Dependencies between line sums

Dalen, B.E. van

Birgit van Dalen

Dependencies between line sums

Master's thesis, defended on July 6, 2007

Thesis advisor: R. Tijdeman

Mathematisch Instituut, Universiteit Leiden

Contents

Chapter 1

Introduction

In many practical situations it is useful to be able to construct an image of the inside of an object without taking it apart. This happens for example in a hospital, in which case the object is the patient. X-rays can be used to make a two-dimensional image of the bones in an arm, for instance. When such a two-dimensional image is not sufficient, a CT-scanner can be used to create a three-dimensional image. The technique that is used to do this is called tomography.

In general, tomography is concerned with reconstructing an image from its projections in several directions. A projection is a kind of X-ray photograph: the more material the X-ray encounters on its way through the object, the lighter the corresponding point on the photograph is. From a projection you can deduce how much material is inside, but not where exactly it is. However, using projections in different directions it is sometimes possible to entirely reconstruct the image.

Aside from the medical applications, tomography is also used in the industry and the nanotechnology.

There are three types of tomography. Continuous tomography deals with solid objects that consist of a continuous spectrum of materials (grey values in a picture). If on the other hand there are only a few different materials, then we call it geometric tomography [3]. Finally discrete tomography concerns images consisting of points on a lattice, where each point has a grey value. As in geometric tomography, the set of grey values should be discrete and often very small.

While continuous tomography is being used in many practical applications, discrete tomography is still fairly new [7]. Recently new algorithms for discrete tomography have been discovered [1, 2, 8], which are much better than the ones that already existed. It is likely that discrete tomography will soon be used in applications as well.

In the mathematical model of discrete tomography we use in this thesis, each integer point inside a rectangle in the plane has an integer value. Lines can be drawn through the points in the rectangle in various directions. If we add up the values of all the points one line passes through, we acquire the line sum of that line. A projection consists of the line sums of all the lines in one direction. The problem discrete tomography revolves about is to reconstruct the values of all the points, when only the projections in a few directions are known.

Often the values of the points are not uniquely determined by the projections [4, 6]. On the other hand, if the line sums are arbitrary numbers, then there may not be a solution at all. There are some relations that the line sums need to satisfy. For example, the sum of the line sums in one direction should be equal to the sum of the line sums in another direction, since both numbers are equal to the sum of the values of all points.

These relations (dependencies) between the line sums are the topic of this thesis. It is possible to determine the number of dependencies for any given set of directions [5]; however, this has been done without actually constructing the dependencies. The question of how to construct the dependencies remains unanswered in the literature. In this thesis we will make an attempt to solve this problem.

We can distinguish between two types of dependencies: global and local dependencies. The relation we mentioned above is a global dependency. In general global dependencies do not have to use all lines in one direction, but they do use lines from all over the rectangle. Local dependencies, on the other hand, only use lines from one corner of the rectangle. For example, if there are two lines (in different directions) that pass through one of the corner points of the rectangle and through no other points, then the line sums of both lines are equal, since they are both equal to the value of the corner point.

There exist local dependencies that are rather more complicated than the above example, but the principle is the same every time: while most lines pass through many points, there are lines that pass through only a few points in a corner. Therefore it is often possible to find a set of points in a corner and lines through only those points, such that at least two lines pass through every point. Then the value of each point occurs in at least two line sums, and you can derive a dependency from that.

Some of the global dependencies are constructed by taking a set of lines in one direction and a set of line in another direction, such that the lines pass through exactly the same points. Then the sum of the line sums of the lines in the first set is equal to the sum of the line sums of the lines in the second set. Other global dependencies use lines from more than two directions and multiply each line sum with a coefficient depending on the parameter of the line. These dependencies are less obvious on first sight, but equally easy to find with a little linear algebra.

In Chapter 2 we will introduce some notation and describe the structure of the dependencies as we conjecture it, making a distinction between global and local dependencies. In Chapter 3 we will attempt to construct the global dependencies, and we will prove that our construction is correct if there are less than five different directions. In Chapter 4 we will construct the local dependencies. Finally, the conclusions are in Chapter 5.

Chapter 2

Notation and background

The main problem of discrete tomography 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. In this thesis we will restrict ourselves to the case $l = 2$ and consider a slightly more general version where the function values are in $\mathbb{Z}$ rather than in $\{0, 1\}$. The original problem with $l = 2$ is a special case of this.

In general, the line sums cannot vary independently of each other. There are some linear dependencies between them, the most obvious of which is that the sum of the line sums in one direction is equal to the sum of the line sums in another direction. This thesis will focus on finding these dependencies when A is a rectangle in $\mathbb{Z}^2$.

2.1 Definitions

Let k, m and n be integers greater than 1. Let

$$A = \{(x, y) \in \mathbb{Z} : 0 \leq x < m, 0 \leq y < n\}$$

and $f : A \to \mathbb{Z}$. A line in $\mathbb{Z}^2$ is given by an equation of the form $ay - bx = h$, where $h \in \mathbb{Z}$ and a and b are integers. We call this a line in the direction (a, b). In order for the directions to be unique, we require that $a \geq 0$, $\gcd(a, b) = 1$ and if $a = 0$, then $b = 1$.

We call a set $\{(a_i, b_i)\}_{i=1}^{k}$ *valid* if $\sum_{i=1}^{k} a_i < m$ and $\sum_{i=1}^{k} |b_i| < n$. For $1 \leq i \leq k$ and $h \in \mathbb{Z}$ we denote by $s(i, h)$ the line sum of the line given by $ay - bx = h$, i.e.

$$s(i, h) = \sum_{\substack{(x,y) \in A, \\ ay - bx = h}} f(x, y).$$

A homogeneous linear dependency between the line sums is of the form

$$\sum_{i=1}^{k} \sum_{h \in \mathbb{Z}} c_{i,h} s(i, h) = 0,$$

where $c_{i,h}$ are coefficients depending on i and h. Note that $s(i,h) = 0$ for all but finitely many h, so this sum is well-defined.

Given two linear dependencies, any linear combination of them is also a linear dependency. We are therefore only interested in a basis of linear dependencies. We will not always explicitly mention this. In particular, by "the number of linear dependencies" we usually mean the maximal number of linearly independent linear dependencies.

It is possible to count the number of linear dependencies between the line sums, provided that the set of directions is valid. L. Hajdu and R. Tijdeman proved the following theorem [5].

Theorem 2.1. *Let $\{(a_i, b_i)\}_{i=1}^k$ be a valid set of directions. The number of linearly independent homogeneous linear dependencies among the line sums is equal to*

$$\sum_{i=1}^k a_i \sum_{i=1}^k |b_i| - \sum_{i=1}^k a_i |b_i|. \tag{2.1}$$

The proof of this theorem given by Hajdu and Tijdeman is not constructive. Therefore a new problem naturally arises from this result: construct a basis for the linear dependencies. This is the problem this thesis focuses on.

2.2 Global and local

A remarkable thing about formula (2.1) is that it does not depend on m and n. As long as m and n are both large enough (so that the set of directions is valid) the number of dependencies apparently does not depend on the size of the rectangle. In fact some of the dependencies do not even depend on the shape of A. We have assumed that A is a rectangle, but for some of the dependencies we will construct, this is not a necessary condition. The dependency mentioned in the introduction of this chapter is an example of that.

We define a *global dependency* as a dependency of the form

$$\sum_{i=1}^k \sum_{h \in \mathbb{Z}} c_{i,h} s(i,h) = 0,$$

that is valid for any finite set $A \subset \mathbb{Z}^2$, that is, the coefficients $c_{i,h}$ do not depend on A. In Chapter 3 we will construct global dependencies.

In general, the global dependencies are not the only dependencies between the line sums. In the case that A is a rectangle, some lines pass through only a few points in the corner of A, which leads to extra dependencies between those line sums. In particular, if there are two directions (a_i, b_i) and (a_j, b_j) with a_i, a_j, b_i and b_j strictly positive, then for each of these two directions there exists a line in that direction that passes only through the point $(m-1, 0)$ in the lower right corner of A. It is clear that those two line sums are equal to each other.

We will call these dependencies *local dependencies*, and we will construct them in Chapter 4.

Let A be a rectangle as defined in Section 2.1 and let $\{(a_i, b_i)\}_{i=1}^k$ be a valid set of directions. Assume without loss of generality that the directions are ordered in such a way that the following properties hold for certain integers l and l' with $0 \leq l \leq l' \leq k$:

- for $1 \leq i \leq l$ we have $a_i > 0$ and $b_i > 0$,
- for $l < i \leq l'$ we have $a_i > 0$ and $b_i < 0$,
- for $l' < i \leq k$ we have $a_i b_i = 0$,
- for the first l directions we have
$$\frac{b_1}{a_1} > \frac{b_2}{a_2} > \ldots > \frac{b_l}{a_l},$$
- for the next $l' - l$ directions we have
$$\frac{|b_{l+1}|}{a_{l+1}} > \frac{|b_{l+2}|}{a_{l+2}} > \ldots > \frac{|b_{l'}|}{a_{l'}}.$$

We conjecture the following.

Conjecture 2.2. *There are*
$$\sum_{1 \leq i < j \leq k} |a_i b_j - a_j b_i|$$
linearly independent global dependencies between the line sums, and there are
$$\sum_{1 \leq i < j \leq l} 2a_i b_j + \sum_{l < i < j \leq l'} 2a_i |b_j|$$
linearly independent local dependencies between the line sums.

Notice that
$$\begin{aligned} \sum_{i=1}^{k} a_i \sum_{j=1}^{k} |b_j| - \sum_{i=1}^{k} a_i |b_i| &= \sum_{i \neq j} a_i |b_j| \\ &= \sum_{1 \leq i < j \leq k} (a_i |b_j| + a_j |b_i|) \\ &= \sum_{1 \leq i < j \leq k} |a_i b_j - a_j b_i| + \sum_{1 \leq i < j \leq l} 2a_i b_j + \sum_{l < i < j \leq l'} 2a_i |b_j|, \end{aligned}$$
so the numbers in the Conjecture 2.2 sum up to (2.1).

Example. Consider the directions $(a_1, b_1) = (2, 3)$ and $(a_2, b_2) = (2, 1)$. Note that we have $\frac{b_1}{a_1} > \frac{b_2}{a_2}$. According to the above conjecture, we should have $|2 \cdot 1 - 2 \cdot 3| = 4$ global dependencies and $2 \cdot 2 \cdot 1 = 4$ local dependencies.

To find the global dependencies, we look for a set of lines in the direction $(2,3)$ and a set of lines in the direction $(2,1)$ so that the lines from both sets pass through the same points. In Figure 2.1 such lines have been drawn in a part of the rectangle A. The sum of the line sums of these lines in one direction is equal to the sum of the values of the points that these lines pass through, which is equal to the sum of the line sums of the lines in the other direction. If we assume that one of the lines passes through the point $(0,0)$, then the lines in the figure are exactly the ones with $h = a_i y - b_i x \equiv 0 \mod 4$. So we have

$$\sum_{h\equiv 0 \bmod 4} s(1,h) = \sum_{h\equiv 0 \bmod 4} s(2,h).$$

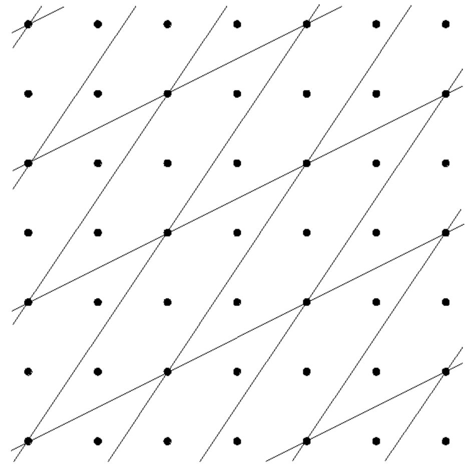

Figure 2.1: A global dependency illustrated for the directions $(2,3)$ and $(2,1)$.

