d=1}^k a_d \sum_{d=1}^k |b_d| - \sum_{d=1}^k a_d |b_d|$$

linearly independent homogeneous linear dependencies among the line sums.

Remark 3. We shall explicitly give the seven dependence relations in case $k = 4$, $S = \{(1,0),(0,1),(1,1),(1,-1)\}$ after the proof of Corollary 2.

Theorem 2. *Let A, k and S be as in Theorem 1. Let all the line sums in the directions of S of some unknown function $f : A \to \mathbb{Z}$ be given. Then there exists an algorithm which is polynomial in $\max\{m,n\}$, providing a function $g : A \to \mathbb{Z}$ such that f and g have the same line sums corresponding to S, and that*

$$|g| \le |f| + 2^{k-1}\sqrt{mn}. \tag{2}$$

Corollary 3. *In the special case $f : A \to \{0,1\}$ we may replace (2) by*

$$|g| \le (2^{k-1} + 1)\sqrt{mn}.$$

4. Proofs

To prove Theorem 1, we need the following result.

Lemma. *Let A be as in Theorem 1, (a,b) be a valid direction for A and $g: A \to R$, where R is a commutative ring. Then g has zero line sums along the lines with direction (a,b) if and only if $f_{(a,b)}(x,y)$ divides $\sum_{(i,j)\in A} g(i,j)x^i y^j$ in $R[x,y]$.*

Proof. The 'if' direction follows trivially by substituting $y \leftarrow x^{-\frac{a}{b}}$ into $h(x,y)$ if $ab \neq 0$, $y \leftarrow 1$ if $a = 0$ and $x \leftarrow 1$ if $b = 0$.

For the converse, put $h(x,y) = \sum_{(i,j)\in A} g(i,j)x^i y^j$. Let H be the set of those $t \in \mathbb{Z}$, for which the intersection of the line $ay = bx + t$ and A is nonempty. Clearly, H is a finite subset of $\mathbb{Z}$. For $t \in H$ let $i_{\min}(t)$ and $i_{\max}(t)$ denote the minimum and maximum of those indices i with $0 \le i < m$ for which $aj' = bi + t$ holds for some $0 \le j' < n$. Similarly, let $j_{\min}(t)$ and $j_{\max}(t)$ denote the minimum and maximum of those indices j with $0 \le j < n$ for which $aj = bi' + t$ holds for some $0 \le i' < m$. Moreover, put

$$I(t) = \begin{cases} (i_{\max}(t) - i_{\min}(t))/a + 1, & \text{if } a \neq 0, \\ m, & \text{if } a = 0. \end{cases}$$

Note that we also have

$$I(t) = \begin{cases} (j_{\max}(t) - j_{\min}(t))/|b| + 1, & \text{if } b \neq 0, \\ n, & \text{if } b = 0. \end{cases}$$

Suppose first that $b = 0$. Then we have $a = 1$ and

$$h(x,y) = \sum_{(i,j)\in A} g(i,j)(x^i - 1)y^j + \sum_{j=0}^{n-1} y^j \sum_{i=0}^{m-1} g(i,j) = (x-1) \sum_{(i,j)\in A} g(i,j)\frac{x^i - 1}{x-1} y^j.$$

Next suppose that $b < 0$. Then we may write

$$h(x,y) = \sum_{t\in H} \sum_{s=0}^{I(t)-1} c_s(t) x^{i_{\min}(t)+sa} y^{j_{\max}(t)+sb},$$

where $c_s(t) = g(i_{\min}(t) + sa, j_{\max}(t) + sb)$. By partial summation

$$h(x,y) = (y^{-b} - x^a) \sum_{t\in H} \sum_{s=0}^{I(t)-1} \left(\sum_{l=0}^{s} c_l(t) \right) x^{i_{\min}(t)+sa} y^{j_{\max}(t)+(s+1)b} +$$

$$+ \sum_{t\in H} \left(\sum_{l=0}^{I(t)-1} c_l(t) \right) x^{i_{\min}(t)+I(t)a} y^{j_{\max}(t)+I(t)b}.$$

Using the assumption

$$\sum_{s=0}^{I(t)-1} c_s(t) = 0 \quad \text{for every } t \in H, \tag{3}$$

we obtain

$$h(x,y) = (y^{-b} - x^a) \sum_{t \in H} \sum_{s=0}^{I(t)-2} \left(\sum_{l=0}^{s} c_l(t) \right) x^{i_{\min}(t)+sa} y^{j_{\max}(t)+(s+1)b}.$$

This proves the 'only if' direction of the lemma if $b < 0$.

