Tomography by Projection Counts

Renyu ZHANG

Abstract

In this paper, we study the discrete analogy of Aleksandrov's projection theorem and prove the three sets given by Gardner, Gronchi and Zong in [12] are the only non-congruent finite origin-symmetric convex lattice subsets of $\{(x,y) \in \mathbb{Z}^2 : |y| \leq 2\}$ with equal lattice projection counts, up to unimodular transformations. Some general results without constraint is also obtained in our paper through out which discrete covariogram functions and the unimodular transformation group are intensively applied.

1 Introduction

[1]From 1937 to 1939, A.D. Aleksandrov published a series of papers([1],[2],[3] and [4]) concerning a geometric tomographic problem: whether the projection function $V_k(A|S)$, $k = n-1$ determine $A \in \mathbb{R}^n$ from origin-symmetric convex bodies and he provided an affirmative answer, *Aleksandrov's Projection Theorem*, to this problem, which becomes the starting point of several lines of research in convex geometry, geometric tomography, etc. The theorem is rigorously stated as follows:

Theorem 1.1 (*Aleksandrov's Projection Theorem*, Theorem 3.3.6 in [13]) Assume $i \leq k \leq n-1$, K_1 and K_2 are origin-symmetric convex bodies of dimension at least $k+1$, in $\mathbb{R}^n$. If $V_i(K_1|S) = V_i(K_2|S)$ for all k-dimensional subspace S, then $K_1 = K_2$.

Remark 1.2 Aleksandrov only proved the case $k = n-1$, but revealed all insights and techniques essential for other k's. The proof of this elegant result, either the original one by Aleksandrov or an alternative version given by Fenchel and Jessen independently in [10], relies essentially on area measures, mixed volumes and *Aleksandrov-Fenchel Inequality.* For a complete discussion, see [13] chapter 3 or [17] chapter 5.

In [12], the authors introduced the discrete analogy of projection functions: $|K|S|$, where K is a finite origin-symmetric convex subset of $\mathbb{Z}^n$, and raised the issue of the discrete analogy of Theorem 1.1: whether the lattice projection counts on $(n-1)$-dimensional subspaces can determine K among all finite origin-symmetric convex subsets of $\mathbb{Z}^n$, stated as follows:

Problem 1.3 (Problem 5.3 in [12]) Let $n \geq 2$, $A, B \in \mathcal{O}$, with dim$A$=dim$B$=n and for each $u \in \mathcal{P}^n$, we have:

$$|A|u^\perp| = |B|u^\perp| \tag{1.1}$$

Can $A = B$ be implied?

Unlike the original theorem, however, [12] provided a counterexample in $\mathbb{R}^2$, as illustrated in Figure 1: S_1, S_2 and S_3 are non-congruent, but they have equal lattice projection counts.

[1]Some definitions and notations in this section will be introduced later in the following section.

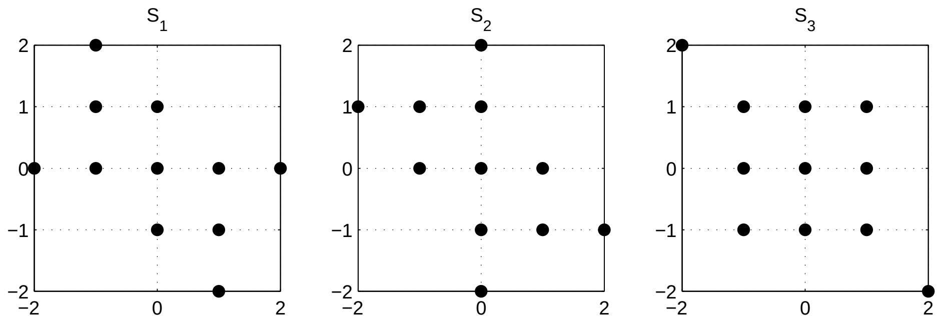

Figure 1: The Counterexample Found in [12]

Remark 1.4 In discrete geometry and computer science, there is a widely studied problem dual to what we discuss in this paper: how to determine and reconstruct a finite convex lattice set from its X-rays $X_uA(v) = |A \cap (L_u + v)|$ where $u, v \in \mathbb{Z}^n$ and L_u is the line through origin parallel to u. Such technique is highly applicable in the study of atoms in crystals and medical imagelogy. Detailed discussions can be found in [11], [14] and the references therein.

The only attempt to the solution of Problem 1.3 was given by Zhou, in [18], and he showed that the counterexample in Figure 1 is the only one in $\mathbb{Z}^2$, up to unimodular transformations and with cardinality not larger than 17. The essence of the proof is to enumerate the form of a finite origin-symmetric convex set with cardinality no larger than 17 and taking unimodular transformations appropriately so as to simplify the structure of the investigated sets.

In 1975, the covariogram function $g_A(u)$ was introduced by Mathereon in [5]. Initially, this function is used to interpret the difference of 2 random variables uniformly distributed on two subsets of $\mathbb{R}^n$: $g_A = \mathbf{1}_A * \mathbf{1}_{-A}$. The *Mathereon's Conjecture* is also stated in [5] as follows: A convex body A is determined by the distribution of $X - Y$, where X and Y are independent random variables uniformly distributed over A. This conjecture is settled, affirmatively in the planar case by Bianchi, but he also gave a series of counterexamples when $\dim(A) \geq 4$, while the $3-$dimensional case is still an open problem, see [6] [7] [8] [9] and [16], for example.

In [12], the authors generalized covariogram function to its discrete analogue: $g_A(u) = |A \cap (A + u)|$ where A is a finite set in $\mathbb{R}^n$, and the connection between Problem 1.3 and discrete covariogram was established (Lemma 2.2), too. In this paper, we are going to make a thorough use of this lemma to show that: S_1, S_2 and S_3 given in Figure 1 is the only finite origin-symmetric convex lattice subsets of $\{(x, y) \in \mathbb{Z}^2 : |y| \leq 2\}$ that cannot be determined by lattice projection counts, up to unimodular transformations. The unimodular transformation group will also be applied frequently in our discussion. The following sections will be organized as follows:

In section 2, we introduce the definitions, notations and preliminaries used in this paper. Some of the basic properties of discrete covariogram and lattice projection counts and several technical lemmas are studied in section 3. Our main result is provided and proved in section 4. Section 5 is devoted to some general results in the planar case without constraint, the last subsection of which contains a few concluding remarks.

2 Definitions, Notations and Preliminaries

As usual, o refers to the origin in Euclidean n-space $\mathbb{R}^n$ and the integer lattice in $\mathbb{R}^n$ is $\mathbb{Z}^n$. For $\mathbb{R}^n \ni u \neq 0$, $u^\perp$ is the $(n-1)$-dimensional subspace orthogonal to u. If $A \subset \mathbb{R}^n$, then $|A|$, $int(A)$ and $conv(A)$ represent the cardinality, the interior and the convex hull of A, respectively. The dimension of A dim$A$ is the dimension of its affine hull. $DA = \{x - y | x, y \in A\}$ is the difference set of A and the *Minkowski Sum* of set A and B refers to $A + B = \{x + y : x \in A, y \in B\}$. In a similar way, we define λA as $\lambda A = \{\lambda x : x \in A\}$ where $\lambda \in \mathbb{R}$ and A is a subset of $\mathbb{R}^n$. In this paper origin-symmetry is always applied to describe a set that is centrally symmetric and its center is o. We say a vector $u \in \mathbb{Z}^n$ is primitive if the greatest common divisor of its n coordinates is 1. And we denote the set of all primitive vectors in $\mathbb{Z}^n$ as $\mathcal{P}^n$. $[x]$ stands for the floor of x, or the greatest integer not bigger than x.