The points these lines pass through form a lattice with lattice determinant $|a_1 b_2 - a_2 b_1| = 4$. This is the reason why there are four global dependencies: by translating the lattice we find three other dependencies. They are

$$\begin{aligned}
\sum_{h\equiv 1 \bmod 4} s(1,h) &= \sum_{h\equiv 3 \bmod 4} s(2,h),\\
\sum_{h\equiv 2 \bmod 4} s(1,h) &= \sum_{h\equiv 2 \bmod 4} s(2,h),\\
\sum_{h\equiv 3 \bmod 4} s(1,h) &= \sum_{h\equiv 1 \bmod 4} s(2,h).
\end{aligned}$$

The local dependencies occur in the lower right and upper left corners. You can find the ones in the upper left corner by rotating A once you have the ones in the lower right corner. In each corner there should be two local dependencies, since there are four altogether. We are again looking for sets of lines that pass through the same points, but this time the

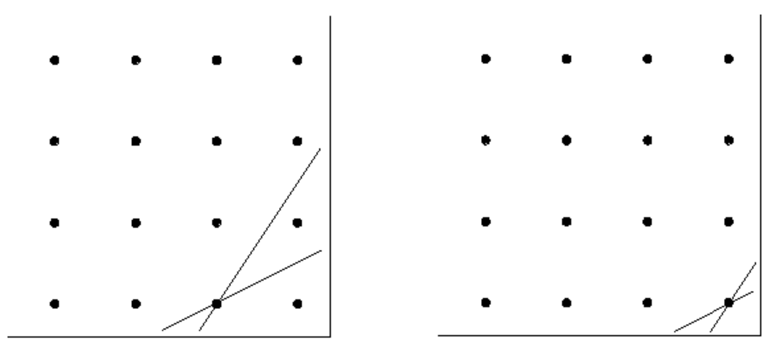

Figure 2.2: The local dependencies illustrated for the directions $(2,3)$ and $(2,1)$.

points should be restricted to the lower right corner. There are two possibilities (as well as a combination of them), which are shown in Figure 2.2.

In the left part of Figure 2.2, the lines both pass through the point $(m-2, 0)$, so we have $h_1 = a_1 y - b_1 x = 2\cdot 0 - 3\cdot(m-2) = -3m+6$ and $h_2 = a_2 y - b_2 x = 2\cdot 0 - 1\cdot(m-2) = -m+2$. So the local dependency corresponding to this figure is

$$s(1, -3m+6) = s(2, -m+2).$$

Similarly, the local dependency corresponding to the right part of Figure 2.2 is

$$s(1, -3m+3) = s(2, -m+1).$$

We can find two more local dependencies in the upper left corner, completing the set of eight linear dependencies. If m and n are very small, then a global dependency might be equal to a local dependency or to the sum of two local dependencies. However, assuming validness (in this case $m \geq 5$ and $n \geq 5$) ensures that each global dependency involves at least one line that does not occur in any local dependency. Then it is clear that the eight dependencies we found form a linearly independent set.

In Chapter 4 we will construct $\sum_{1 \leq i < j \leq l} 2a_i b_j + \sum_{l < i < j \leq l'} 2a_i |b_j|$ linearly independent local dependencies. To prove Conjecture 2.2 it then suffices to prove that there are $\sum_{1 \leq i < j \leq k} |a_i b_j - a_j b_i|$ linearly independent global dependencies, which are on A independent of the local ones. We will take some steps towards such a result in Chapter 3.

Chapter 3

Global dependencies

The first section of this chapter will be devoted to constructing global dependencies between line sums. Not all of these will be linearly independent of each other. Therefore, after that we want to pick $\sum_{1 \leq i < j \leq k} |a_i b_j - a_j b_i|$ of them and prove that they are linearly independent. In the final two sections of the chapter, we will describe two different approaches to this and show that they work if $k \leq 4$.

3.1 Constructing global dependencies

First we prove a useful lemma.

Lemma 3.1. *Let (a_i, b_i) and (a_j, b_j) be two directions. Let d be a positive integer such that $d \mid a_i b_j - a_j b_i$. Then for any integers X and Y we have*

$$a_i Y \equiv b_i X \mod d \quad \Leftrightarrow \quad a_j Y \equiv b_j X \mod d.$$

Proof. We will prove only one direction; the other follows from symmetry.

So suppose it holds that

$$a_i Y \equiv b_i X \mod d.$$

Let $g = \gcd(a_i, d)$. First assume that $g = 1$. Then we may multiply the given congruence by $\frac{a_j}{a_i}$, so we have

$$a_j Y \equiv \frac{a_j}{a_i} b_i X \mod d.$$

We may replace $a_j b_i$ by $a_i b_j$ on the right-hand side, as $a_j b_i - a_i b_j \equiv 0 \mod d$, hence

$$a_j Y \equiv b_j X \mod d,$$

which is what we had to prove.

Now assume $g > 1$. Since g divides a_i as well as d, it must also divide $b_i X$. Since $\gcd(a_i, b_i) = 1$, it follows that $g \mid X$. We now have

$$\frac{a_i}{g} Y \equiv b_i \frac{X}{g} \mod \frac{d}{g}.$$

From $g \mid d$ and $d \mid a_ib_j - a_jb_i$ we get $g \mid a_ib_j - a_jb_i$. As g divides a_i, it must also divide a_jb_i and therefore a_j. Now substitute $X' = \frac{X}{g}$, $a_i' = \frac{a_i}{g}$, $a_j' = \frac{a_j}{g}$ and $d' = \frac{d}{g}$. Then

$$a_i'Y \equiv b_iX' \mod d'.$$

We obviously have $\gcd(a_i', b_i) = \gcd(a_j', b_j) = 1$, as well as $\gcd(a_i', d') = 1$. So we can apply the above proof for the case that $\gcd(a_i, d) = 1$, now taking X', a_i', a_j' and d' instead of X, a_i, a_j and d, respectively, and we conclude that

$$a_j'Y \equiv b_jX' \mod d'.$$

From this it follows that

$$a_jY \equiv b_jX \mod d,$$

which completes the proof. □

Let S be a subset of $\{1, 2, \ldots, k\}$ of cardinality $l \geq 2$. We identify each $j \in S$ with the direction (a_j, b_j). Let $g = \gcd_{i,j \in S} |a_ib_j - a_jb_i|$. Let c be an arbitrary number with $0 \leq c \leq g - 1$. Fix $i \in S$. Consider the set $B \subset \mathbb{Z}^2$ defined by

$$B = \{(x, y) \in \mathbb{Z}^2 : a_iy - b_ix \equiv c \mod g\}.$$

Suppose $(x_0, y_0) \in B$ and $j \in S$. Then also $(x_0 + a_j, y_0 + b_j) \in B$, since

$$a_i(y_0 + b_j) - b_i(x_0 + a_j) = a_iy_0 - b_ix_0 + a_ib_j - a_jb_i \equiv c + a_ib_j - a_jb_i \equiv c \mod g,$$

as $a_ib_j - a_jb_i$ is divisible by g. So for a line in the direction (a_j, b_j) it holds that either all points on the line are in B or none of the points on the line are in B.

If (x_0, y_0) and (x_1, y_1) are two points in B, then we have $a_iy_0 - b_ix_0 \equiv a_iy_1 - b_ix_1 \mod g$ by definition, so $a_i(y_0 - y_1) \equiv b_i(x_0 - x_1) \mod g$. If $j \in S$, then Lemma 3.1 with $X = x_0 - x_1$ and $Y = y_0 - y_1$ implies that $a_j(y_0 - y_1) \equiv b_j(x_0 - x_1) \mod g$, so $a_jy_0 - b_jx_0 \equiv a_jy_1 - b_jx_1 \mod g$. Now we see that if H_j is the set of integers h for which the line defined by $a_jy - b_jx = h$ passes through points in B, then H_j is of the form $\{h : h \equiv d_j \mod g\}$ for a certain d_j.

Remark. If $c = 0$, then the set B is a lattice in $\mathbb{Z}^2$ with determinant g. Otherwise, it is a translate of such a lattice.

Theorem 3.2. *Let S' be a subset of S of cardinality $l' \geq 2$. Then there exists a dependency of the form*

$$\sum_{j \in S'} c_j \sum_{h \in H_j} h^{l'-2} s(j, h) = 0, \tag{3.1}$$

with the c_j not all equal to zero. We call this a dependency of the power $l' - 2$.

Proof. Fix a point $(x, y) \in B$. Through this point passes a line in each direction (a_j, b_j) with $j \in S'$. Each of those lines corresponds to an $h \in H_j$ given by $h = a_j y - b_j x$. Assume we can find c_j, $j \in S'$, independent of (x, y) such that

$$\sum_{j \in S'} c_j (a_j y - b_j x)^{l'-2} = 0.$$

Each point in B contributes for each j to exactly one $s(j, h)$ with $h \in H_j$, so if we sum over all points in B, we acquire the dependency in (3.1). It now suffices to prove that such $c_1, c_2, \ldots, c_k$ exist.

We can view $(a_j y - b_j x)^{l'-2}$ as a linear expression in the $l' - 1$ variables $x^{l'-2}$, $x^{l'-3}y$, ..., $y^{l'-2}$. We have l' of these expressions (one for each $j \in S'$) so they cannot all be linearly independent. Therefore there must be coefficients c_j, $j \in S'$, not all equal to zero, such that

$$\sum_{j \in S'} c_j (a_j y - b_j x)^{l'-2} = 0.$$

The coefficients are obviously independent of x and y, as we have considered $x^{l'-2}$, $x^{l'-3}y$, ..., $y^{l'-2}$ as formal variables. □

Theorem 3.3. *Let S' be a subset of S of cardinality $l' \geq 2$. Then there does not exist a dependency of the form*

$$\sum_{j \in S'} c_j \sum_{h \in H_j} h^{l'-1} s(j, h) = 0,$$

with the c_j not all equal to zero.

Proof. Suppose such a dependency does exist. We can vary the value of one point in B and fix the values of all other points, so for every $(x, y) \in B$ it must hold that

$$\sum_{j \in S'} c_j (a_j y - b_j x)^{l'-1} = 0.$$

For fixed x we can view the left-hand side as a polynomial in y of degree $l' - 1$. If $(x, y) \in B$, then also $(x, y + g) \in B$, so there are infinitely many values of y for which this equation must hold. Therefore the polynomial must be the zero polynomial. From this we acquire a set of equations:

$$\begin{cases} \sum_{j \in S'} c_j a_j^{l'-1} &= 0, \\ \sum_{j \in S'} c_j \binom{l'}{1} a_j^{l'-2}(-b_j x) &= 0, \\ \sum_{j \in S'} c_j \binom{l'}{2} a_j^{l'-3}(-b_j x)^2 &= 0, \\ &\vdots \\ \sum_{j \in S'} c_j (-b_j x)^{l'-1} &= 0. \end{cases}$$

We can divide the t-th equation by $\binom{l'}{t}(-x)^t$, $t = 0, 1, \ldots, l'-1$, and write the system in matrix form:

$$\begin{pmatrix} a_{j_1}^{l'-1} & a_{j_2}^{l'-1} & \cdots & a_{j_{l'}}^{l'-1} \\ a_{j_1}^{l'-2}b_{j_1} & a_{j_2}^{l'-2}b_{j_2} & \cdots & a_{j_{l'}}^{l'-2}b_{j_{l'}} \\ \vdots & \vdots & \ddots & \vdots \\ b_{j_1}^{l'-1} & b_{j_2}^{l'-1} & \cdots & b_{j_{l'}}^{l'-1} \end{pmatrix} \begin{pmatrix} c_{j_1} \\ c_{j_2} \\ \vdots \\ c_{j_{l'}} \end{pmatrix} = 0,$$

where $S' = \{j_1, j_2, \ldots, j_{l'}\}$. Observe that the matrix is a Vandermonde-type matrix and has non-zero determinant. The only solution of this set of equations is therefore $c_j = 0$ for all $j \in S'$. □

Corollary 3.4. *The coefficients c_j in Theorem 3.2 are uniquely determined (up to a nonzero factor) and all nonzero.*

Proof. Suppose there exist two sets of coefficients such that one is not a nonzero multiple of the other. Then any linear combination of them would give a dependency as well, so we could construct a dependency where one of the coefficients is zero. In that case we could delete the corresponding direction from S' and get a contradiction with Theorem 3.3. □

3.2 The case $k = 2$

Assume that $k = 2$. Take $S = S' = \{1, 2\}$ and apply Theorem 3.2. For each c with $0 \le c < |a_1b_2 - a_2b_1|$, we have a global dependency on the set

$$B(c) = \{(x, y) \in \mathbb{Z}^2 : a_1y - b_1x \equiv c \mod |a_1b_2 - a_2b_1|\}.$$

Since the sets $B(0)$, $B(1)$, $\ldots$, $B(|a_1b_2 - a_2b_1| - 1)$ are all disjoint, it is obvious that the corresponding $|a_1b_2 - a_2b_1|$ dependencies form a linearly independent set. This is exactly the number of independent linear dependencies we were looking for, so this solves the case $k = 2$.

The dependencies we have found are of the form

$$c_1 \sum_{h \in H_1} s(1, h) + c_2 \sum_{h \in H_2} s(2, h) = 0,$$

so the power of h that occurs here is equal to zero. We have $c_1 = -c_2$, and the dependency just means that if you add the line sums of the lines in H_1, you will get the same sum as when you add the line sums of the lines in H_2. This is obviously true, since both sums are simply the sum of the values $f(x, y)$ for $(x, y) \in B$.