Finally suppose that $b > 0$. Now

$$h(x,y) = \sum_{t \in H} \sum_{s=0}^{I(t)-1} c_s(t) x^{i_{\min}(t)+sa} y^{j_{\min}(t)+sb}$$

holds, where $c_s(t) = g(i_{\min}(t) + sa, j_{\min}(t) + sb)$. By partial summation and (3) we obtain

$$h(x,y) = (x^a y^b - 1) \sum_{t \in H} \sum_{s=0}^{I(t)-2} \left(\sum_{l=s+1}^{I(t)-1} c_l(t) \right) x^{i_{\min}(t)+sa} y^{j_{\min}(t)+sb}$$

which completes the proof of the lemma. □

Proof of Theorem 1. By definition, for every u and v the function $F_{(u,v;S)}$ is divisible by $f_{(a_d,b_d)}$ for any d with $1 \le d \le k$. Hence by the lemma $m_{(u,v;S)}$ has zero line sums along all the lines corresponding to S. This proves the second statement of Theorem 1.

The first part of the theorem is now clearly equivalent to saying that the switching elements

$$m_{(u,v;S)} \quad (0 \le u < m - M,\ 0 \le v < n - N)$$

form a basis of the module

$$H = \{e :\ A \to R\ :\ e \text{ has zero line sums corresponding to the directions in } S\}$$

over R. To show this, we first prove that the switching elements generate H. Suppose $g \in H$ and put $h(x,y) = \sum_{(i,j) \in A} g(i,j) x^i y^j$. Let $f_{(a_d,b_d)}(x,y)$ and $F_S(x,y)$ be the functions corresponding to the direction set S as defined in Section 2. Now by the lemma and the fact that the polynomials $f_{(a_d,b_d)}(x,y)$ are primes in the unique factorization domain $R[x,y]$, we obtain

$$F_S(x,y) \mid h(x,y) \ \text{ in } \ R[x,y].$$

Hence there exists a polynomial $t(x,y) = \sum_{u=0}^{m-1-M} \sum_{v=0}^{n-1-N} c_{uv} x^u y^v$ in $R[x,y]$ such that $t(x,y)F_S(x,y) = h(x,y)$. We rewrite this equation as

$$h(x,y) = \sum_{u=0}^{m-1-M} \sum_{v=0}^{n-1-N} c_{uv} F_{(u,v;S)}(x,y).$$

Now by the definitions of $h(x,y)$ and the switching elements $m_{(u,v;S)}$ we immediately obtain

$$g = \sum_{u=0}^{m-1-M} \sum_{v=0}^{n-1-N} c_{uv} m_{(u,v;S)},$$

which proves that the functions $m_{(u,v;S)}$ generate H.

Suppose now that for some coefficients $c_{uv} \in R$ we have

$$\sum_{u=0}^{m-1-M} \sum_{v=0}^{n-1-N} c_{uv} m_{(u,v;S)}(i,j) = 0 \quad \text{for} \quad 0 \le i < m,\ 0 \le j < n. \tag{4}$$

By the definitions of the switching elements, at the bottom-left corner of $m_{(0,0;S)}$ all the other switching elements vanish. This immediately implies $c_{00} = 0$. Considering now $m_{(0,1;S)}$ and using the same argument we obtain $c_{01} = 0$. Continuing this process (taking the switching elements $m_{(u,v;S)}$ in increasing lexicographical order in (u,v) for $0 \le u < m - M$, $0 \le v < n - N$), we easily conclude that all the coefficients c_{uv} must be zero in (4). This shows that the switching elements are linearly independent, which completes the proof of the theorem. □

Proof of Corollary 1. We start from f, and follow the method used in the preceding paragraph. As every switching element takes value ± 1 at its bottom-left corner, we obtain that there are unique coefficients $c_{uv} \in R$ ($0 \le u < m - M$, $0 \le v < n - N$) such that

$$g := f + \sum_{u=0}^{m-1-M} \sum_{v=0}^{n-1-N} c_{uv} m_{(u,v;S)}$$

has the prescribed values at the squares belonging to L. By the second statement of the theorem the line sums of f and g corresponding to S coincide. □