A set $A \subset \mathbb{R}^n$ is a convex set if $\forall x, y \in A$, we have $\lambda x + (1-\lambda) y \in A, \forall \lambda \in [0, 1]$. A convex body C is a compact convex set with non-empty interior, and the sets of all convex bodies is denoted as $\mathcal{K}^n$. $V_k(\cdot)$ is the k-dimensional Lebesgue measure in $\mathbb{R}^n$, where $k = 1, 2, 3, \ldots, n$, while $|A|$ is the cardinality of a finite set A. $A|S$ means the orthogonal projection of A onto a subspace S of $\mathbb{R}^n$. So $V_k(K|S)$ is the kth projection function of a convex body K onto a $k-$hyperplane, $1 \leq k \leq n-1$. $A \subset \mathbb{Z}^n$ is a called a convex lattice set if $A = conv(A) \cap \mathbb{Z}^n$. As a discrete analogy of $V_k(K|S)$, we define $|A|u^\perp|$ as the lattice projection count of a finite lattice set A in $\mathbb{Z}^n$ onto the $(n-1)-$dimensional hyperplane orthogonal to $u \neq 0$. Clearly $|A|u^\perp|$ is the number of lines parallel to u which contain at least one point in A.

For the convenience of our discussion, we apply some unstandard notations which can only be found, strictly, in this paper: $\mathcal{O}^n$ is the collection of finite origin-symmetric convex lattice subsets of $\mathbb{Z}^n$. S is applied to denote the slab $\{(x, y) : |y| \leq 2\}$. We first prove a lemma that characterizes the convexity of a set in $\mathcal{O}^2$.

Lemma 2.1 Let $A \in \mathcal{O}^2$. Suppose $P_1 = (x_1, y_1), P_2 = (x_2, y_2) \in A$, $y_1 > y_2$, $x_1 < x_2$, and o is contained in the left-half plane separated by the line through P_1 and P_2, then for any $y_2 \leq y \leq y_1$, we have $P = (x, y) \in A$ where $x := [x_1 + \frac{(x_2-x_1)(y_1-y)}{y_1-y_2}]$. Further $x \geq x_1 + \frac{(x_2-x_1)(y_1-y)-(y_1-y_2)+1}{y_1-y_2}$.

Proof The first assertion is just a consequence of the definition of convex lattice set while the next assertion follows from the first and that $[x] \leq x \leq [x] + \frac{n-1}{n}$, when $x = \frac{m}{n}$, $gcd(m, n) = 1$. □

There are other criteria for the convexity of a lattice set, but we only need the one presented in Lemma 2.1.

Assume A is a bounded Lebesgue measurable subset of $\mathbb{R}^n$,

$$g_A(u) := V_n((A + u) \cap A) \tag{2.1}$$

is the (usual) covariogram function of A. Analogously, if B is a finite lattice subset of $\mathbb{Z}^n$, the discrete covariogram function g_B is defined as follows:

$$g_B(u) := |(B + u) \cap B| \tag{2.2}$$

We will introduce some basic properties of discrete and usual covariogram functions later in this section.

The fundamental lemma, provided in [12], in our discussion reads as follows:

Lemma 2.2 (Lemma 5.1 of [12]) If A is a finite convex lattice set in $\mathbb{Z}^n$ and $u \in \mathcal{P}^n$, then

$$|A|u^\perp| = |A| - g_A(u) \tag{2.3}$$

Proof (see also [12]) Notice that $|A| = g_A(0u)$, so $|A| - g_A(u) = g_A(0u) - g_A(1u)$. Since $u \in \mathcal{P}^n$ and A is convex, every line parallel to u with at least one point in A contributes exactly 1 to $g_A(0u) - g_A(1u)$. The number of such lines equals $|A|u^\perp|$, so the lemma follows. □

We will frequently use this lemma in our paper. Next, we define the terms *similar* and *exception*:

Definition 2.1 Assume that $A, B \in \mathcal{O}^n$. If $|A|u^\perp| = |B|u^\perp|$, we say A and B are *similar*, and write $A \sim B$ if A and B are similar. (A, B) is an *exception*, if $A \sim B$ but A is not congruent with B.

It's easy to see that *similarity* is an equivalence relation, and, with the help of Lemma 2.2, we have $|A| = |B|$ and $g_A(u) = g_B(u)$ $(\forall u \in \mathcal{P}^n)$ if $A \sim B$.

For a linear transformation $T \in GL(n)$, if $|\det(T)| = 1$ and all of T's entries are integers, T is called unimodular. Obviously, T is nondegenerate and has a unimodular inverse T^{-1}. In our paper G^n denotes the unimodular linear transformation group, i.e. $G^n = \{T \in GL(n) : |\det(T)| = 1, \text{all of } T\text{'s entries are integers}\}$. We are going to show that there are only three orbits of *exception*s contained in S under G^2.

3 The Invariance Properties of Covariogram Functions

As is shown in [18] Theorem 2.1, for $A, B \in \mathcal{O}^n$ if $|A|u^\perp| = |B|u^\perp|$ for any $u \in \mathcal{P}^n$, then $|T(A)|u^\perp| = |T(B)|u^\perp|$ for any $u \in \mathcal{P}^n$ where $T \in G^n$. We restate this property in the language of *similarity*:

Lemma 3.1 Assume $A, B \in \mathcal{O}^n$, $A \sim B$ and $T \in G^n$, then we have $T(A) \sim T(B)$.

Proof The proof is almost the same as the one provided in [18], proving $T(A), T(B) \in \mathcal{O}^n$, u is primitive if and only if $T(u)$ is, and $g_{T(A)}(T(u)) = g_{T(B)}(T(u))$ if and only if $g_A(u) = g_B(u)$. However, the proof of $T(A)$ and $T(B)$'s convexity is not missing in [18], so we fill in the gap here.

Since T is nondegenerate and linear, we have that for $P \in \mathbb{Z}^n$, $P \in bd(conv(A))$ if and only if $T(P) \in bd(T(conv(A)))$. In other words, $T(bd(conv(A)) \cap \mathbb{Z}^n) = T(bd(conv(A))) \cap \mathbb{Z}^n$ $|\det(T)| = 1$, so, for $P \in \mathbb{Z}^n$, if $P \in int(conv(A))$ then we have $T(P) \in int(conv(T(A)))$. The same argument applies to T^{-1} and $T(A)$ and we get $T(int(conv(A)) \cap \mathbb{Z}^n) = T(int(conv(A))) \cap \mathbb{Z}^n$. Consequently, the above two equalities imply that the convexity of $T(A)$ is equivalent to that of A when $T \in G^n$. □

As a direct consequence, we have:

Corollary 3.2 For any $A, B \in \mathcal{O}^2$, $A \sim B$, if and only if $T_k(A) \sim T_k(B)$, where $T_k(x, y) = (x + ky, y)$. □

So we define a subset of G^2 mentioned in Corollary 3.2:

$$\mathcal{T} = \{T_k \in \mathcal{O}^2 : T_k(x, y) = (x + ky, y), k \in \mathbb{Z}\} \tag{3.1}$$

Lemma 3.1 inspires us to look for *exception*s in different equivalent classes according to different orbits under G^2. Now we define this rigorously.