3.3 Some properties

Before we start looking at the cases $k = 3$ and $k = 4$, we need some more results. First of all, there is an important property of the numbers $g = \gcd_{i,j \in S} |a_ib_j - a_jb_i|$ for subsets S of $\{1, 2, \ldots, k\}$.

Lemma 3.5. *Let S_1, S_2 be subsets of $\{1, 2, \ldots, k\}$ with $|S_1| \geq 2$ and $|S_2| \geq 2$. For $t = 1, 2$ let $g_t = \gcd_{i,j \in S_t} |a_i b_j - a_j b_i|$. Let $g = \gcd_{i,j \in S_1 \cup S_2} |a_i b_j - a_j b_i|$. If $S_1 \cap S_2 \neq \emptyset$, then $g = \gcd(g_1, g_2)$.*

Proof. Without loss of generality, assume $1 \in S_1 \cap S_2$. Let $i \in S_1$ and $j \in S_2$. Let $d = \gcd(a_i b_1 - a_1 b_i, a_j b_1 - a_1 b_j)$. Let $c = \gcd(d, b_1)$. Since $d \mid a_i b_1 - a_1 b_i$, we have $c \mid a_1 b_i$, and as $\gcd(a_1, b_1) = 1$, it follows that $c \mid b_i$. Analoguously, $c \mid b_j$. Now we can divide b_1, b_i, b_j and d by c and denote the results by b'_1, b'_i, b'_j and d' respectively. We have

$$\gcd(a_i b'_1 - a_1 b'_i, a_j b'_1 - a_1 b'_j) = \frac{d}{c} = d',$$

so

$$d' \mid b'_j(a_i b'_1 - a_1 b'_i) - b'_i(a_j b'_1 - a_1 b'_j) = b'_1(b'_j a_i - b'_i a_j).$$

Since $\gcd(d', b'_1) = 1$, it follows that $d' \mid b'_j a_i - b'_i a_j$ and hence $d \mid a_i b_j - a_j b_i$. As $g_1 \mid a_i b_1 - a_1 b_i$, we have $\gcd(g_1, g_2) \mid a_i b_1 - a_1 b_i$. Similarly, $\gcd(g_1, g_2) \mid a_j b_1 - a_1 b_j$, and therefore $\gcd(g_1, g_2) \mid d$. We conclude $\gcd(g_1, g_2) \mid a_i b_j - a_j b_i$.

This holds for all $i \in S_1$ and $j \in S_2$, hence

$$g = \gcd(g_1, g_2, \gcd_{i \in S_1, j \in S_2} |a_i b_j - a_j b_i|) = \gcd(g_1, g_2).$$

□

In Theorem 3.2 we constructed dependencies containing different powers of h. We will now show that if A is sufficiently large, then dependencies of different powers are always linearly independent of each other.

Theorem 3.6. *For $t = 0, 1, \ldots, k-2$ let T_t be a set of dependencies with power t as constructed in Theorem 3.2. Suppose that there is a linear dependency between the dependencies in $T_0 \cup T_1 \cup \cdots \cup T_{k-2}$. Then if A is sufficiently large, there is a t such that there is a linear dependency between the dependencies in T_t.*

Proof. By assumption there is a linear dependency between the dependencies in $T_0 \cup T_1 \cup \cdots \cup T_{k-2}$, which we can formally write as

$$\sum_{D \in T_0 \cup T_1 \cup \cdots \cup T_{k-2}} c_D D = 0.$$

We can pull the coefficients c_D into the dependencies themselves, so if D is the dependency

$$\sum_{j \in S'} c_j \sum_{h \in H_j} h^{l'-2} s(j, h) = 0,$$

then we write $c_D D$ as

$$\sum_{j \in S'} c_D c_j \sum_{h \in H_j} h^{l'-2} s(j, h) = 0$$

Do this for all dependencies and then add all dependencies of the power t together, so we acquire for each t one dependency

$$D_t: \quad \sum_h c_{t,1}(h)h^t s(1,h) + \sum_h c_{t,2}(h)h^t s(2,h) + \cdots + \sum_h c_{t,k-2}(h)h^t s(k,h) = 0,$$

where the coefficients are now dependent on h. For each i the i-th sum runs over the numbers h for which the line given by $a_i y - b_i x = h$ passes through at least one point of A. We call these values of h valid.

Define $P = \mathrm{lcm}_{i \neq j}|a_i b_j - a_j b_i|$. For the sets H_j in Theorem 3.2 we have: if $h \in H_j$, then also $h + P \in H_j$. So the coefficients $c_{t,i}(h)$ are a periodic function of h with period P, that is, $c_{t,i}(h) = c_{t,i}(h+P)$ for all valid h, as long as $h+P$ is valid as well.

Keeping in mind that we pulled all the coefficients into the dependencies, we can write the linear dependency between the dependencies formally as

$$D_0 + D_1 + \ldots + D_{k-2} = 0.$$

This means that for every $i \in \{1, 2, \ldots, k\}$ and for every h the sum of the coefficients of $s(i,h)$ is zero, i.e.

$$c_{0,i}(h) + c_{1,i}(h)h + \cdots + c_{k-2,i}(h)h^{k-2} = 0.$$

Fix h_0, then we have for all integers r such that $h_0 + rP$ is valid that

$$c_{0,i}(h_0) + c_{1,i}(h_0) \cdot (h_0 + rP) + \cdots + c_{k-2,i}(h_0) \cdot (h_0 + rP)^{k-2} = 0,$$

since $c_{t,i}(h_0 + rP) = c_{t,i}(h_0)$ for all r. Assume that A is sufficiently large, so that we can plug in $k-1$ different values of r, implying that the polynomial

$$c_{0,i}(h_0) + c_{1,i}(h_0)X + \cdots + c_{k-2,i}(h_0)X^{k-2}$$

is identically zero. Hence

$$c_{t,i}(h_0) = 0$$

for all t and i. This now holds for any valid h_0, so D_t can actually be written as $0 = 0$ for all t. Since D_t is the sum of dependencies of the power t, this means that for each t either the dependencies of power t did not feature at all, or they are not all linearly independent. The latter case must hold for at least one t, which proves the theorem. □

Remark. The condition that the set of directions is valid for the rectangle A implies a lower bound on the size of A, but this is in general not sufficient for the above theorem. The number P can become quite huge, and in that case A needs to be huge as well in order for the proof to work.

Using Theorem 3.6, we can consider the dependencies of different powers separately. We can express the number of dependencies of each power in the numbers $g = \gcd_{i,j \in S} |a_i b_j - a_j b_i|$ for subsets S of $\{1, 2, \ldots, k\}$.

For $2 \leq d \leq k$ define

$$G_l = \sum_{|S|=l} \gcd_{i,j \in S} |a_i b_j - a_j b_i|,$$

where the sum runs over the sets $S \subset \{1, 2, \ldots, k\}$ of cardinality l. Notice that G_2 is the total number of global dependencies we want to have.

Conjecture 3.7. *The number of global dependencies of power t is equal to*

$$\sum_{j=0}^{k-t-2} (-1)^j \binom{t+j}{j} G_{t+j+2}.$$

If this is true, the total number of global dependencies is

$$\sum_{t=0}^{k-2} \sum_{j=0}^{k-t-2} (-1)^j \binom{t+j}{j} G_{t+j+2}.$$

Changing the first summation index from t to $i = t + j$, we can write this as

$$\sum_{i=0}^{k-2} \sum_{j=0}^{i} (-1)^j \binom{i}{j} G_{i+2}.$$

For $i \geq 1$, we have

$$\sum_{j=0}^{i} (-1)^j \binom{i}{j} = 0,$$

so the total number of global dependencies according to this conjecture is equal to G_2, as it should.

For convenience, we write out the numbers in the cases $k = 3$ and $k = 4$.
For $k = 3$:

the number of dependencies of the power 1:	G_3
the number of dependencies of the power 0:	$G_2 - G_3$

For $k = 4$:

the number of dependencies of the power 2:	G_4
the number of dependencies of the power 1:	$G_3 - 2G_4$
the number of dependencies of the power 0:	$G_2 - G_3 + G_4$

We will solve the cases $k = 3$ and $k = 4$ in two different ways.

3.4 The first approach

The idea of this approach is to take a set of dependencies constructed in Theorem 3.2 and count the linear dependencies between them. In that way we show that there is a linearly independent subset of the right cardinality.

3.4.1 Dependencies of the power $k-2$

Take $S = S' = \{1, 2, \ldots, k\}$ and apply Theorem 3.2. Analogously to the case $k = 2$ (see Section 3.2) we get $\gcd_{i,j \in S} |a_i b_j - a_j b_i| = G_k$ global dependencies of the power $k-2$, which are all independent of each other because they are defined on disjoint sets B.

3.4.2 Dependencies of the power $k-3$

Assume $k \geq 3$. For $t = 1, 2, \ldots, k$, let $S_t = \{1, 2, \ldots, k\}/\{i\}$ and $g_t = \gcd_{i,j \in S_t} |a_i b_j - a_j b_i|$. Let $g = \gcd_{1 \leq i < j \leq k} |a_i b_j - a_j b_i| = G_k$. According to Lemma 3.5, we have $g = \gcd(g_t, g_s)$ for all $t \neq s$, because no two of S_1, S_2, $\ldots$, S_k are disjoint.

For some t, take $S = S' = S_t$ and apply Theorem 3.2. That gives us g_t different dependencies (one for each c with $0 \leq c \leq g_t - 1$). Summing over all t we get G_{k-1} dependencies in total. We will show that there are at most $(k-2)G_k$ linearly independent linear dependencies between them. That implies that the number of linearly independent dependencies between the line sums is at least $G_{k-1} - (k-2)G_k$, which agrees with Conjecture 3.7.

Let $t \in \{1, 2, \ldots, k\}$. Notice that the g_t dependencies from Theorem 3.2 all have the same coefficients, only different sets H_j. We can add $\frac{g_t}{g}$ of the dependencies to get a new dependency

$$\sum_{j \in S_t} c_j \sum_{h \in H'_j} h^{l-2} s(j, h) = 0,$$

where $H'_j = \{h : h \equiv d'_j \mod g\}$ for appropriate choices of d'_j, $j \in S_t$. The set of points that this dependency is defined on, is given by

$$B = \{(x, y) \in \mathbb{Z}^2 : a_j y - b_j x \equiv d'_j \mod g\},$$

where $j \in S_t$. By the proof of Theorem 3.2, we know that the coefficients c_j are chosen such that for each $(x, y) \in B$ we have

$$\sum_{j \in S_t} c_j (a_j y - b_j x)^{k-3} = 0.$$

Note that for each t, there is such a dependency on the same set B. Now let c_j denote the coefficients for $t = 1$, c'_j the coefficients for $t = 2$ and c''_j the coefficients for $t = 3$. For each (x, y) in B we have

$$\sum_{j \in S_1} c_j (a_j y - b_j x)^{k-3} = 0, \tag{3.2}$$

$$\sum_{j \in S_2} c'_j (a_j y - b_j x)^{k-3} = 0, \tag{3.3}$$

$$\sum_{j \in S_3} c''_j (a_j y - b_j x)^{k-3} = 0. \tag{3.4}$$

From S_3 the number 3 is missing. If we multiply equation (3.2) by c'_3 and equation (3.3) by c_3 and then subtract them, the coefficient at $j = 3$ vanishes and we get

$$\sum_{j \in S_3} (c_j c'_3 - c'_j c_3)(a_j y - b_j x)^{k-3} = 0, \tag{3.5}$$

where we put $c_1 = c'_2 = 0$. According to Corollary 3.4, the vector of coefficients of this new dependency must be a nonzero multiple of the vector of coefficients in (3.4). That means that the above dependencies for S_1, S_2 and S_3 are linearly dependent.

Analogously we can show that there exists a linear dependency between the dependencies defined on the set B for S_1, S_2 and S_t, where $3 \leq t \leq k$. We will call this dependency $Z(t, B)$. Note that for B we can take g different sets, which are translations of each other. So in total we have $(k-2)g$ dependencies between the dependencies. We will now show that any dependency between the dependencies is a linear combination of these $(k-2)g$ ones.