Proof of Corollary 2. Let T denote the quotient field of R, and consider the statement over T first. It is well-known that in case of any system of linear equations over T, the number of variables equals the sum of the nullity and the rank of the system. Moreover, the rank is just the difference of the number of equations and the number of linearly independent homogeneous linear dependencies among these equations. In the present case the number of variables is mn, and by Theorem 1 the nullity of the system is the dimension of the linear space generated by the switching elements, that is $\left(m - \sum_{d=1}^{k} a_d\right)\left(n - \sum_{d=1}^{k} |b_d|\right)$. There are $a_d n + |b_d| m - a_d |b_d|$ line sums corresponding to a direction (a_d, b_d) in S. Hence for the dependency number among the line sums we obtain

$$\left(m - \sum_{d=1}^{k} a_d\right)\left(n - \sum_{d=1}^{k} |b_d|\right) + n \sum_{d=1}^{k} a_d + m \sum_{d=1}^{k} |b_d| - \sum_{d=1}^{k} a_d |b_d| - mn =$$

$$= \sum_{d=1}^{k} a_d \sum_{d=1}^{k} |b_d| - \sum_{d=1}^{k} a_d |b_d|,$$

which proves the Corollary over T.

Now observe that every linear dependence relation over T yields a linear dependence relation over R and vice versa. □

Remark 4. In the special case $k = 4$, $S = \{(1,0), (0,1), (1,1), (1,-1)\}$ Corollary 2 states that the dependency number is seven. We give a basis. For this let f be an arbitrary function defined on A, and put

$$r_j = \sum_{i=0}^{m-1} f(i,j) \quad \text{for} \quad 0 \le j < n, \qquad s_i = \sum_{j=0}^{n-1} f(i,j) \quad \text{for} \quad 0 \le i < m;$$

$$t_h = \sum_{\substack{j=i+h \\ (i,j)\in A}} f(i,j) \quad \text{for} \quad -m+1 \le h < n;$$

and

$$u_h = \sum_{\substack{j=-i+h \\ (i,j)\in A}} f(i,j) \quad \text{for} \quad 0 \le h < m+n-1.$$

Now consider the following seven linear dependence relations among the line sums:

$$\sum_{j=0}^{n-1} r_j = \sum_{i=0}^{m-1} s_i = \sum_{h=-m+1}^{n-1} t_h = \sum_{h=0}^{m+n-2} u_h$$

$$\sum_{\substack{h=-m+1 \\ h \text{ is odd}}}^{n-1} t_h = \sum_{\substack{h=0 \\ h \text{ is odd}}}^{m+n-2} u_h$$

$$-\sum_{j=0}^{n-1} j r_j + \sum_{i=0}^{m-1} i s_i = \sum_{h=-m+1}^{n-1} h t_h$$

$$\sum_{j=0}^{n-1} j r_j + \sum_{i=0}^{m-1} i s_i = \sum_{h=0}^{m+n-2} h u_h$$

$$2\sum_{j=0}^{n-1} j^2 r_j + 2\sum_{i=0}^{m-1} i^2 s_i = \sum_{h=-m+1}^{n-1} h^2 t_h + \sum_{h=0}^{m+n-2} h^2 u_h$$

To see that these relations are independent it is sufficient to check that the determinant of the minor corresponding to $r_1, r_2, s_1, s_2, t_0, t_1, u_0$ in the above system of equations does not vanish. By Corollary 2 this immediately implies that the above dependencies generate a basis.

Proof of Theorem 2. To prove the statement, we give an algorithm for the construction of g having the desired properties. Put $M = \sum_{d=1}^{k} a_d$, $N = \sum_{d=1}^{k} |b_d|$.