Definition 3.1 We say an *exception* (A, B) is *equivalent* to *exception* (A', B'), if $\exists T \in G^n$ such that $A' = T(A), B' = T(B)$ or $A' = T(B), B' = T(A)$.

For our later use, we restate the main result in [18] as follows:

Theorem 3.3 (Theorem 4.2 in [18]) Assume $A, B \in \mathcal{O}^2$ and (A, B) is an *exception.* If $|A| = |B| \leq 17$, then (A, B) is equivalent to one of the following: (S_1, S_2), (S_2, S_3) and (S_3, S_1), where S_1, S_2 and S_3 are illustrated in Figure 1.

In the next section, we will demonstrate that there are only three *equivalent* classes of *exception*s if the centered convex lattice sets are contained in the slab S.

4 Projection Counts of Sets in $\{(x, y) : |y| \leq 2\}$

4.1 Main Results

As is mentioned in section 1, there are three *exception*s to Problem 1.3, each composed of 2 of the three sets in Figure 1. In this section, however, We will show they are the only *exception*s contained in S. The main result of this paper is established in the following theorem.

Theorem 4.1 Let $A, B \in \mathcal{O}^2$, $A, B \subset S$. If (A, B) is an *exception*, then (A, B) is *equivalent* to one of the following: (S_1, S_2), (S_2, S_3) and (S_3, S_1), where S_1, S_2 and S_3 are illustrated in Figure 1.

Remark 4.2 Theorem 4.1 is generalizable with the help of the following lemma:

Lemma 4.3 If $u = (x_1, x_2, \cdots, x_n) \in \mathcal{P}^n$, then there exists $T \in G^n$ such that $T(u) = (1, 0, 0, \cdots, 0)$.

This is a fundamental and widely applicable result in the theory of integer matrices. The reader may refer to [15], chapter 14 for a proof and extensive discussions. Applying Lemma 4.3, we generalize Theorem 4 into the following result:

Theorem 4.4 Let $A, B \in \mathcal{O}^2$ and (A, B) is an *exception.* If $\inf\{|A|u^\perp| : u \in \mathcal{P}^2\} \leq 5$, we have (A, B) is *equivalent* to one of the following: (S_1, S_2), (S_2, S_3) and (S_3, S_1), where S_1, S_2 and S_3 are illustrated in Figure 1.

We leave the proof, based on some analysis on convexity, of Theorem 4.4 to the end of this section after showing Theorem 4.1.

The key to our proof is that we choose primitive vectors $u's$ appropriately that lead to $g_A(u) \neq g_B(u)$ when $A \neq B$ for $A, B \in \mathcal{O}^2$, thus ruling out other possible *exception*s located in the slab S.

4.2 Analysis on the Structures of Possible *Exception*s

Before entering the details of the proof, we'd like to introduce a few notations first. $A_i = A \cap \{(x, y) : y = i\}$, $B_i = B \cap \{(x, y) : y = i\}$, $l_i^A = \inf\{x : (x, y) \in A_i\}$, $r_i^A = \sup\{x : (x, y) \in A_i\}$, $l_i^B = \inf\{x : (x, y) \in B_i\}$ and $r_i^B = \sup\{x : (x, y) \in B_i\}$. To illustrate, A_i is the intersection of A and $\{(x, y) : y = i\}$, while l_i^A (r_i^A) is the x coordinate of the leftmost (rightmost respectively) point in A_i. By origin-symmetry, we have $A_{-i} = -A_i$, $l_{-i}^A = -r_i^A$ and $r_{-i}^A = -l_i^A$, and analogous equalities hold for B_i, l_i^B and r_i^B. In the rest of the paper, we use the structure of A (or B) to depict the relative location and cardinality of A_i's (B_i's respectively), where $i \in \mathbb{Z}$.[1] We define $n_k^A := l_{-1}^{T_k(A)} - l_2^{T_k(A)}$ and $m_k^A := r_{-1}^{T_k(A)} - r_2^{T_k(A)}$ where $T_k \in \mathcal{T}$ defined in (3.1). n_k^B and m_k^B are defined analogously. The insight of n's and m's will be clear later in our discussion. Now let's get started from ruling out *exception*s in $S' = \{(x, y) : |y| \le 1\}$. A simple consequence of Lemma 3.4 in [18] yields the following lemma.

Lemma 4.5 If $A \sim B$ and $A, B \subset S'$, then A is congruent with B.

Proof **Case I:** set A lies entirely in the x-axis.
This case is trivial.
Case II: set A lies in the 3 lines $y = 0, y = \pm 1$.
Under this condition, the lemma is a direct corollary of Lemma 3.4 in [18]. □

With **Lemma 4.5**, we assume that $A_i \neq \emptyset$ where $i = 0, \pm 1, \pm 2$ in the rest of the paper. Our first step to simplify the structure of possible *exception*s is the following lemma.

Lemma 4.6 If $A \sim B$ and $|A_2| = |A_{-2}| \ge 2$, then $A = B$.

Proof Let $u_k = (2k + 1, 4), k = 0, \pm 1, \pm 2 \cdots\cdots$ The equality $g_A(u_k) = g_B(u_k)$ ($\forall k \in \mathbb{Z}$) yields $B_2 = A_2$ and $B_{-2} = A_{-2}$. If $|A_1| = 1$, by convexity, $|A_2| = 2$, the problem is reduced to the case in Lemma 4.5, if we exchange the role of x and y. If $|A_1| \ge 2$, we let $v_k^1 = (3k + 1, 3)$, $v_k^2 = (3k - 1, 3)$. Similarly, by $g_A(v_k^1) = g_B(v_k^1)$, $g_A(v_k^2) = g_B(v_k^2)$ and $B_2 = A_2$, we derive that $B_1 = A_1$, thus $B_{-1} = A_{-1}$, and $B_0 = A_0$ by the equality of cardinality, i.e. $A = B$. □

So, we obtain the following corollary:

Corollary 4.7 If (A, B) is an *exception*, then $|A_2| = |B_2| = 1$.