For $t \in \{1, 2, \ldots, k\}$, write a linear combination of dependencies constructed in Theorem 3.2 as

$$D_t: \quad \sum_{j \in S_t} \sum_h c_{j,h}^{(t)} \; h^{k-3} \; s(j,h) = 0,$$

where $c_{j,h}^{(t)} = c_{j,h'}^{(t)}$ if $h \equiv h' \mod g_t$. Suppose there is a linear dependency between $D_1, \ldots, D_k$, where we pull the coefficients of the dependency into the D_t themselves, so we have (comparing the coefficients of $s(j,h)$)

$$\sum_{t \neq j} c_{j,h}^{(t)} \; h^{k-3} = 0$$

for all j and h. Since for fixed j the coefficients $c_{j,0}^{(t)}$, $t \neq j$, are equal to the coefficients $c_{j,h}^{(t)}$ where $h = h + \text{lcm}(g_1, g_2, \ldots, g_k)$, we can omit the factor h^{k-3}:

$$\sum_{t \neq j} c_{j,h}^{(t)} = 0.$$

Take $j = k$. As $c_{k,h}^{(t)} = c_{k,h'}^{(t)}$ when $h \equiv h' \mod g_t$, we have

$$(c_{k,h}^{(2)}, \ldots, c_{k,h}^{(k-1)}) = (c_{k,h'}^{(2)}, \ldots, c_{k,h'}^{(k-1)})$$

when $h \equiv h' \mod \text{lcm}(g_2, \ldots, g_{k-1})$. So

$$c_{k,h}^{(1)} = -\sum_{t=2}^{k-1} c_{k,h}^{(t)} = -\sum_{t=2}^{k-1} c_{k,h'}^{(t)} = c_{k,h'}^{(1)}$$

when $h \equiv h' \mod \text{lcm}(g_2, \ldots, g_{k-1})$. Therefore $c_{k,h}^{(1)}$ is a periodic function of h with period

$$\gcd(g_1, \text{lcm}(g_2, \ldots, g_{k-1})).$$

We already knew that $\gcd(g_t, g_s) = g$ for $t \neq s$, so

$$\begin{aligned}\gcd(g_1, \operatorname{lcm}(g_2, g_3, \ldots, g_{k-1})) &= \operatorname{lcm}(\gcd(g_1, g_2), \gcd(g_1, g_3), \ldots, \gcd(g_1, g_{k-1})) \\ &= \operatorname{lcm}(g, g, \ldots, g) \\ &= g.\end{aligned}$$

Hence $c_{k,h}^{(1)}$ is a periodic function of h with period g. Analogously, $c_{j,h}^{(t)}$ is a periodic function of h with period g.

Now let $3 \leq t \leq k$. We can split D_t into g dependencies on the sets B we used above to construct $Z(t, B)$ on. Any linear combination of $Z(t, B)$ for various t and B gives us a set D'_1, D'_2, ..., D'_k of dependencies that are linearly dependent, and we can now take the linear combination such that $D'_t = D_t$ for $3 \leq t \leq k$. After all, for $3 \leq t \leq k$ the set S_t is only involved in $Z(t, B)$ for various B, and not in any other $Z(t', B)$. So we can take a linear combination of $Z(3, B)$ so that $D'_3 = D_3$, and then a linear combination of $Z(4, B)$ so that $D'_4 = D_4$ (which does not change D'_3) and so on.

This implies that $D_1 - D'_1$ and $D_2 - D'_2$ are linearly dependent. Since S_1 and S_2 are not equal, this is only possible if $D_1 = D'_1$ and $D_2 = D'_2$. We conclude that we can write the dependency between D_1, ..., D_k as a linear combination of dependencies $Z(t, B)$. This is what we wanted to prove.

In the case $k = 3$ the only global dependencies are the ones of the power $k - 2 = 1$ and $k - 3 = 0$. We have shown that there are at least G_3 linearly independent dependencies of the power 1 and at least $G_2 - G_3$ linearly independent dependencies of the power 0. This solves the case $k = 3$.

3.4.3 The case $k = 4$

Let $k = 4$. In the previous two sections we have shown that there are at least G_4 and $G_3 - 2G_4$ linearly independent linear dependencies of the power 2 and 1, respectively. It therefore suffices to prove that there are $G_2 - G_3 + G_4$ linearly independent dependencies of the power 0. Applying Theorem 3.2 with $S = S'$ sets of cardinality 2 we obtain G_2 dependencies of the power 0. For $i, j \in \{1, 2, 3, 4\}$ let $g_{ij} = |a_i b_j - a_j b_i|$. The dependencies with $S = \{i, j\}$ are of the form

$$\sum_{h \in H_i} s(i, h) - \sum_{h \in H_j} s(j, h) = 0, \tag{3.6}$$

where $H_i = \{h : h \equiv d_i \mod g_{ij}\}$ and $H_j = \{h : h \equiv d_j \mod g_{ij}\}$ for some d_i, d_j.

Let $g_{123} = \gcd(g_{12}, g_{13}, g_{23})$ and define g_{124}, g_{134} and g_{234} similarly. Let $H'_1 = \{h : h \equiv d'_1 \mod g_{123}\}$ for some d'_1 and let H'_2 and H'_3 corresponding sets of values of h in directions (a_2, b_2) and (a_3, b_3) respectively. Then the following are linear combinations of dependencies of the form (3.6):

$$\sum_{h \in H'_1} s(1, h) - \sum_{h \in H'_2} s(2, h) = 0,$$

$$-\sum_{h\in H_1'} s(1,h) + \sum_{h\in H_3'} s(3,h) = 0.$$

$$\sum_{h\in H_2'} s(2,h) - \sum_{h\in H_3'} s(3,h) = 0,$$

It is obvious that these three dependencies are linearly dependent. The dependency between those three we call $Z_{123}(B)$, where B is the set of points through which the lines in the direction (a_1, b_1) with $h \in H_1'$ pass. There are $g_{123} - 1$ other dependencies on the translates of B.

Define $Z_{124}(B)$, $Z_{134}(B)$ and $Z_{234}(B)$ in a similar way. Note that the sets B here are not the same.

Let $g = \gcd(g_{123}, g_{124}, g_{134}, g_{234}) = G_4$. By combining $\frac{g_{123}}{g}$ dependencies $Z_{123}(B)$ with $\frac{g_{124}}{g}$ dependencies $Z_{124}(B)$ and $\frac{g_{134}}{g}$ dependencies $Z_{134}(B)$, we can create a combination of $\frac{g_{234}}{g}$ dependencies $Z_{234}(B)$. So these dependencies $Z(B)$ are not all independent; there are at most $G_3 - G_4$ independent ones. If we prove that any dependency between dependencies of the form (3.6) can be written as a linear combination of dependencies $Z(B)$, then it will follow that there are at least $G_2 - G_3 + G_4$ linearly independent global dependencies of the power 0.

Consider linear combinations of dependencies of the form (3.6):

$$\begin{array}{lllllllll}
D_1: & \sum_h c^{(1)}_{1,h} s(1,h) & + & \sum_h c^{(1)}_{2,h} s(2,h) & & & & & = 0, \\
D_2: & \sum_h c^{(2)}_{1,h} s(1,h) & & & + & \sum_h c^{(2)}_{3,h} s(3,h) & & & = 0, \\
D_3: & \sum_h c^{(3)}_{1,h} s(1,h) & & & & & + & \sum_h c^{(3)}_{4,h} s(4,h) & = 0, \\
D_4: & & & \sum_h c^{(4)}_{2,h} s(2,h) & + & \sum_h c^{(4)}_{3,h} s(3,h) & & & = 0, \\
D_5: & & & \sum_h c^{(5)}_{2,h} s(2,h) & & & + & \sum_h c^{(5)}_{4,h} s(4,h) & = 0, \\
D_6: & & & & & \sum_h c^{(6)}_{3,h} s(3,h) & + & \sum_h c^{(6)}_{4,h} s(4,h) & = 0.
\end{array}$$

Here $c^{(t)}_{j,h}$ is a periodic function of h for all j and t, with periods g_{12}, g_{13}, g_{14}, g_{23}, g_{24} and g_{34}, respectively. Assume that these six dependencies are linearly dependent and that the coefficients of the dependency between them have been absorbed in the dependencies themselves. Then we have

$$\sum_t c^{(t)}_{j,h} = 0$$

for all j and h, where the sum runs over all t for which $c^{(t)}_{j,h}$ exists.

We have

$$(c^{(2)}_{1,h}, c^{(3)}_{1,h}) = (c^{(2)}_{1,h'}, c^{(3)}_{1,h'})$$

if $h \equiv h' \mod \operatorname{lcm}(g_{13}, g_{14})$, so

$$c^{(1)}_{1,h} = -c^{(2)}_{1,h} - c^{(3)}_{1,h} = -c^{(2)}_{1,h'} - c^{(3)}_{1,h'} = c^{(1)}_{1,h'}$$

if $h \equiv h' \mod \operatorname{lcm}(g_{13}, g_{14})$. Hence $c^{(1)}_{1,h}$ is a periodic function of h with period

$$\gcd(g_{12}, \operatorname{lcm}(g_{13}, g_{14})) = \operatorname{lcm}(\gcd(g_{12}, g_{13}), \gcd(g_{12}, g_{14})) = \operatorname{lcm}(g_{123}, g_{124}).$$

Notice that we use Lemma 3.5 here.

Fix h and let s and r be integers. It holds that

$$\begin{aligned} c^{(1)}_{1,h} + c^{(1)}_{1,h+sg_{13}+rg_{14}} &= -c^{(2)}_{1,h} - c^{(3)}_{1,h} - c^{(2)}_{1,h+sg_{13}+rg_{14}} - c^{(3)}_{1,h+sg_{13}+rg_{14}} \\ &= -c^{(2)}_{1,h+sg_{13}} - c^{(3)}_{1,h+rg_{14}} - c^{(2)}_{1,h+rg_{14}} - c^{(3)}_{1,h+sg_{13}} \\ &= c^{(1)}_{1,h+sg_{13}} + c^{(1)}_{1,h+rg_{14}}. \end{aligned} \tag{3.7}$$

Now we define the numbers $\alpha_0, \alpha_g, \ldots, \alpha_{(g_{123}-1)g}$ and $\beta_0, \beta_g \ldots, \beta_{(g_{124}-1)g}$ as follows. Put $\alpha_0 = 0$ and $\beta_0 = c^{(1)}_{1,0}$. For each u' with $0 \leq u' \leq \frac{g_{124}}{g} - 1$ there is a unique u with $0 \leq u \leq \frac{g_{124}}{g} - 1$ such that $u' \cdot g \equiv u \cdot g_{13} \mod g_{124}$, because $\gcd(g_{13}, g_{124}) = g$. On the other hand, each u corresponds to a unique u'. For such a pair (u, u') define

$$\beta_{u'\cdot g} = c^{(1)}_{1,u\cdot g_{13}}.$$

For $u = 0$ we have $u' = 0$ and this coincides with the earlier definition of β_0. Similarly, there are pairs (v, v') with $0 \leq v \leq \frac{g_{123}}{g} - 1$, $0 \leq v' \leq \frac{g_{123}}{g} - 1$ and $v \cdot g_{14} \equiv v' \cdot g \mod g_{123}$. We define

$$\alpha_{v'\cdot g} = c^{(1)}_{1,v\cdot g_{14}} - c^{(1)}_{1,0}.$$

For $v = 0$ we have $v' = 0$ and this coincides with the earlier definition of α_0.

Now let $w \in \mathbb{Z}$ and define u' and v' such that $0 \leq u' \leq \frac{g_{124}}{g} - 1$, $0 \leq v' \leq \frac{g_{123}}{g} - 1$, $u' \cdot g \equiv w \cdot g \mod g_{124}$ and $v' \cdot g \equiv w \cdot g \mod g_{123}$. Let u and v such that (u, u') and (v, v') are pairs as above. Then we have

$$\alpha_{v'\cdot g} + \beta_{u'\cdot g} = c^{(1)}_{1,v\cdot g_{14}} - c^{(1)}_{1,0} + c^{(1)}_{1,u\cdot g_{13}} = c^{(1)}_{1,u\cdot g_{13}+v\cdot g_{14}},$$

where in the second step we use (3.7). We have

$$u \cdot g_{13} \equiv u' \cdot g \equiv w \cdot g \mod g_{124},$$

and

$$v \cdot g_{14} \equiv v' \cdot g \equiv w \cdot g \mod g_{123}.$$

As $g_{123} \mid g_{13}$ and $g_{124} \mid g_{14}$, it follows that

$$u \cdot g_{13} + v \cdot g_{14} \equiv w \cdot g \mod g_{124},$$

and

$$u \cdot g_{13} + v \cdot g_{14} \equiv w \cdot g \mod g_{123},$$

so

$$u \cdot g_{13} + v \cdot g_{14} \equiv w \cdot g \mod \operatorname{lcm}(g_{123}, g_{124}).$$

Hence, using that the period of the coefficients in D_1 is $\operatorname{lcm}(g_{123}, g_{124})$,

$$c^{(1)}_{1,u\cdot g_{13}+v\cdot g_{14}} = c^{(1)}_{1,w\cdot g}.$$

Therefore
$$\alpha_{v'\cdot g} + \beta_{u'\cdot g} = c^{(1)}_{1,w\cdot g}.$$
Now define $\alpha_1 = \ldots = \alpha_{g-1} = 0$ and $\beta_1 = c^{(1)}_{1,1}, \ldots, \beta_{g-1} = c^{(1)}_{1,g-1}$. Define α_i and β_j for all other values i and j with $0 \le i \le g_{123} - 1$ and $0 \le j \le g_{124} - 1$ similar to above. Then we have for each h
$$c^{(1)}_{1,h} = \alpha_{h'} + \beta_{h''}$$
for some h' and h'' with $h' \equiv h \mod g_{123}$ and $h'' \equiv h \mod g_{124}$.