First, compute some function $q : A \to \mathbb{Q}$ having the same line sums as f. It can be done by solving the system of linear equations provided by the line sums. This step is known to be polynomial in $\max\{m,n\}$ (see e.g. [2], p. 48). We construct a function $s : A \to \mathbb{Z}$ with the same line sums as f. We follow the procedure used in the second part of the proof of Theorem 1 and start with the bottom-left corner (i^*, j^*) of $m_{(0,0;S)}$. With an appropriate rational coefficient r_{00} with $|r_{00}| \le 1/2$, the value $(q + r_{00} m_{(0,0;S)})(i^*, j^*)$ will be an integer. We now continue with the bottom-left corner $(i^*, j^* + 1)$ of $m_{(0,1;S)}$ and choose a coefficient r_{01} subject to $|r_{01}| \le 1/2$ such that $(q + r_{00} m_{(0,0;S)} + r_{01} m_{(0,1;S)})(i^*, j^* + 1)$ is an integer. Observe that the value at (i^*, j^*) is not changed in the second step. Repeating this procedure for all the bottom-left corners of the switching elements $m_{(u,v;S)}$ (taking them in increasing lexicographical order in (u, v) for $0 \le u < m - M$, $0 \le v < n - N$), we obtain a function s having integer value at the bottom-left corner of every switching element. It is clear that the values at the other squares also remain rationals, and by Corollary 1 with $R = \mathbb{Q}$, they are uniquely determined. Applying now Corollary

1 again with $R = \mathbb{Z}$, we conclude that these values have to be integers. Clearly, this construction of s needs only a polynomial number of steps in $\max\{m, n\}$.

According to Section 2, consider now all the functions as vectors (mn-tuples), and solve over $\mathbb{Q}$ the following system of $(m - M) \times (n - N)$ linear equations

$$(\vec{s}, \vec{m}_{(w,z;S)}) = \sum_{u=0}^{m-1-M} \sum_{v=0}^{n-1-N} c^*_{uv} (\vec{m}_{(u,v;S)}, \vec{m}_{(w,z;S)})$$

in c^*_{uv}, where $(.,.)$ denotes the inner product of vectors. As the switching elements are linearly independent according to Theorem 1, this system of equations will have a unique solution. This can be computed again in time polynomial in $\max\{m, n\}$. Put $\vec{g} = \vec{s} - \sum_{u=0}^{m-1-M} \sum_{v=0}^{n-1-N} ||c^*_{uv}|| \vec{m}_{(u,v;S)}$, where $||\alpha||$ denotes the nearest integer to α. Observe that $\vec{s} - \sum_{u=0}^{m-1-M} \sum_{v=0}^{n-1-N} c^*_{uv} \vec{m}_{(u,v;S)}$ is just the projection of $\vec{f}$ onto the orthogonal complement of the linear subspace generated by the switching elements. This implies

$$|\vec{g}| \leq |\vec{f}| + \left| \sum_{u=0}^{m-1-M} \sum_{v=0}^{n-1-N} (c^*_{uv} - ||c^*_{uv}||) \vec{m}_{(u,v;S)} \right|. \tag{5}$$

There are at most 2^k switching elements which contribute to the value of any fixed square, each with a contribution at most $1/2$ in absolute value in (5). Thus we may conclude $|\vec{g}| \leq |\vec{f}| + 2^{k-1}\sqrt{mn}$.

Finally, notice that all the steps of the above algorithm were polynomial in $\max\{m, n\}$. Thus the proof of Theorem 2 is complete. □

Proof of Corollary 3. By assumption we have $|f| \leq \sqrt{mn}$. □

5. Acknowledgement

The first author is grateful to the University of Leiden for its hospitality during this research. The authors thank R. J. Gardner and M. Nivat for their encouragement.

References

[1] E. Barucci, A. Del Lungo, M. Nivat, R. Pinzani, *Reconstructing convex polynominoes from horizontal and vertical projections*, Theor. Computer Sc. **155** (1996), 321–347.

[2] H. Cohen, *A Course in Computational Algebraic Number Theory*, Springer-Verlag, Berlin Heidelberg, 1993.

[3] R. J. Gardner, *Geometric tomography*, Encyclopedia of Mathematics and its Applications 58, Cambridge University Press, Cambridge, 1995.

[4] R. J. Gardner, P. Gritzmann, *Discrete tomography: determination of finite sets by X-rays*, Trans. Amer. Math. Soc. **6** (1997), 2271–2295.

[5] R. J. Gardner, P. Gritzmann, D. Prangenberg, *On the computational complexity of reconstructing lattice sets from their X-rays*, Discrete Math. **202** (1999), 45–71.

[6] G. T. Herman, A. Kuba, *Discrete Tomography: Foundations, Algorithms and Applications*, Birkhäuser, Boston, 1999.

Leiden University
Mathematical Institute
P.O. Box 9512
2300 RA Leiden
The Netherlands

E-mail address:
hajdu@math.leidenuniv.nl
tijdeman@math.leidenuniv.nl