Without loss of generality, we assume that $A_2 = \{(\alpha, 2)\}$ $B_2 = \{(\beta, 2)\}$,and let $u_k = (3k+1, 3)$, $v_k = (3k - 1, 3)$, $k = 0, \pm 1, \pm 2 \cdots\cdots$ in the rest of the paper. Deducing from the definition of discrete covariogram, we have that $g_A(u_k) = g_B(u_k) = 2$ or 0, $g_A(v_k) = g_B(v_k) = 2$ or 0. So it does make sense to investigate the position of cardinality of the points in A_{-1} and B_{-1}. In the following discussion, we let $l_{-1}^A = \alpha + t_0$, $r_{-1}^A = \alpha + t_0 + t$ while $l_{-1}^B = \beta + t_1$, $r_{-1}^B = \beta + t_1 + t^*$. Without loss of generality, we assume $t \ge t^*$. From $g_A(u_k) = g_B(u_k)$ and $g_A(v_k) = g_B(v_k)$ ($\forall k \in \mathbb{Z}$), we reach the point that $t - t^* = |A_{-1}| - |B_{-1}| \le 2$, while the difference between t and t^*, if there is any, owes entirely to the 4 boundary points:$(\alpha + t_0, -1)$, $(\alpha + t_0 + t, -1)$, $(\beta + t_1, -1)$ and $(\beta + t_1 + t^*, -1)$. To explicate, we have:

Lemma 4.8 Let t_0, t_1, t and t^* be defined as above. They must satisfy one of the 6 following conditions:

$$t_0 + t = t_1 + t^*, t_0 = 3k, t_1 = 3k + 1 \tag{4.1}$$

$$t_0 = t_1, t_0 + t = 3k, t_1 + t^* = 3k - 1 \tag{4.2}$$

$$t_0 = 3k, t_1 = 3k + 1, t_0 + t = 3k', t_1 + t^* = 3k' - 1 \tag{4.3}$$

$$t_0 = 3k, t_1 = 3k + 1, t_0 + t = 3k' - 1, t_1 + t^* = 3k' \tag{4.4}$$

$$t_0 = 3k + 1, t_1 = 3k, t_0 + t = 3k', t_1 + t^* = 3k' - 1 \tag{4.5}$$

$$t_0 = t_1, t = t^*. \tag{4.6}$$

[1] This is not a rigorous definition, but we state it here for the convenience of our exposition.

Proof We observe, again from the definition of discrete covariogram, that whether $(\alpha + 3l, -1) \in A_{-1}$ does not affect the values of $g_A(u_{l'})$ and $g_A(v_{l''})$ $(l', l'' \in \mathbb{Z})$ when $\alpha + 3l = l^A_{-1}$ or $\alpha + 3l = r^A_{-1}$ (that is $3l = t_0$, or $3l = t_0 + t$, respectively). Analogously, we have similar results for B. Whether $(\beta + 3l, -1) \in B_{-1}$, does not affect the value of $g_B(u_{l'})$ and $g_B(v_{l''})$ $(l', l'' \in \mathbb{Z})$ when $\beta + 3l = l^B_{-1}$ or $\beta + 3l = r^B_{-1}$ (that is $3l = t_1$, or $3l = t_1 + t^*$ respectively). So the only possible difference between the relative location of A_{-1} and A_2 and that of B_{-1} and B_2 only occurs at $(l^A_{-1}, -1)$, $(r^A_{-1}, -1)$, $(l^B_{-1}, -1)$ or $(r^B_{-1}, -1)$. Based on this essential fact and the assumption that $t \geq t^*$, we derive, by enumeration, that the possible *exceptions* must satisfy one of the 6 equations above. □

Lemma 4.8 further simplifies the problem, since we only need to study the structure of $A_2 \cup A_{-1}$ to find the *exceptions* now. We discuss the easiest condition of Lemma 4.8, given by (4.6), first.

Lemma 4.9 When (4.6) holds, $A = B$.

Proof If $|A_1| = |A_{-1}| = |B_1| = |B_{-1}| = 1$, we let $A_1 = \{(\alpha^*, 1)\}$, $A_{-1} = \{(-\alpha^*, -1)\}$, $B_1 = \{(\beta^*, 1)\}$ and $B_{-1} = \{(-\beta^*, -1)\}$. The convexity implies that $\alpha = 2\alpha^*$, $\beta = 2\beta^*$, and $|A_0| = |B_0| = 3$. Let $u = (\alpha^*, 1)$, so $g_B(u) = g_A(u) = 4$, which is equivalent to $\alpha^* = \beta^*$, i.e. $A = B$.

If $|A_1| = |A_{-1}| = |B_1| = |B_{-1}| = t = t^* \geq 2$, we let $\lambda_k = (2k+1, 2), k = 0, \pm 1. \pm 2, \cdots\cdots$ It is clear that $|A_0| = |B_0|$. What remains to be verified is $\alpha = \beta$. If this is not true, we assume, without loss of generality, $\alpha > \beta$. And we let $k^* = \sup\{k : (\alpha, 2) - \lambda_k \in A_0\}$. However, $g_A(\lambda_{k^*}) - g_B(\lambda_{k^*}) \geq 2$ by the definition of k^* and the convexity of A and B. This contradiction concludes the proof. □

4.3 The Structure of $A_2 \cup A_{-1}$

The structure of the *exceptions* under the first 5 conditions are more obscure thus requiring preciser analysis. The set of transformations $\mathcal{T} = \{T_k \in \mathcal{O}^2 : T_k(x, y) = (x + ky, y), k \in \mathbb{Z}\}$ is an efficient tool to analyze the structure of$A_2 \cup A_{-1}$ (or $B_2 \cup B_{-1}$) mainly because it preserves the y coordinate of each point in A and B and it changes n^A_k and m^A_k regularly.

$$n^A_k - n^A_{k-1} = -3, m^A_k - m^A_{k-1} = 3 \tag{4.7}$$

Similar equalities hold for n^B_k and m^B_k too.

Motivated by Theorem 3.3, we first discuss the case when $|A_1|$ is small by the next lemma.

Lemma 4.10 Let $A, B \subset \mathcal{O}^2$, $A, B \subset S$. Suppose $A \sim B$, $|A_2| = 1$ and $|A_1| \leq 4$, then we have $A = B$ if $A, B \notin \{S_1, S_2, S_3\}$, where S_1, S_2 and S_3 are illustrated in Figure 1.

Proof The assertion is a direct consequence of Theorem 3.3. Suppose, further, there exists an *exception* (A, B) which satisfy the assumptions of the lemma. Theorem 3.3 implies $|A| \geq 19$. Hence, $|A_0| \geq 19 - 2|A_1| - 2|A_2| = 9$. However, due to the convexity of A, $|A_0| \leq 2(|A_1| - 1) + 1 = 7$. As a result, there is no *exception* satisfying all the assumptions in the lemma, so $A = B$. □

By Lemma 4.10, we only need to consider the *exception* (A, B) where $|A_1| \geq 5$, and we have:

Theorem 4.11 Let $A, B \in \mathcal{O}^2$, $A, B \subset S$. If $|A_1| = |A_{-1}| \geq 5$, $|A_2| = 1$ and $A \sim B$, then $A = B$.