Now take the dependencies $Z_{123}(B)$ for the various translations of B exactly $\alpha_0, \alpha_1, \ldots, \alpha_{g_{123}-1}$ times, and the dependencies $Z_{124}(B)$ exactly $\beta_0, \beta_1, \ldots, \beta_{g_{124}-1}$ times, and take them all together. We get a new dependency between five dependencies involving the pairs of directions 1 and 2, 1 and 3, 1 and 4, 2 and 3, and 2 and 4. We call them D'_1, D'_2, D'_3, D'_4 and D'_5, respectively. Because of what we showed above, we have $D'_1 = D_1$. Therefore $D_2 - D'_2$, $D_3 - D'_3$, $D_4 - D'_4$, $D_5 - D'_5$ and D_6 are also linearly dependent. The first two are the only ones featuring direction (a_1, b_1), so we find that the coefficients must be periodic with period $\gcd(g_{13}, g_{14}) = g_{134}$. Hence we can subtract appropriate multiples of $Z_{134}(B)$ in order to eliminate direction (a_1, b_1) completely. In the same way, we show that what is left is linear combination of $Z_{234}(B)$ for various B.

We have now shown that the dependency between dependencies we started with is in fact a linear combination of the $Z(B)$, which is what we had to prove.

3.4.4 The general case

It seems quite hard to generalise this approach for any k. For one thing, it becomes quite technical even for $k = 4$. Perhaps it is possible to simplify the proof, but there is another big problem. For the dependencies of the power $k-3$ we needed an upper bound on the number of dependencies between them. For the dependencies of the power $k-4$ (which we only did for $k = 4$) we needed an upper bound on the number of dependencies between them as well, but for that we needed a lower bound on the dependencies between those. In general, we would be dealing with dependencies between dependencies between dependencies between ... and so on. So in order to generalise this method, one would need a way to acquire those bounds without actually writing down the dependencies, perhaps by some form of induction.

3.5 The second approach

The idea of this approach is to pick exactly G_2 global dependencies in such a way that it is relatively easy to show that they are linearly independent of each other. Each dependency will be defined on a set containing a *forbidden point* that does not occur in any smaller dependencies, in some sense. That way, going from large to small dependencies, we can exclude them one by one from a linear dependency between them, until there is nothing left.

3.5.1 Choosing dependencies

For $S \subset \{1, 2, \ldots, k\}$ with $|S| \geq 2$, define

$$g(S) = \gcd_{i,j \in S} |a_i b_j - a_j b_i|.$$

Take $i \in S$ and define for $0 \leq c \leq g(S) - 1$

$$B_c(S) = \{(x, y) \in \mathbb{Z}^2 : a_i y - b_i x \equiv c \mod g(S).\}$$

Note that if we take a different i, we get the same sets $B_c(S)$ but possibly in a different order.

We pick for each S some sets $B_c(S)$ to apply Theorem 3.2 to and we assign to each $B_c(S)$ a *forbidden point* $(x, y) \in B_c(S)$. If we have already done this for sets S of cardinality larger than t, then for a set S with $|S| = t$ we do the following. Throw out all sets $B_c(S)$ that contain a forbidden point of a set $B_{c'}(S')$ with $S' \supsetneq S$. If there are sets that contain more than one forbidden point, then throw out arbitrary other sets as well, so that the number of sets that are thrown out is equal to the number of forbidden points for $S' \supsetneq S$. The sets that are left are called *chosen sets.*

The way we will choose the forbidden points later on will ensure that each set contains at most one forbidden point, so there is a unique way to pick the sets that are thrown out.

Let $\alpha(S)$ be the number of chosen sets $B_c(S)$. We have

$$\alpha(S) = g(S) - \sum_{S' \supsetneq S} \alpha(S'). \tag{3.8}$$

On each chosen set $B_c(S)$ we apply Theorem 3.2. Write $S = \{i_1, i_2, \ldots, i_l\}$, then we apply the theorem with each of the following sets as S':

$$\{i_1, i_2\}, \{i_1, i_3\}, \ldots, \{i_1, i_l\},$$

$$\{i_1, i_2, i_3\}, \{i_1, i_2, i_4\}, \ldots, \{i_1, i_2, i_l\},$$

$$\vdots$$

$$\{i_1, i_2, \ldots, i_l\}.$$

So of the power 0 we get $l-1$ dependencies, of the power 1 we get $l-2$ dependencies, ..., and of the power $l-2$ we get 1 dependency. In total this gives us

$$\sum_{i=1}^{l-1} i = \frac{1}{2} l(l-1) = \binom{l}{2}$$

dependencies.

Proposition 3.8. *By this method we pick exactly G_2 global dependencies.*

Proof. The number of dependencies we pick is

$$\sum_{|S|\geq 2} \alpha(S) \cdot \binom{|S|}{2}.$$

On the other hand we have

$$G_2 = \sum_{1\leq i<j\leq k} |a_i b_j - a_j b_i| = \sum_{|S|=2} g(S).$$

Hence we have to prove

$$\sum_{|S|\geq 2} \alpha(S) \cdot \binom{|S|}{2} = \sum_{|S|=2} g(S).$$

Distinguishing between $|S| = 2$ and $|S| \geq 3$ on the left-hand side and using (3.8), we get

$$\sum_{|S|=2} \left(g(S) - \sum_{S' \supsetneq S} \alpha(S') \right) + \sum_{|S|\geq 3} \alpha(S) \cdot \binom{|S|}{2} \stackrel{?}{=} \sum_{|S|=2} g(S).$$

Rearranging terms, we acquire

$$\sum_{|S|\geq 3} \alpha(S) \cdot \binom{|S|}{2} \stackrel{?}{=} \sum_{|S|=2} \sum_{S' \supsetneq S} \alpha(S').$$

For each S' with $|S'| \geq 3$, there are $\binom{|S'|}{2}$ sets S with $S = 2$ and $S' \supsetneq S$, so $\alpha(S')$ occurs exactly $\binom{|S'|}{2}$ times on the right-hand side. That proves the equality. □

Fix a set $B_{c'}(S')$. By definition of the chosen sets $B_c(S)$, the forbidden point of $B_{c'}(S')$ never occurs in a chosen set $B_c(S)$ with $S \subsetneq S'$. However, we would like for the forbidden point to not occur in any chosen set $B_c(S)$ with $|S| \leq |S'|$. But if $S \not\subset S'$, the forbidden point of $B_{c'}(S')$ is not taken into account when the sets $B_c(S)$ are chosen. Therefore we want the forbidden point of $B_{c'}(S')$ to be in the same set $B_c(S)$ as a forbidden point that *is* taken into account. In that case the set $B_c(S)$ containing the forbidden point of $B_{c'}(S')$ is thrown out because of the other forbidden point, so the forbidden point of $B_{c'}(S')$ then does not occur in any chosen set $B_c(S)$.

Let $S \not\subset S'$. Let S'' such that $S \subset S''$ and $S' \subset S''$ and let $B_{c''}(S'')$ such that $B_{c'}(S') \subset B_{c''}(S'')$. Let (x', y') be the forbidden point of $B_{c'}(S')$ and let (x'', y'') be the forbidden point of $B_{c''}(S'')$. Then we want that (x', y') and (x'', y'') are in the same set $B_c(S)$.

We will work this out in detail for the cases $k = 3$ and $k = 4$.

3.5.2 The case $k = 3$

Assume $k = 3$. Let $g_{123} = g(\{1, 2, 3\})$, $g_{12} = g(\{1, 2\})$, $g_{13} = g(\{1, 3\})$ and $g_{23} = g(\{2, 3\})$. Without loss of generality we may assume that $g_{123} = 1$. Otherwise we split $\mathbb{Z}^2$ into the

g_{123} parts $B_c(\{1,2,3\})$, and then any set $B_{c'}(S)$ is a subset of one of these parts, so we can consider all the parts separately.

For $S = \{1,2,3\}$ we have only one set $B_c(S) = A$ and no set is thrown away. We take $(0,0)$ as the forbidden point of A.

Now let $S = \{1,2\}$. If $g_{12} = g(S) = 1$, then all sets $B_c(S)$ are thrown out, so there is nothing to do. Suppose $g(S) > 1$ and let $B = B_c(S)$ be a chosen set, that is, a set that does not contain $(0,0)$. So we have

$$B = \{(x,y) \in \mathbb{Z}^2 : a_1y - b_1x \equiv c \mod g_{12}\},$$

with $c \not\equiv 0 \mod g_{12}$. Let $S' = \{1,3\}$. From the sets $B_{c'}(S')$ one is thrown away (namely the one with $c' = 0$) because of the forbidden point of A, and we want the forbidden point of B to be in this set. So for the forbidden point (x,y) of B we want to have

$$a_3y - b_3x \equiv 0 \mod g_{13}.$$

Similarly, we want for $S'' = \{2,3\}$ that

$$a_3y - b_3x \equiv 0 \mod g_{23}.$$

We can combine these two requirements by imposing

$$a_3y - b_3x \equiv 0 \mod \operatorname{lcm}(g_{13}, g_{23}). \tag{3.9}$$

Consider the point $(x_0,y_0) = (ua_3, ub_3)$ for some integer u. We have

$$a_3y_0 - b_3x_0 = ua_3b_3 - ua_3b_3 = 0,$$

so (x_0,y_0) satisfies (3.9). Furthermore,

$$a_1y_0 - b_1x_0 = ua_1b_3 - ua_3b_1 = \pm ug_{13},$$

so $(x_0,y_0) \in B$ if and only if $\pm ug_{13} \equiv c \mod g_{12}$. As $\gcd(g_{13}, g_{12}) = g_{123} = 1$ by Lemma 3.5, we can find an integer u such that $(x_0,y_0) \in B$. We take this point as the forbidden point of B. By construction, this point does not occur in any chosen set $B_{c'}(S')$ or $B_{c''}(S'')$. We choose forbidden points for S' and S'' in a similar way.

We have now picked forbidden points for all the chosen sets. On these sets we construct dependencies using Theorem 3.2 as described on page 24. We now want to prove that these dependencies are linearly independent.

Suppose that there is a linear dependency between the dependencies we have selected. We have picked only one dependency of the power 1, and by using Theorem 3.6 we may assume that it is linearly independent of the other dependencies. So we have a linear dependency between dependencies of the power 0.

The line in the direction (a_2,b_2) with $h = 0$ passes through the point $(0,0)$, which is not contained in any of the chosen sets for S, S' and S''. So none of these dependencies have a nonzero coefficient for $s(2,0)$. The dependency on A involving the directions (a_1,b_1) and

(a_3, b_3) obviously does not have a nonzero coefficient for $s(2, 0)$ either. However, the other dependency on A (the one involving (a_1, b_1) and (a_2, b_2)) does have a nonzero coefficient for $s(2, 0)$. So the latter dependency cannot be involved in the linear dependency between the dependencies. In a completely similar way, we show that the former dependency on A cannot be involved.

Only the dependencies for S, S' and S'' are left. Each of the sets of points on which these dependencies have been constructed contains a forbidden point. That point does not occur in any of the other sets except A. Since the dependencies on A have been eliminated, for each of the dependencies that are still left exist h and i such that this dependency is the only one with a nonzero coefficient for $s(i, h)$. So we can eliminate them all as well. We conclude that there is no linear dependency between the global dependencies we have chosen.

This solves the case $k = 3$.

3.5.3 The case $k = 4$

Assume $k = 4$. We use the usual notation $g_{12} = g(\{1, 2\})$ and so on. We may assume without loss of generality that $g_{1234} = 1$. For $S = \{1, 2, 3, 4\}$ there is only one set $B_c(S) = A$ and we choose $(0, 0)$ as the forbidden point of A.

Now let $S = \{1, 2, 3\}$. If $g_{123} = 1$, then no sets $B_c(S)$ are chosen and there is nothing to do. Assume $g_{123} > 1$ and let

$$B = \{(x, y) \in \mathbb{Z}^2 : a_1 y - b_1 x \equiv c \mod g_{123}\}$$

be a chosen set for S, so $c \not\equiv 0 \mod g_{123}$.