As we have assumed, $A_{-1} = \{(\alpha + t_0, -1), (\alpha + t_0 + 1, -1) \cdots (\alpha + t_0 + t, -1)\}$ where $t \geq 5$. Without loss of generality, we assume that $t_0 < 0$ and $t + t_0 > 0$. If not, by (4.7) $\exists k^*$ such that $-3 \leq n^A_{k^*} < 0$ and $m^A_{k^*} \geq n^A_{k^*} + 4 > 0$, then we replace A and B with $T_{k^*}(A)$ and $T_{k^*}(A)$. This is a crucial assumption in our later proof and is the reason why we choose the number 5. Prior to looking for an appropriate vector $u \in \mathcal{P}^2$ which violates $g_A(u) = g_B(u)$, we assign some values to α, t_0 and t. Let $\alpha = -a$, $t_0 = -b$ and $t = b + 2a + c$, $b > 0, c \geq 0$. So

$$A_{-1} = \{(-b - a, -1), (-b - a + 1, -1) \cdots\cdots (a + c, -1)\}$$

$$A_1 = \{(-a - c, 1), (-a - c + 1, -1) \cdots\cdots (a + b, 1)\}$$

Further, let

$$A_0 = \{(-d, 0), (-d + 1, 0) \cdots\cdots (d, 0)\}$$

Analogously, let $\beta = -a^*$, $t_1 = -b^*$ and $t^* = b^* + 2a^* + c^*$, so we have:

$$B_2 = \{P_1^* = (-a^*, 2)\}, B^*_{-2} = \{P_2^* = (a^*, -2)\}$$

$$B_{-1} = \{(-b^* - a^*, -1), (-b^* - a^* + 1, -1) \cdots\cdots (a^* + c^*, -1)\}$$

$$B_1 = \{(-a^* - c^*, 1), (-a^* - c^* + 1, 1) \cdots\cdots (a^* + c^*, 1)\}$$

$$B_0 = \{(-d^*, 0), (-d^* + 1, 0) \cdots\cdots (d^*, 0)\}$$

We take $\mathcal{P}^2 \ni u = (a+b+d, 1)$ in the rest of the paper. In fact, u is a vector pointing from the left-most point of A_{-1} to the right-most side of A_0, so $g_A(u) = 4$ if $c \geq a + b + d$, while $g_A(u) = 2$ if $c < a + b + d$. Essentially, $g_A(u) = 4$ or 2 only depends on whether $P_2 + u \in A_{-1}$. We first consider the case that $g_A(u) = 4$, where the structure of A is more explicit.

Lemma 4.12 Let $A, B \in \mathcal{O}^2$, $A, B \subset S$. If $|A_1| = |A_{-1}| \geq 5$, $|A_2| = 1$, $g_A(u) = 4$ and $A \sim B$, we must have $A = B$.

Proof $g_A(u) = 4$, so $g_{A_{-1} \cup A_{-2}}(u) = 1$, i.e. $c \geq a + b + d$. Lemma 2.1 indicates that $2a + b \geq [\frac{d+a}{2}]$, $2a + b \geq [\frac{2a+c}{3}]$, $a + d \geq [\frac{c+4a+b}{2}]$ and $d + a > [\frac{4a+2c}{3}]$. Solve these integer linear inequalities, and we get

$$3a + 2b - 1 \leq d \leq 3a + 2b + 1, a + b + d \leq c \leq 4a + 3b + 2 \tag{4.8}$$

With these inequalities, we can identify every possible value of c and d:

1. $d = 3a + 2b - 1, c = 4a + 3b - 1$

2. $d = 3a + 2b, c = 4a + 3b$ or $4a + 3b + 1$

3. $d = 3a + 2b + 1, c = 4a + 3b + 1$ or $4a + 3b + 2$.

Without loss of generality, we assume that $|A_1| \geq |B_1|$ and (A, B) is an *exception* to derive contradictions. We divide the problem into several parts according to Lemma 4.8.

Case 1 (4.1) holds, i.e. $b^* = b - 1, c^* + 2a^* = c + 2a$

From the identical cardinality of A and B, we get $d^* = d + 1$. Since $g_B(u) = 4$, the inequality $a + 1 \geq a^* \geq a$ must hold.

If $a^* = a$, we consider the convexity of B. We observe that $r^B_1 = a$, but $[\frac{r^B_0 + r^B_2}{2}] = \frac{d+1+a}{2} - a \geq a + 2b > r^B_1$. Such inequality unfortunately violates the convexity of B.

If $a^* = a + 1$, we take vector $u' = (0, 1)$. It is rather obvious that $g_B(u') < g_A(u')$.

Case 2 (4.2) holds, i.e. $b^* = b, c^* + 2a^* = c + 2a - 1$

Then we have $d^* = d$. Taking $u' = (0,1)$, we see $a^* = a+1$ and $c^* = c-1$ by $g_A(u') = g_B(u')$. $g_B(u) = 4$, so $c^* \geq d+a+b$, $c \geq d+a+b+1$. Since $c+2a \equiv 2(\text{mod}3)$, it follows that $c = 4a+3b+2, c^* = 4a+3b+1, d^* = 3a+2b$. Assuming $u' = (2a^*+b^*, -1) = (2a+b+1, -1)$, $g_B(u') - g_A(u') = 2$. This is, again, a contradiction.

Case 3 (4.3) holds, i.e. $b^* = b-1, c^*+2a^* = c+2a-1$

Then $d^* = d+2$, $c+2a \equiv 1(\text{mod}3)$, i.e. $c+2a = 6a+3b+1$. Let $u' = (0,1)$, $g_A(u') = g_B(u')$, so $a^* = a-1$. The convexity of B is also violated at the rightmost point of B_1 because $r_1^B = 2a+b-3 < [\frac{r_0^B+r_2^B}{2}] = [\frac{4a+2b+1}{2}]$.

Case 4 (4.4) holds, i.e. $b^* = b-1, c^*+2a^* = c+2a+1$

Explicitly $d^* = d+1$, $c+2a \equiv 1(\text{mod}3)$, i.e. $c+2a = 6a+3b+1$. Since $g_B(u) = 4$, one of following holds: $a^* = a$ or $a^* = a-1$.

If $a^* = a$, we take $u' = (0,1)$ to deduce $g_A(u') \neq g_B(u')$.

If $a^* = a-1$, the contradiction follows immediately from the violation of B's convexity at the rightmost point of B_1, as is shown in Case 3.

Case 5 (4.5) holds, i.e. $b^* = b+1, c^*+2a^* = c+2a-1$

We have $d^* = d+1$, $c+2a \equiv 1(\text{mod}3)$, i.e. $c+2a = 6a+3b+1$. Taking $u' = (0,1)$, $g_B(u') = g_A(u')$, we find it easy to see $a^* = a-1$, from which $g_B(u)$ follows. The last assertion contradicts our assumption that $g_A(u) = 4$. The conclusion of the lemma is a consequence of the results shown in the cases above. □

The proof of Theorem 4.11 when $g_A(u) = 2$ is a bit tricker, relying on the observation of some other vectors in $\mathcal{P}^2$ violating $A \sim B$.

Lemma 4.13 Let $A, B \in \mathcal{O}^2$, $A, B \subset S$. If $|A_1| = |A_{-1}| \geq 5$, $|A_2| = 1$, $g_A(u) = 2$ and $A \sim B$, we must have $A = B$.

Proof As is assumed in Lemma 4.12, $|A_1| \geq |B_1|$ and (A, B) is an *exception*. To reach some contradictions, we also divide the problem into 5 cases according to Lemma 4.8.

Case 1 (4.1) holds, i.e. $b^* = b-1, c^*+2a^* = c+2a$

Since $|A| = |B|$, it is clear that $d^* = d+1$. $g_A(u) = g_B(u) = 2$, so $a^* = a$.

As before, we let vectors $\lambda_k = (2k+1, 2), k = 0, \pm1, \pm2 \cdots\cdots$. If $|A_{-1}| \geq 6$, there exists more than 3 k's, s.t. $g_{A_{-1}\cup A_1}(\lambda_k) - g_{B_{-1}\cup B_1}(\lambda_k) = 2$. However, there are at most 2 λ_k's which may satisfy $g_{B_{-2}\cup B_0\cup B_2}(\lambda_k) - g_{A_{-2}\cup A_0\cup A_2}(\lambda_k) = 2$. Hence, $\exists k_0 \in \mathbb{Z}$ s.t. $g_A(\lambda_{k_0}) \neq g_B(\lambda_{k_0})$, which contradicts the assumption that $A \sim B$. So $|A_{-1}| \leq 5$, plus $|A_{-1}| \geq 5$, we have $|A_{-1}| = 5$. By Theorem 3.3, we know that $d \geq \frac{19-10-2-1}{2} = 3$, so $d^* \geq d+1 = 4$. Since $t_0 < 0, t+t_0 > 0$, we have $b = 3$, $t+t_0 = 2a+c = 1$. By convexity of A, all possible values of a are 0 and -1. However, each case results in a violation of B's convexity. This contradiction implies $A = B$ in Case 1.

Case 2 (4.2) holds, i.e. $b^* = b, c^*+2a^* = c+2a-1$

Due to $|A| = |B|$ and $g_A(u) = g_B(u)$, we have $d^* = d+1$, $a^* = a-1$. We apply the same method used in Case 1, taking λ_k's to show $\{A : |A_1| \geq 6\}$ is free from *exceptions* and enumerating all possible A's when $|A_1| = 5$. The argument almost the same (To be precise set A in Case 2 is a mirror reflection by the $y-$axis of set A in Case 1.) as the one used in Case 1 leads to a contradiction, thus proving the assertion in Case 2.

Case 3 (4.3) holds, i.e. $b^* = b-1, c^*+2a^* = c+2a-1$

Clearly, with$|A_1| = |A_{-1}|$ and $g_A(u) = g_B(u)$, we obtain $d^* = d+2$ and $a^* = a+1$. By Lemma 4.8, we deduce $b \geq 3$ and $2a+c \geq 3$, so $|A_{-1}| = 2a+c+b+1 \geq 7$. Repeating the argument in the proof of Case 1 and Case 2, we take λ_k's and demonstrate that A is free from *exceptions*, thus concluding our proof of Case 3.

Case 4 (4.4) holds, i.e. $b^* = b-1, c^* + 2a^* = c + 2a + 1$

We have $d^* = d$ because $d = d^*$.

If $a^* \leq a$, we take $k_0 = \sup\{k : g_{B_2 \cup B_0 \cup B_{-2}}(\lambda_k) \neq 0\}$ so it is clear that $g_{A_2 \cup A_0 \cup A_{-2}}(\lambda_{k_0}) \leq g_{B_2 \cup B_0 \cup B_{-2}}(\lambda_{k_0})$. However, $g_{A_1 \cup A_{-1}}(\lambda_{k_0}) < g_{B_1 \cup B_{-1}}(\lambda_{k_0})$, by $r_1^A - l_{-1}^A \leq l_1^B - r_{-1}^B - 2$, which is yielded from (4.4).

If $a^* \geq a+2$, $g_B(u) \geq 4$, contradictory to our assumption that $g_A(u) = 2$.

If $a^* = a+1$, let $u' = (2a^* + b^*, -1)$. We have that $g_B(u') = g_A(u') + 2$, contradiction again.

Case 5 (4.5) holds, i.e. $b^* = b+1, c^* + 2a^* = c + 2a - 1$

Similar to the Case 4, $d^* = d$. Essentially, it is a inverse case of the last one. In other words, if we exchange the role of A and B, the argument utilized in Case 4 is still valid in this case, which results in another contradiction.

Combining the last five cases together, we safely conclude that there is no *exception* as long as $g_A(u) = 2$. □

Proof of Theorem 4.1 Lemma 4.12 and Lemma 4.13 immediately leads to Theorem 4.11. Summarizing the results given by Lemma 4.5, 4.8, 4.9, 4.10, Corollary 4.7 and Theorem 4.11, we have proved Theorem 4.1. □

4.4 On Theorem 4.4

We will generalize Theorem 4.1 to Theorem 4.4 in this subsection. Suppose $A, B \in \mathcal{O}^2$ with $A \sim B$ and $u_* \in \mathcal{P}^2$ such that $|A|u_*^{\perp}| = \inf\{|A|u^{\perp}| : u \in \mathcal{P}^2\} \leq 5$. We also assume that (A, B) is not equivalent to (S_1, S_2), (S_2, S_3) or (S_3, S_1). We apply Lemma 4.3 to A and B, so we have: $\exists T \in G^2$, such that $|T(A)|T(u_*)^{\perp}| = |T(B)|T(u_*)^{\perp}| \leq 5$ and $T(u_*) = (1, 0)$. So we replace A and B with $T(A)$ and $T(B)$. In fact, we can prove, by the next lemma, that $A, B \subset S$, thus reducing Theorem 4.4 to Theorem 4.1.

Lemma 4.14 Let $A, B \in \mathcal{O}^2$ and $A \sim B$. Suppose again that $|A|u_*^{\perp}| \leq 5$ and (A, B) is not *equivalent* to (S_1, S_2), (S_2, S_3) or (S_3, S_1). We have $A, B \subset S$, where $u_* = (1, 0)$ and $|A|u_*^{\perp}|$ is the smallest among all the $u \in \mathcal{P}^2$.

Proof By Theorem 3.3, $|A| \geq 19$. Assume that $A \cap S \neq A$, then $A_1 = \emptyset$ or $A_2 = \emptyset$.

Case 1 $A_1 = \emptyset$

First we observe that $|A_i| \leq 1$ for all $i \geq 1$. Otherwise, by the convexity of A, we have $|A_j| \geq 1$ when $j \leq k = \sup\{i : |A_i| = 2\}$, contradictory to $|A_1| = 0$. If $|A_0| \geq 3$, by convexity again, we have $|A_1| \geq [\frac{2}{3} \cdot 2] = 1$, contradicting the assumption that $A_1 = \emptyset$. Hence, $|A_0| = 1$. That is to say $|A_i| \leq 1, \forall i \in \mathbb{Z}$, so $|A| \leq 5$. We have established a contradiction in Case 1.

Case 2 $A_2 = \emptyset$

$|A| \geq 19$, so $2|A_1| + |A_0| + 2 \geq 19$ and, by convexity of A, $|A_0| \geq |A_1| - 1$. This two inequalities imply $|A_0| \geq 4$. Since $|A_0|$ is odd, we have $|A_0| \geq 5$. Hence $|A_2| \geq [\frac{1}{3}(|A_0| - 1)] \geq [\frac{4}{3}] = 1$, contradictory to that $A_2 = \emptyset$.