Each set S' with $S' \not\subset S$ and $S' \neq \{1, 2, 3, 4\}$ gives us a congruence that the forbidden point of B must satisfy. We list them all here:

$$\begin{aligned} a_4 y - b_4 x &\equiv 0 \mod g_{124} \\ a_4 y - b_4 x &\equiv 0 \mod g_{134} \\ a_4 y - b_4 x &\equiv 0 \mod g_{234} \\ a_4 y - b_4 x &\equiv 0 \mod g_{14} \\ a_4 y - b_4 x &\equiv 0 \mod g_{24} \\ a_4 y - b_4 x &\equiv 0 \mod g_{34} \end{aligned}$$

The last three imply the first three, and we can take the last three together:

$$a_4 y - b_4 x \equiv 0 \mod \operatorname{lcm}(g_{14}, g_{24}, g_{34}). \tag{3.10}$$

Consider the point $(x_0, y_0) = (ua_4, ub_4)$ for some integer u. We have

$$a_4 y_0 - b_4 x_0 = ua_4 b_4 - ua_4 b_4 = 0,$$

so (x_0, y_0) satisfies (3.10). Furthermore,

$$a_1 y_0 - b_1 x_0 = ua_1 b_4 - ua_4 b_1 = \pm u g_{14},$$

so $(x_0, y_0) \in B$ if and only if $\pm u g_{14} \equiv c \mod g_{123}$. As $\gcd(g_{14}, g_{123}) = g_{1234} = 1$ by Lemma 3.5, we can find an integer u such that $(x_0, y_0) \in B$. We take this point as the forbidden point of B.

We can find forbidden points for the other sets S with $|S| = 3$ in a similar way.

Now let $S = \{1, 2\}$. Assume that $\alpha(S) > 0$, so there exists at least one set $B_c(S)$ for which we need to find a forbidden point. Let

$$B = \{(x, y) \in \mathbb{Z}^2 : a_1 y - b_1 x \equiv c \mod g_{12}\}$$

be a chosen set. Deriving the congruences is a little more complicated than before, as we now have more forbidden points. Let $B_{c'}(\{1, 2, 3\})$ be the set (chosen or thrown out) that contains B as a subset. If it is a chosen set, then let (x', y') be its forbidden point. If it has been thrown out, then it contains $(0, 0)$ and we take $(x', y') = (0, 0)$. In both cases we have

$$a_1 y' - b_1 x' \equiv a_1 y - b_1 x \mod g_{123} \tag{3.11}$$

for all points $(x, y) \in B$. We define (x'', y'') similarly for the set $\{1, 2, 4\}$ and we have

$$a_1 y'' - b_1 x'' \equiv a_1 y - b_1 x \mod g_{124} \tag{3.12}$$

for all points $(x, y) \in B$.

For $\{1, 3\}$ and $\{2, 3\}$ we want the forbidden point (x, y) of B to be in the same set as (x', y'), so we want

$$\begin{aligned} a_3 y - b_3 x &\equiv a_3 y' - b_3 x' \mod g_{13} \\ a_3 y - b_3 x &\equiv a_3 y' - b_3 x' \mod g_{23} \end{aligned}$$

We can take them together:

$$a_3 y - b_3 x \equiv a_3 y' - b_3 x' \mod \operatorname{lcm}(g_{13}, g_{23}). \tag{3.13}$$

Analogously, for $\{1, 4\}$ and $\{2, 4\}$ we get

$$a_4 y - b_4 x \equiv a_4 y'' - b_4 x'' \mod \operatorname{lcm}(g_{14}, g_{24}). \tag{3.14}$$

Finally, for $\{3, 4\}$ we want the forbidden point of B to be in the same set as $(0, 0)$, so

$$a_4 y - b_4 x \equiv 0 \mod g_{34}. \tag{3.15}$$

Consider the point $(x_0, y_0) = (x' + u a_3, y' + u b_3)$. We have

$$a_3 y_0 - b_3 x_0 = a_3 y' - b_3 x' + u a_3 b_3 - u a_3 b_3 = a_3 y' - b_3 x',$$

so (x_0, y_0) satisfies (3.13). Furthermore,

$$a_1 y_0 - b_1 x_0 = a_1 y' - b_1 x' + u(a_1 b_3 - a_3 b_1),$$

so $(x_0, y_0) \in B$ if and only if $a_1y' - b_1x' \pm ug_{13} \equiv c \mod g_{12}$. As $\gcd(g_{13}, g_{12}) = g_{123}$, we can find an integer u such that $(x_0, y_0) \in B$ if and only if $a_1y' - b_1x' \equiv c \mod g_{123}$. The latter follows from (3.11), so we can find a point (x_0, y_0) that is in B and satisfies (3.13).

Consider the point $(x_1, y_1) = (x_0 + v_1 \cdot \mathrm{lcm}(g_{12}, g_{13}, g_{23}), y_0 + v_2 \cdot \mathrm{lcm}(g_{12}, g_{13}, g_{23}))$. It is clear that this point is also in B and satisfies (3.13). Furthermore,

$$a_4y_1 - b_4x_1 = a_4y_0 - b_4x_0 + (v_2a_4 - v_1b_4) \cdot \mathrm{lcm}(g_{12}, g_{13}, g_{23}).$$

As $\gcd(a_4, b_4) = 1$, the linear combination $v_2a_4 - v_1b_4$ of a_4 and b_4 can assume any integer value. It holds that

$$\gcd(\mathrm{lcm}(g_{14}, g_{24}), \mathrm{lcm}(g_{12}, g_{13}, g_{23})) = \mathrm{lcm}(g_{124}, g_{134}, g_{234}),$$

so we can take v_1 and v_2 such that (x_1, y_1) satisfies (3.14) if and only if

$$a_4y_0 - b_4x_0 \equiv a_4y'' - b_4x'' \mod \mathrm{lcm}(g_{124}, g_{134}, g_{234}).$$

We will prove that indeed

$$a_4y_0 - b_4x_0 \equiv a_4y'' - b_4x'' \mod g_{124}, \tag{3.16}$$
$$a_4y_0 - b_4x_0 \equiv a_4y'' - b_4x'' \mod g_{134}, \tag{3.17}$$
$$a_4y_0 - b_4x_0 \equiv a_4y'' - b_4x'' \mod g_{234}. \tag{3.18}$$

According to (3.12),

$$a_1y_0 - b_1x_0 \equiv a_1y'' - b_1x'' \mod g_{124}.$$

By applying Lemma 3.1 with $Y = y_0 - y''$ and $X = x_0 - x''$, we acquire (3.16). Now consider that (x', y') was chosen such that for $\{3, 4\}$ it ended up in the same set as the forbidden point of A, which is $(0, 0)$. So

$$a_4y' - b_4x' \equiv 0 \mod g_{34}.$$

Analogously,

$$a_4y'' - b_4x'' \equiv 0 \mod g_{34},$$

hence

$$a_4y' - b_4x' \equiv a_4y'' - b_4x'' \mod g_{34}. \tag{3.19}$$

Also, (x_0, y_0) satisfies (3.13), so in particular

$$a_3y_0 - b_3x_0 \equiv a_3y' - b_3x' \mod g_{134}.$$

Applying Lemma 3.1 again, we get

$$a_4y_0 - b_4x_0 \equiv a_4y' - b_4x' \mod g_{134}$$

and therefore, using (3.19),

$$a_4y_0 - b_4x_0 \equiv a_4y'' - b_4x'' \mod g_{134},$$

which proves (3.17). In a completely similar way we can derive (3.18) from (3.13) and (3.19), now using g_{234} rather than g_{134}.

This proves that we can find a point $(x_1, y_1) \in B$ that satisfies both (3.13) and (3.14). Now consider

$$(x_2, y_2) = (x_1 + w_1 \cdot \operatorname{lcm}(g_{12}, g_{13}, g_{23}, g_{14}, g_{24}), y_1 + w_2 \cdot \operatorname{lcm}(g_{12}, g_{13}, g_{23}, g_{14}, g_{24})).$$

It is clear that this point is in B and satisfies both (3.13) and (3.14). We now want to choose w_1 and w_2 in such a way that it also satisfies (3.15). We have

$$a_4 y_2 - b_4 x_2 = a_4 y_1 - b_4 x_1 + (a_4 w_2 - b_4 w_1) \cdot \operatorname{lcm}(g_{12}, g_{13}, g_{23}, g_{14}, g_{24}).$$

As $\gcd(a_4, b_4) = 1$, the linear combination $w_2 a_4 - w_1 b_4$ of a_4 and b_4 can assume any integer value. Since

$$\gcd(g_{34}, \operatorname{lcm}(g_{12}, g_{13}, g_{23}, g_{14}, g_{24})) = \operatorname{lcm}(g_{134}, g_{234}),$$

we can choose w_1 and w_2 such that (x_2, y_2) satisfies (3.15) if and only if

$$a_4 y_1 - b_4 x_1 \equiv 0 \mod \operatorname{lcm}(g_{134}, g_{234}).$$

Hence we have to prove

$$a_4 y_1 - b_4 x_1 \equiv 0 \mod g_{134}, \qquad (3.20)$$
$$a_4 y_1 - b_4 x_1 \equiv 0 \mod g_{234}. \qquad (3.21)$$

We know that (x_1, y_1) satisfies (3.13), so in particular

$$a_3 y_1 - b_3 x_1 \equiv a_3 y' - b_3 x' \mod g_{134}.$$

Applying Lemma 3.1 and using that $a_4 y' - b_4 x' \equiv 0 \mod g_{34}$ and therefore also $a_4 y' - b_4 x' \equiv 0 \mod g_{134}$, we find precisely (3.20). We can derive (3.21) analogously.

We have now found a point (x_2, y_2) that is in B and satisfies all three requirements (3.13), (3.14) and (3.15). We can take this point as the forbidden point of B. We can find forbidden points for the other sets S with $|S| = 2$ in a similar way.

For each chosen set $B_c(S)$ we have now found a forbidden point that does not occur in any chosen set $B_{c'}(S')$ if $|S'| \leq |S|$ and $S' \neq S$. Analogously to the case $k = 3$, this means that the global dependencies of the power 0 that we have selected are all linearly independent of each other.

For the dependencies of the power 1 and 2 we have to be a little more careful. The argument we use for the power 0 is bases on the fact that a certain coefficient is nonzero for only one dependency. However, in the case of higher powers, the coefficients are multiplied by the corresponding power of h. Therefore, the argument will not hold if $h = 0$. Since $(0, 0)$ is the forbidden point of A, none of the dependencies defined on sets $B \neq A$ have a nonzero coefficient of $s(j, 0)$ for any j. So the only problematic forbidden point is $(0, 0)$.

However, notice that if $(0,0)$ does not occur in any set $B_c(S)$ for $|S| < 4$, then neither does the point

$$(u \cdot \mathrm{lcm}(g_{12}, g_{13}, g_{23}, g_{14}, g_{24}, g_{34}), v \cdot \mathrm{lcm}(g_{12}, g_{13}, g_{23}, g_{14}, g_{24}, g_{34})),$$

where u and v are integers. Such a point lies on the line in the direction (a_i, b_i) with $h = 0$ if and only if $a_i v - b_i u = 0$. As there are only four possibilities for i, we can easily find u and v such that this does not happen for any i. Then we can replace $(0,0)$ as the forbidden point of A by this new point, and we can use the same argument after all.

This solves the case $k = 4$.

3.5.4 The general case

It seems quite feasible to prove the general case by using an approach similar to this. However, there are several problems with this.

While picking new forbidden points, we have to take into account the forbidden points that are already there. In the case $k = 3$ as well as in the case $k = 4$ for $|S| = 3$, this is only the point $(0,0)$, which makes things quite easy. In the case $k = 4$ and $|S| = 2$, we already had to use three different forbidden points and the relations between them (such as (3.19)). In the general case, there are a huge number of forbidden points and things become rather complicated.

Another problem is that with larger k it may happen that if S_1 and S_2 are disjoint, then $\gcd(g(S_1), g(S_2)) \neq g(S_1 \cup S_2)$ (compare Lemma 3.5). The more complicated relation

$$\gcd(g(S_1), g(S_2), a_i b_j - a_j b_i) = g(S_1 \cup S_2)$$

holds, where $i \in S_1$ and $j \in S_2$. This complication makes reasonings like the ones we have used above much more difficult.

Chapter 4

Local dependencies

Local dependencies involve only a limited number of line sums, corresponding to lines passing through points in a corner of the rectangle A. Directions with a positive b give local dependencies in the lower right corner as well as the upper left corner, while directions with a negative b give local dependencies in the lower left corner as well as the upper right corner. In this chapter we will only construct the dependencies in the lower right corner. The others can be constructed analogously.

Let $\{(a_i, b_i)\}_{i=1}^{k}$ be a set of directions with $b_i > 0$ for $1 \leq i \leq k$. Assume without loss of generality that

$$\frac{b_1}{a_1} > \frac{b_2}{a_2} > \cdots > \frac{b_k}{a_k}. \tag{4.1}$$

Define the *lower right corner* of A as the points of A within or on the triangle with vertices $(m-1, 0)$, $(m-(a_1+a_2+\ldots+a_k), 0)$ and $(m-1, b_1+b_2+\ldots+b_k-1)$. Assume that m and n are sufficiently large so that all those points belong to A.

Theorem 4.1. *There exist $a_1(b_2+\ldots+b_k)$ linear dependencies involving at least one line in the direction (a_1, b_1) and $\sum_{2\leq i<j\leq k} a_i b_j$ linear dependencies involving only lines in the directions (a_2, b_2), ..., (a_k, b_k), such that all of these $\sum_{1\leq i<j\leq k} a_i b_j$ dependencies are linearly independent and pass only through points in the lower right corner of A.*

The total number of local dependencies according to this theorem agrees with the number mentioned in Conjecture 2.2. So this theorem, together with its analogous counterparts for the other corners, proves the local part of Conjecture 2.2.

4.1 The lines

We will first construct a set of lines to make a dependency on. We will call this set S. The first line of this set will have some special properties, as mentioned in the following definition. We will regularly refer back to this definition.

Definition 4.1. *Let l_1 be a line in the direction (a_1, b_1) such that for the rightmost point (x_1, y_1) on this line it holds that $y_1 < b_2+\ldots+b_k$.*

Start with S consisting only of the line l_1. For $i = 2, 3, \dots, k$ let $(x_i, y_i) = (x_{i-1} - a_i, y_{i-1} - b_i)$. Through the points (x_{i-1}, y_{i-1}) and (x_i, y_i) passes a line in the direction (a_i, b_i). Call this line l_i and add it to S. See Figure 4.1.

Now S contains exactly one line in each direction. We add more lines to S with the following procedure. See Figure 4.2.

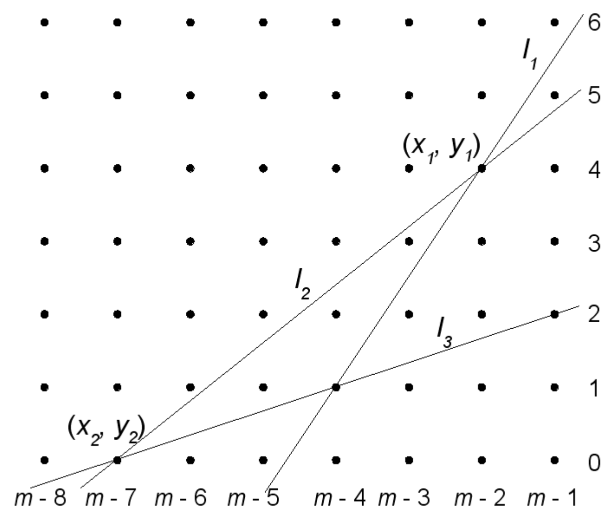

Figure 4.1: An example for the directions $(2, 3)$, $(5, 4)$ and $(3, 1)$.

- If one of the lines in S contains a point (x, y) with $x > x_1$, then add the line in the direction (a_1, b_1) through (x, y) to S.
- Let $2 \leq i \leq k - 1$. If one of the lines in S contains a point (x, y) with $x_i < x \leq x_{i-1}$, then add the line in the direction (a_i, b_i) through (x, y) to S.
- If one of the lines in S contains a point (x, y) with $x \leq x_{k-1}$, then add the line in the direction (a_k, b_k) through (x, y) to S.

Repeat this until no more lines can be added according to the above.

Proposition 4.2. *For all r, all lines in the direction (a_r, b_r) in S are lying below l_r unless they are equal to l_r.*

Proof. For $1 \leq i \leq k - 1$, the lines l_i and l_{i+1} intersect in (x_i, y_i). Since $\frac{b_i}{a_i} > \frac{b_{i+1}}{a_{i+1}}$, the line l_i lies above l_{i+1} to the right of (x_i, y_i) and below l_{i+1} to the left of (x_i, y_i). Now let $j > i$. To the right of (x_i, y_i), the line l_i lies above l_{i+1}, which lies above l_{i+2}, and so on, and l_{j-1} lies above l_j. So l_i lies above l_j. Similarly, to the left of (x_{j-1}, y_{j-1}), the line l_i lies below l_j.

Now let $1 \leq t \leq k$ and let p be a line in the direction (a_t, b_t) that lies below l_t or is equal to l_t. Let (x, y) be a point on p. If $x > x_1$, take $r = 1$. If $x \leq x_{k-1}$, take $r = k$. Otherwise, take i such that $x_r < x \leq x_{r-1}$.

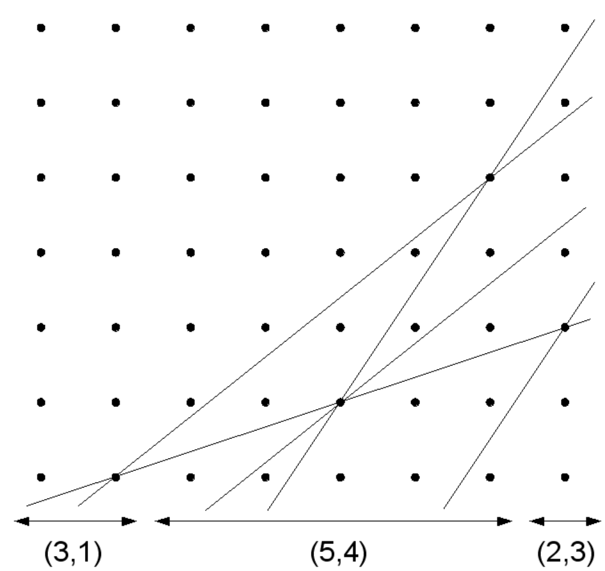

Figure 4.2: The example from Figure 4.1 continued. New lines should be drawn in the directions indicated below.

Let q be the line in the direction (a_r, b_r) that passes through (x, y). We will prove that q lies below l_r unless it is equal to l_r.

Since p is lying below l_t or is equal to l_t, the point (x, y) lies below or on l_t. Since $x_r < x \leq x_{r-1}$, this implies that (x, y) lies below or on l_r. Therefore q also lies below or on l_r. This shows that every new line in the direction (a_r, b_r) that is added to S lies below l_r. □

Corollary 4.3. *The procedure of adding lines to S always terminates.*

Proof. For each i, there are only finitely many lines in the direction (a_i, b_i) lying below l_i and passing through at least one point in A. □

Proposition 4.4. *The lines in S pass only through points that are in the lower right corner of A, as defined above.*

Proof. For the point (x_1, y_1) we have $x_1 \geq m - a_1$ and $y_1 < b_2 + \ldots + b_k$ according to Definition 4.1. To the right of this point, all other lines in S are lying below l_1, so any points (x, y) on these lines with $x \geq x_1$ satisfy $y < b_1 + b_2 + \ldots + b_k$. Similarly, points (x, y) with $y \leq y_{k-1}$ satisfy $x \geq m - (a_1 + a_2 + \ldots + a_k)$. Because the lines $l_1, l_2, \ldots, l_k$ are ordered by steepness, these lines and therefore all other lines in S only pass through points within or on the triangle with vertices $(m - 1, 0)$, $(m - (a_1 + a_2 + \ldots + a_k), 0)$ and $(m - 1, b_1 + b_2 + \ldots + b_k - 1)$. □

Definition 4.2. *Let $1 \leq i \leq k$ and let p be a line in S in the direction (a_i, b_i). A* defining point *of p is a point (x, y) on p with the following property:*

$$\begin{cases} x > x_1 & \text{if } i = 1, \\ x_i < x \leq x_{i-1} & \text{if } 2 \leq i \leq k-1 \\ x \leq x_{k-1} & \text{if } i = k. \end{cases}$$

Proposition 4.5. *Every line in S except l_1 contains exactly one defining point. The line l_1 contains no defining point.*

Proof. The statement about l_1 follows directly from the definition of x_1. Now let $2 \leq i \leq k - 1$. We have $x_{i-1} - x_i = a_i$, which immediately implies that every line in the direction (a_i, b_i) contains at most one point (x, y) with $x_i < x \leq x_{i-1}$. The point (x_{i-1}, y_{i-1}) is a defining point of l_i. For any other line the existence of a defining point follows from the fact that the line has been added to S. So each line in S in the direction (a_i, b_i) contains exactly one defining point.

From Definition 4.1 it follows that $y_{k-1} = y_1 - b_2 - b_3 - \ldots - b_{k-1} < b_k$. So there are no points on l_k to the left of (x_{k-1}, y_{k-1}). Therefore l_k contains exactly one defining point, namely (x_{k-1}, y_{k-1}). Now let p be another line in S in the direction (a_k, b_k). Since this line is in S, it must contain a point $(x, y) \in A$ with $x \leq x_{k-1}$. Now suppose there are two points (x, y) and (x', y') on p with $x, x' \leq x_{k-1}$. As p is lying below l_k by Proposition 4.2, it must hold that $y, y' < b_k$. However, the difference between y and y' must be at least b_k. Contradiction. So p contains exactly one defining point. □

Let T be the set of points $(x, y) \in A$ with the property that through (x, y) passes at least one line in S.

Lemma 4.6. *Every point in T is the defining point of exactly one line in S.*

Proof. Let $(x, y) \in T$. Set $i = 1$ if $x > x_1$, set $i = k$ if $x \leq x_{k-1}$ and otherwise set i such that $x_i < x \leq x_{i-1}$. There is a line in S passing through (x, y). Because of the construction of S, there must also be a line $p \in S$ in the direction (a_i, b_i) passing through (x, y). Hence (x, y) is the defining point of p.

On the other hand, if (x, y) is the defining point of some line, then the direction of that line must be (a_i, b_i). Since only one line in the direction (a_i, b_i) passes through (x, y), there can only be one line of which (x, y) is the defining point. □

4.2 The coefficients

We will now prove that there exists a dependency between the line sums of the lines in S. For $p \in S$ let $s(p)$ denote the sum of the values of the points on p. We will show that there exist coefficients c_p, $p \in S$, such that

$$\sum_{p \in S} c_p s(p) = 0.$$

Moreover, we will be able to choose the coefficients in such a way that the coefficient of l_1 is equal to 1.

Consider lines $p_1, \ldots, p_k$ in S, where p_i is a line in the direction (a_i, b_i) with defining point (x'_i, y'_i). We do not allow l_1 to be one of these lines, so according to Proposition 4.5, the points (x'_i, y'_i) exist and are unique.

A point (x'_i, y'_i) is lying on or below p_j if and only if the line in the direction (a_j, b_j) through (x'_i, y'_i) is equal to p_j or lying below p_j. This is equivalent to

$$a_j y'_i - b_j x'_i \leq a_j y'_j - b_j x'_j.$$

Lemma 4.7. *Let r, s and t be integers from $\{1, 2, \ldots, k\}$ such that $r < t$ and $s < t$. Suppose that (x'_r, y'_r) lies on or below p_t and (x'_t, y'_t) lies on or below p_s. Then (x'_r, y'_r) lies below p_s.*

Proof. The point (x'_r, y'_r) lies on or below p_t, so

$$a_t y'_r - b_t x'_r \leq a_t y'_t - b_t x'_t,$$

or equivalently

$$a_t (y'_r - y'_t) \leq b_t (x'_r - x'_t).$$

Since $r < t$, we have $x'_r - x'_t > 0$. Also, since $s < t$, we have $\frac{b_s}{a_s} > \frac{b_t}{a_t}$. So

$$y'_r - y'_t \leq \frac{b_t}{a_t}(x'_r - x'_t) < \frac{b_s}{a_s}(x'_r - x'_t),$$

which we can rewrite as

$$a_s y'_r - b_s x'_r < a_s y'_t - b_s x'_t.$$

As (x'_t, y'_t) lies on or below p_s, we have

$$a_s y'_t - b_s x'_t \leq a_s y'_s - b_s x'_s,$$

so

$$a_s y'_r - b_s x'_r < a_s y'_s - b_s x'_s.$$

This means that (x'_r, y'_r) lies below p_s. □

Lemma 4.8. *There exists an $i \in \{1, 2, \ldots, k\}$ such that for all $j \neq i$, the point (x'_i, y'_i) is lying above p_j.*

Proof. We will prove this by contradiction. Suppose that for all i there exists a $j \neq i$ such that (x'_i, y'_i) is lying on or below p_j. Then there must be a sequence of distinct integers $i(1), i(2), \ldots, i(v)$ for some $v \geq 2$ such that for $1 \leq j \leq v$ the point $(x'_{i(j)}, y'_{i(j)})$ is lying on or below $p_{i(j+1)}$, where we define $i(v+1) = i(1)$. Without loss of generality, we may assume that $i(1) = \min_{1 \leq j \leq v} i(j)$.