Concluding the above two cases, we find that $A \subset S$. Identical argument holds for B too, so we also have $B \subset S$. □

As a corollary, it follows that:

Corollary 4.15 Suppose $A, B \in \mathcal{O}^2$ with $A \sim B$, and $\exists u_* \in \mathcal{P}^2$ such that $|A|u_*^{\perp}| = \inf\{|A|u^{\perp}| : u \in \mathcal{P}^2\} \leq 5$. There exists $T \in G^2$ such that $T(u_*) = (1, 0)$, and $T(A), T(B) \subset S$.

Proof If (A,B) is *equivalent* to $(S_i,S_j), 1\le i,j\le 3$, where S_1,S_2 and S_3 are illustrated in Figure 1, the assertion follows immediately by definition. If (A,B) is not *equivalent* to $(S_i,S_j), 1\le i,j\le 3$, the conclusion follows from Lemma 4.14. □

Proof of Theorem 4.4 Once we have established Corollary 4.15 and Theorem 4.1, the conclusion of Theorem 4.4 follows immediately.

5 Projection of Sets without Constraint

In this section, we relax the constraint of $|y|\le 2$ and try to develop some general results about Problem 1.3. We start from the case with a clear structure: rectangles. We say $A\in\mathcal{O}^2$ is a *rectangle* if $A=\{(x,y)\in\mathbb{Z}^2: -m\le x\le m, -n\le y\le n\}$ and we denote A as $R_{m,n}$. (We only consider when $m\ge 3, n\ge 3$ due to Theorem 4.1.) Our next result shows that *rectangles* can be determined by lattice projection counts.

Proposition 5.1 Suppose $R_{m,n}$ and $A\in\mathcal{O}^2$, and they satisfy that $R_{m,n}\sim A$, then $A=R_{m,n}$.

Proof Clearly, by Lemma 2.2, we have $g_A(u)=g_{R_{m,n}}(u),\forall u\in\mathcal{P}^2$ and $|A|=(2m+1)(2n+1)$. If $\exists j>n$, such that $|A_j|\ne 0$, there must exist, by $|A|\{(x,y):x=0\}=2n+1|, 0<k\le n$ such that $|A_k|=0$. Following the argument in the proof of Lemma 4.14, by convexity, $|A_l|\le 1,\forall k\le |l|\le j$. Suppose $|\{l: |A_l|=0, k\le |l|\le n\}|=2\alpha$, then $N:=|\{(x,y):(x,y)\in R_{m,n},(x,y)\notin A\}|\ge 2\alpha(2m+1)$. However, $|A\cap\{(x,y):|y|>n\}|\le 2\alpha$. Let $k_0:=\inf\{k>0:|A_k|=0\}$, then $k_0\ge 1$ and it is the least k that makes $\{(x,y):y=k\}$ free of points in A. So

$$\sum_{i=-k_0+1}^{k_0-1}|A_i|\ge N-2\alpha+(2m+1)(2k_0-1)>(2m+1)(2k_0-1)$$

Hence, by *Dirichlet's Pigeonhole Principle*, $\exists q, -k_0+1\le q\le k_0-1$, such that $|A_q|\ge 2m+2$. That is to say, $|A|\{(x,y):y=0\}|\ge 2m+2$, contradicting the assumption that $|A|\{(x,y):y=0\}|=|R_{m,n}|\{(x,y):y=0\}|=2m+1$, thus concluding the proof. □

By Lemma 2.2, 3.1 and the last proposition, we know that any $A=T(R_{m,n})$, when $T\in G^2$, is also determined by its projection.

The following result illustrates that, applying suitable transformation in G^2, we can reshape the original set in $\mathcal{O}^2$ into one with a simple structure defined below. Further, for convenience again, we let $A'_i:=A\cap\{(x,y):x=i\}$.

Definition 5.1 Suppose $A\in\mathcal{O}^2$, we say A is *compressed*, if $\exists a,b\ge 0$ such that $A\subset R_{a,b}$, $|A_i|>0$ and $|A'_j|>0$, $\forall -b\le i\le b, -a\le j\le a$. C is called the *maximal compressed subset* of A, if $\exists a_0,b_0\ge 0$ such that $|C_i|>0$ and $|C'_j|>0$, $\forall -b_0\le i\le b_0, -a_0\le j\le a_0$, but $|C_{b_0+1}|=0$ and $|C'_{a_0+1}|=0$. The *maximal compressed subset* of A is denoted as $MC(A)$.

Essentially, for a *compressed* set A, we have a *rectangle* $R_{a,b}$ such that $A\subset R_{a,b}$ and each of the lines: $\{(x,y):y=i\}$ or $\{(x,y):x=j\}$, where $|i|\le b$ and $|j|\le a$ has at least one point in A.

Lemma 5.2 Let $A\in\mathcal{O}$, $C=M(A)$ and $C\subsetneq A$, then $\exists T^*\in G^2$ such that $|MC(T^*(A))|\ge |C|+2$.

Proof Since $o\in A$, $MC(A)\ne\emptyset$. We first claim that there are exactly 2 points in A which have the smallest *Hausdorff Metric* or *Manhattan Distance* from R_{a_0,b_0}.

To start with, the points in A but not in C must lie in $R_1 = \{(x,y) \in \mathbb{Z}^2 : x > a_0, y > b_0\}$, $R_2 = \{(x,y) \in \mathbb{Z}^2 : x > a_0, y < -b_0\}$, $R_3 = \{(x,y) \in \mathbb{Z}^2 : x < -a_0, y > b_0\}$ or $R_4 = \{(x,y) \in \mathbb{Z}^2 : x < -a_0, y < -b_0\}$. $|A_i| \leq 1$ for $|i| \geq b_0 + 1$, $|A'_j| \leq 1$ for $|j| \geq a_0 + 1$. Similar argument, based on convexity, with that of Lemma 4.14 shows that every point in A but not in C must be contained in either $R_1 \cup R_4$ or $R_2 \cup R_3$. Without loss of generality, we assume that $A \backslash C \subset R_3 \cup R_2$. If there are two points $P_1 = (x_1, y_1), P_2 = (x_2, y_2) \in R_3$ where $x_1 < x_2$ and $y_1 > y_2$ with the same smallest distance to R_{a_0,b_0}. The convexity of A soon yields that $(x_1, y_2) \in A$ and it is nearer than P_1 and P_2. So there is only one point of the smallest distance to R_{a_0,b_0} in $A \cap R_3$, so is one in $A \cap R_2$. The claim follows.

We assume P is the point nearest to R_{a_0,b_0} and $P \in R_3$. Clearly, by the convexity of A, $\hat{P} = (-a_0, b_0) \in A$, since $A_{b_0} \neq \emptyset$ and $A'_{-a_0} \neq \emptyset$. Suppose $P - \hat{P} = (-p, q)$, where $(p, q) = 1$. As before, we assume $\mathcal{T} = \{T_k : T_k(x,y) = (x + ky, y), k \in \mathbb{Z}\}$ and $\bar{\mathcal{T}} = \{\bar{T}_k : \bar{T}_k(x,y) = (x, y + kx), k \in \mathbb{Z}\}$.

We now construct a suitable T^* satisfying the requirement of the lemma. For convenience, let $A^0 = A, C^0 = C, P^0 = P, \hat{P}^0 = \hat{P}$. Without loss of generality, we simply assume that $q > p$ then by elementary number theory, we have $\exists k_1 \in \mathbb{Z}$ such that $y_{\bar{T}_{k_1}(P)} - y_{\bar{T}_{k_1}(\hat{P})} = q - k_1 p = p_1 < p$ and $p_1 > 0$.