Now let j be minimal with the property that $i(j) < i(j-1)$. Then $3 \leq j \leq v+1$. Now apply Lemma 4.7 with $r = i(j-2)$, $t = i(j-1)$ and $s = i(j)$. We find that $(x'_{i(j-2)}, y'_{i(j-2)})$ lies below $p_{i(j)}$. So we can omit $i(j-1)$ from the sequence. Repeat this step for the new sequence until no j exists with $i(j) < i(j-1)$.

For the new sequence $i(1), i(2), \ldots, i(w)$ we now have $i(j) \leq i(j+1)$ for all j with $1 \leq j \leq w$ with equality if and only if $w = 1$. However, $i(w+1) = i(1)$, so apparently $w = 1$. Since $v \geq 2$, at least one element has been omitted from the original sequence. So during this process there has been a sequence consisting of exactly two elements, r and s, with $r < s$. Now the point (x'_r, y'_r) lies on or below p_s and the point (x'_s, y'_s) lies on or below p_r. So

$$a_s y'_r - b_s x'_r \leq a_s y'_s - b_s x'_s.$$

Since $r < s$, we have $x'_r - x'_s > 0$ and $\frac{b_s}{a_s} < \frac{b_r}{a_r}$. Therefore

$$y'_r - y'_s \leq \frac{b_s}{a_s}(x'_r - x'_s) < \frac{b_r}{a_r}(x'_r - x'_s),$$

which we can rewrite as

$$a_r y'_r - b_r x'_r < a_r y'_s - b_r x'_s.$$

This is a contradiction with the fact that (x'_s, y'_s) lies below or on p_r. □

Now we can prove the existence of the dependency.

Proposition 4.9. *There are coefficients c_p, $p \in S$, such that*

$$\sum_{p \in S} c_p s(p) = 0$$

and $c_{l_1} = 1$.

Proof. We will assign coefficients to the lines one by one in the following way.

Start by setting $c_{l_1} = 1$. If not all lines have now been assigned a coefficient, then (as we will prove below) there is a line $p \in S$ with defining point (x, y) such that p has not yet been assigned a coefficient, but all other lines passing though (x, y) have been assigned a coefficient. Now set the coefficient of p such that the sum of the coefficients of all lines in S passing through (x, y) is equal to 0. Repeat this until the coefficients of all lines in S have been set. See Figure 4.3.

First we will prove that such a line p always exists. For $i = 1, 2, \ldots, k$ let p_i be the line in the direction (a_i, b_i) with the property that it has not yet been assigned a coefficient and that all lines in S in the direction (a_i, b_i) lying above p_i have already been assigned a coefficient. So p_i is the highest line in its direction of which the coefficient has not yet been determined. Now p_1 cannot be equal to l_1, as the coefficient of l_1 has already been set, so we can for all i define (x'_i, y'_i) as the defining point of p_i.

According to Lemma 4.8, there exists an i such that (x'_i, y'_i) is lying above p_j for all $j \neq i$. If through (x'_i, y'_i) passes a line in the direction (a_j, b_j) with $j \neq i$ that has not yet been assigned a coefficient, then (x'_i, y'_i) must be lying on or below p_j. That yields a contradiction if $j \neq i$. So through (x'_i, y'_i) pass only lines that have already been assigned a coefficient, with the exception of p_i itself. Now take $p = p_i$.

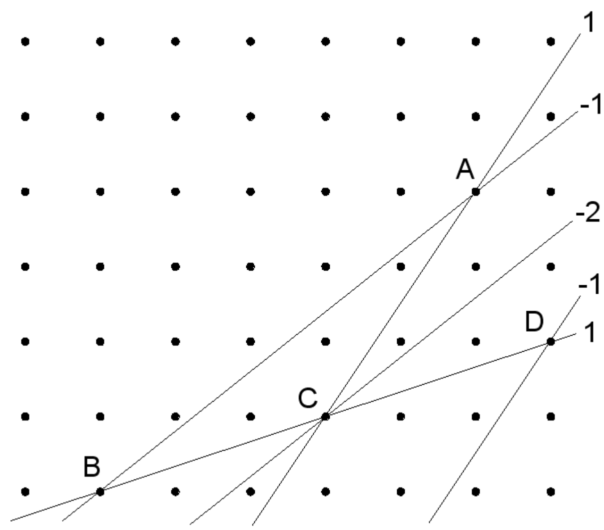

Figure 4.3: The example from Figure 4.2 continued. The coefficients of the lines are indicated next to the lines. The coefficients can be determined by looking at the points A, B, C and D in that order.

In this way, each line is assigned a coefficient exactly once, because of Proposition 4.5. Also, every point in T is a defining point for some line according to Lemma 4.6. Therefore, we have for each $(x, y) \in T$:

$$\sum_{p:(x,y) \in p} c_p = 0.$$

Now if $f(x, y)$ denotes the value attached to the point (x, y), we have

$$\sum_{p \in S} c_p s(p) = \sum_{p \in S} c_p \sum_{(x,y) \in p} f(x, y) = \sum_{(x,y) \in T} f(x, y) \sum_{p:(x,y) \in p} c_p = 0.$$

□

Remarks.

1. By Proposition 4.5 and Lemma 4.6, the number of lines in S is one more than the number of points in T. As a line sum is a linear expression in the values of the points on that line, this immediately implies that there exists a linear dependency between the line sums of the lines in S. However, it is not clear that the coefficient of l_1 in this dependency is not zero, and this is something we need in order to count the linearly independent dependencies.

2. Some of the coefficients determined in Proposition 4.9 may be zero. So not necessarily all lines in S are needed to construct a dependency.

4.3 Summing up

Now we are ready to prove Theorem 4.1. In the previous two sections, we constructed a linear dependency between line sums that contains a line l_1 satisfying Definition 4.1. Any other lines in the direction (a_1, b_1) that are involved in this dependency are lying below l_1.

Now suppose we have a set $\{l_{11}, l_{12}, \ldots, l_{1t}\}$ of lines satisfying Definition 4.1, ordered in such a way that l_{1i} is lying above l_{1j} if $i < j$. With each of the lines l_{1i}, we construct a dependency D_i with $l_1 = l_{1i}$. We write this dependency as

$$\sum_{p \in S_i} c_{pi} s(p) = 0.$$

Assume that all these dependencies are not linearly independent, so there exists a dependency

$$\sum_{i=1}^{t} c_i D_i = 0$$

between them, with c_i not all equal to zero. Now for each line p that occurs in at least one dependency, we must have

$$\sum_{i: p \in S_i} c_i c_{pi} = 0.$$

Let j be the smallest index such that $c_j \neq 0$. The dependency D_j contains the line l_{1j} with coefficient 1, but the dependencies D_i with $i > j$ do not contain l_{1j} at all. Since $c_i = 0$ for $i < j$, we have

$$\sum_{i: l_{1j} \in S_i} c_i c_{pi} = c_j \cdot 1 \neq 0.$$

Contradiction. We conclude that $D_1, D_2, \ldots, D_t$ are linearly independent.

Now consider the set $B = \{(x, y) \in A : x \geq m - a_1, y < b_2 + \ldots + b_k\}$. Let l be a line in the direction (a_1, b_1) passing through a point (x, y) of B. Then it passes through exactly one point of B and (x, y) is the rightmost point on l, as $x \geq m - a_1$. Since $y < b_2 + \ldots + b_k$, the line l satisfies Definition 4.1. The number of points in B is equal to $a_1(b_2 + \ldots + b_k)$. So there exist at least $a_1(b_2 + \ldots + b_k)$ lines that satisfy Definition 4.1.

Proposition 4.4 shows that all these dependencies pass only through points in the lower right corner of A. This concludes the proof of Theorem 4.1.

Remark. It is easy to see that in fact the only lines satisfying Definition 4.1 are the ones that pass through a point of B. However, we do not need this.

We have now shown that it is possible to construct a basis of local dependencies in the lower right corner consisting of

$$\begin{array}{rl} a_1b_2 + a_1b_3 + \ldots + a_1b_k & \text{dependencies involving directions } (a_1, b_1), (a_2, b_2), \ldots, (a_k, b_k), \\ a_2b_3 + \ldots + a_2b_k & \text{dependencies involving directions } (a_2, b_2), (a_3, b_3), \ldots, (a_k, b_k), \\ \ddots \quad \vdots & \\ a_{k-1}b_k & \text{dependencies involving directions } (a_{k-1}, b_{k-1}) \text{ and } (a_k, b_k). \end{array}$$

Chapter 5

Conclusions

Our goal was to construct a basis for the linear dependencies between the line sums, given any valid set of directions. Here *valid* means that $\sum_{i=1}^{k} a_i < m$ and $\sum_{i=1}^{k} |b_i| < n$. We have not completely reached this goal; however, we have acquired some partial results.

We have distinguished between global and local dependencies. Global dependencies can in some sense be defined on the entire $\mathbb{Z}^2$. To avoid infinite sums of values in $\mathbb{Z}$, we use finite subsets of $\mathbb{Z}^2$ instead, but the dependencies are essentially the same no matter what finite subset we use. Local dependencies, on the other hand, depend on the shape of the subset. We have studied them for a rectangle, in which case they involve line sums in a corner of the rectangle. In the case of other subsets of $\mathbb{Z}^2$ there will also be lines passing through only a few points, causing local dependencies, though obviously different ones than in the case of a rectangle.

In Chapter 4 we have constructed the exact number of local dependencies that agrees with Conjecture 2.2, and we have shown that they are all linearly independent of each other.

In Chapter 3 we have constructed the exact number of global dependencies that agrees with Conjecture 2.2 in the case $k \leq 4$, and we have shown that they are all linearly independent of each other. However, the condition that the set of directions is *valid* is not sufficient for the proofs we gave. We need a far larger m and n than the validness provides.

For the case $k \geq 5$ we have not succeeded in constructing a basis for the global dependencies. This also means that the number of local dependencies we have found is for now merely a lower bound. It may be possible to generalise one of the two approaches described in Chapter 3 to find global dependencies for any k. The second one seems to be the most promising in that aspect, although it is probably necessary to simplify it before generalising.

Summarising, we have solved the problem for $k \leq 4$, although we need fairly large values for m and n. We have only partially solved the problem for $k \geq 5$: we have not been able to prove the linear independency of the global dependencies.

Another interesting question that is left open is what happens when we change the shape of A. As pointed out before, the global dependencies do not depend on the shape of A, while the local ones do. Perhaps one could generalise the method from Chapter 4 in order to find local dependencies of any convex subset A of $\mathbb{Z}^2$.

Relevant for applications is the three-dimensional version of the problem. No doubt there will be global and local dependencies in three dimensions as well, and perhaps it is possible to generalise some of the results in this thesis.

Bibliography

[1] K.J. Batenburg, ”Network Flow Algorithms for Discrete Tomography”, Ph.D. thesis, Universiteit Leiden (2006). http://hdl.handle.net/1887/4564

[2] K.J. Batenburg, ”Network Flow Algorithms for Discrete Tomography”, chapter in the book: G.T. Herman and A. Kuba, eds., ”Advances in Discrete Tomography and Its Applications”, Birkhäuser, p. 175-205 (2007).

[3] R.J. Gardner, ”Geometric Tomography”, Cambridge University Press, second edition (2006).

[4] R. Gardner, P. Gritzmann, ”Discrete tomography: determination of finite sets by X-rays”, Trans. Am. Math. Soc. 349, 6, p. 2271-2295 (1997).

[5] L. Hajdu and R. Tijdeman, ”Algebraic aspects of discrete tomography”, J. Reine Angew. Math. 534, p. 119-128 (2001).

[6] L. Hajdu and R. Tijdeman, ”Algebraic Discrete Tomography”, chapter in the book: G.T. Herman and A. Kuba, eds., ”Advances in Discrete Tomography and Its Applications”, Birkhäuser, p. 55-81 (2007).

[7] G.T. Herman, A. Kuba and J.J. Benedetto, ”Discrete Tomography: Foundations, Algorithms and Applications”, Birkhäuser, first edition (1999).

[8] T. Schüle, C. Schnörr, S. Weber and J. Hornegger, ”Discrete tomography by convex-concave regularization and D.C. programming”, Discrete Applied Mathematics, Volume 151, Issue 1-3, p. 229-243 (2005).