We observe that $T^1(C^0)$ is still a *compressed* subset of $T^1(A^0)$. If not, $\exists P^* \in T^1(C^0)$ such that its y coordinate is larger than that of $T^1(\bar{P}^0)$. Hence, together with the convexity of $T^1(A)$ and the fact $p_1 > 0$, $T^1(\bar{P}^0) + (0,1) \in T^1(C^0)$. Therefore, $\bar{P}^0 + (0,1) \in C^0$, contradicting the maximality of C^0.

Now we replace A, A^0, P, $\hat{P}$, p and q in the above argument with $A^1 = T^1(A^0)$, $C^1 = T^1(C^0)$, $P^1 = T^1(P^0)$, $\hat{P}^1 = T^1(\hat{P})$, p_1 and $q_1 = p$ respectively. We have $P^1 - \hat{P}^1 = (-q_1, p_1)$. This time we take $T^2 = T_{k_2} \in \mathcal{T}$, such that $x_{T_{k_2}(P)} - x_{T_{k_2}(\hat{P})} = -q_1 + k_2 p_1 = -p_2 > -q_1$ and the maximality of $T^2(C_0)$ as a *compressed* subset is still satisfied. As is shown in the argument above, the essence of the induction process is the same as that of *Euclidean's Algorithm* to find the greatest common divisor. Hence, we have a finite sequence of transformations $T^1, T^2, \cdots\cdots T^n \in G^2$ the composite composite $T^* = T^n \cdot T^{n-1} \cdots T^1$ of which satisfies $T^*(P) = T^*(\hat{P}) + (-1, 1)$ and $T^*(C)$ is still a *compressed* subset of $T^*(A)$, so $T^*(C) \cup \{T^*(P)\} \cup \{T^*(-P)\} \subset MC(T^*(A))$. This inclusion concludes the proof. □

We are motivated by Lemma 5.2 to induce on the cardinality of $MC(T^*_n(A))$, where $T^*_n \in G^2$.

Proposition 5.3 Suppose $A \in \mathcal{O}$, $\exists T \in G^2$ such that $T(A)$ is *compressed*.

Proof If A is *compressed*, there is nothing to prove and we just let $T = Id$. If $MC(A) \subsetneqq A$, by Lemma 5.2, $\exists T^*_1, T^*_2, T^*_3 \cdots \in G^2$, such that $|CM(T^*_k(A))| \geq |CM(A)| + 2k$. Hence, $\exists n$ such that $|CM(T^*_n(A))| = |A|$, which is equivalent to $CM(T^*_n(A)) = T^*_n(A)$. It suffices to let $T = T^*_n$. □

5.1 Concluding Remarks

We have answered Problem 1.3 partly in this paper, under a strong condition. The proof relies so heavily on the explicit and simple structure of the sets that it is not well generalizable. Further, though with Lemma 2.2, we still know little about the discrete covariogram function. We can hardly retrieve the original set from the discrete covariogram function. The only thing we know is that without the assumption of convexity and origin-symmetry, the discrete covariogram function even fails to ensure the uniqueness of the original set, see [12] for counterexamples of either case (loss of convexity and loss of origin-symmetry).

Applying Fourier transformation to the covariogram function, in [12], the authors show that discrete covariogram function can determine sets in $\mathcal{O}^n$:

Proposition 5.4 (Corollary 4.5 in [12]) If $A, B \in \mathcal{O}^n$ and $g_A = g_B$, it follows that $A = B$.

With Lemma 2.2, Problem 1.3 can be restated as follows: if $A, B \in \mathcal{O}^n$ and $g_A(u) = g_B(u) \forall u \in \mathcal{P}^n$ can $A = B$ be implied? By Proposition 5.4, for any *exception* (A, B), $\exists v \in \mathcal{P}^n$ and $k \geq 2$ such that $g_A(kv) \neq g_B(kv)$.

Acknowledgement

Thanks very much for the generous sponsorship of National Innovation Project, as well as my advisor, Professor Chuanming Zong's helpful suggestions and discussions. All these help me significantly finish this paper.

References

[1] A. D. Aleksandrov, On the theory of mixed volumes of convex bodies. I. Extensions of certain concepts in the theory of convex bodies [in Russian]. *Mat. Sb.* **2** (1937), 947-972.

[2] A. D. Aleksandrov, On the theory of mixed volumes of convex bodies. II. New inequalities between mixed volumes and their applications [in Russian]. *Mat. Sb.* **2** (1937), 1205-1238.

[3] A. D. Aleksandrov, On the theory of mixed volumes of convex bodies. III. Extensions of two theorems of Minkowski on convex polyhedra to arbitrary convex bodies [in Russian], *Mat. Sb.* **3** (1938), 27-46.

[4] A. D. Aleksandrov, On the surface area function of a convex body [in Russian]. *Mat. Sb.* **6** (1939), 167-174.

[5] G. Matheron, *Random Sets and Integral Geometry*, John Wiley Sons, New York-London-Sydney, 1975.

[6] G. Averkov and G.Bianchi, Confirmation of Matheron's conjecture on the covariogram of a planar convex Body, *J. Eur. Math. Soc. (JEMS)* **11**(2009), 1187-1202.

[7] G. Bianchi, Determining convex polygons from their covariograms, *Adv. in Appl. Probab* **34** (2002), 261-266.

[8] G. Bianchi, Matheron's conjecture for the covariogram problem, *J. Lond. Math. Soc.* **71** (2005), 203-229.

[9] G. Bianchi, The covariogram determines three-dimensional convex polytopes, *Adv. Math.* **220** (2009), 1771-1808.

[10] W. Fenchel and B.Jessen, Mengenfunktionen und konvexe Korper, *Mat.-Fys. Medd. Dansake Vid. Selsk.* **16** (1938), 1-31.

[11] R. J. Gardner and P. Gritzmann, Discrete tomography: Determination of finite sets by X-rays, *Trans. Amer. Math. Soc.* **349** (1997), 22712295.

[12] R. J. Gardner, P.Gronchi and C.M.Zong. Sums, projections, and sections of lattice sets, and the discrete covariogram, *Discrete Comput. Geom.* **34** (2005),391-409.

[13] R. J. Gardner, *Geometric Tomography*, Cambridge University Press, New York, 2006.

[14] G. T. Herman and A. Kuba, *Discrete Tomography: Foundations, Algorithms, and Applications*, Birkhauser, Boston, MA, 1999.

[15] L. K. Hua translated from the Chinese by Peter Shiu, *Introduction to Number Theory*, Springer-Verlag, Berlin Heidelberg and New York, 1982.

[16] W. Nagel, Orientation-dependent chord length distribution characterize convex polygons, *J. Appl. Probab.* **30** (1993), 730-760.

[17] R. Scheneider, *Convex bodies, the Brunn-Minkowski theory*, Cambridge University Press, Cambridge, 1993.

[18] J. Zhou, On the Projections of Convex Lattice Sets, *Acta Math Sin., English Series* (2010), published online.