Hardy-Ramanujan Journal 41 (2018), 98-103 submitted 19/10/2018, accepted 05/11/2018, revised 06/11/2018

Two applications of number theory to discrete tomography

Rob Tijdeman

To the memory of S. Srinivasan

Abstract. Tomography is the theory behind scans, e.g. MRI-scans. Most common is continuous tomography where an object is reconstructed from numerous projections. In some cases this is not applicable, because the object changes too quickly or is damaged by making hundreds of projections (by X-rays). In such cases discrete tomography may apply where only few projections are made. The present paper shows how number theory helps to provide insight in the application and structure of discrete tomography.

Keywords. Discrete tomography, sums of two squares, switching components

2010 Mathematics Subject Classification. 94A08, 15A06.

1. Introduction

Tomography deals with the inverse problem of reconstructing an object from the knowledge of its projections in a number of given directions. Mathematically the object is represented by a function and a projection is the set of line integrals for all lines in a given direction. Tomography has a wide range of applications, from medicine to industrial environments. Usually the number of used projections is several hundreds and continous tomography applies and there is a unique solution which can be found by Fourier analysis, the so-called filter-back method. See e.g. [Nat01].

Sometimes it is necessary to limit the number of used directions, e.g. since the object would be damaged by using many X-rays or the object changes too rapidly. If the reconstruction is based on only few projections, discrete tomography applies. The model for discrete tomography we consider is an unknown real function on a finite lattice where the line sums in a small number of lattice directions are given and the challenge is to reconstruct the original function.

A criterion for the uniqueness of the solution was given by M. Katz, [Kat77]. If his criterion is satisfied, there is a fast method to find the solution, see e.g. [PaTi]. In general there will be many solutions and the question arises which structure the set of solutions has. Here the Chinese Remainder Theorem for polynomials provides insight. Since the solutions turn out to be well-spread, it may be possible to decide which solution is the most likely to represent the original object by using additional knowledge on the object, see e.g. [DaHaTi13]. For general information on discrete tomography we refer to [HerKu99, HerKu07].

It turns out that discrete tomography can be used for coding theory, data storage, cryptography, etc. by choosing the directions such that the solution is unique. See e.g. [GN95]. A theorem on the sums of two squares of integers indicates how to choose the directions of the projections such that already a small number of directions suffices to be able to reconstruct the original object.

We thank episciences.org for providing open access hosting of the electronic journal *Hardy-Ramanujan Journal*

This paper is based on papers which contain much more material. The application of the Chinese Remainder Theorem appeared for the first time in [HaTi01] and was elaborated in [HaTi07]. The application of the sum of two squares theorem appeared in [PaTi]. The purpose of the present paper is to highlight the applicability of classical number theory theorems to discrete tomography.

2. The mathematical model

We assume that the object is located in an m by n *rectangle* $A = \{\mathbf{a} = (a, b) \in \mathbb{Z}^2 : 1 \le a \le m, 1 \le b \le n\}$ of pixels and that the object is characterized by a function $f : A \to \mathbb{R}$ where we assume $f(\mathbf{a}) = 0$ for those $\mathbf{a} \in A$ which are not in the domain of the object. A *direction* is a nonzero vector $\mathbf{d} = (d, e) \in \mathbb{Z}^2$ with $\gcd(d, e) = 1, d \ge 0$ and $e = 1$ if $d = 0$. We denote the *line sum* of the line through $\mathbf{a} = (a, b) \in A$ in the direction $\mathbf{d} = (d, e)$ for any $h \in \mathbb{Z}$ by

$$\ell(\mathbf{d}, h) = \sum_{(a,b)\in A,\ ea-db=h} f(a, b). \tag{2.1}$$

Let $k > 1$. Let $D = \{\mathbf{d}_i = (d_i, e_i) : i = 1, \dots, k)\}$ be a set of directions. We assume throughout the paper that the line sums $\ell(\mathbf{d}_i, h)$ are given for $i = 1, \dots, k$ and all $h \in \mathbb{Z}$. Note that the sum of all the line sums in one direction equals the sum of all the line sums in any other direction so that the line sums are not independent of each other.

If $f, g : A \to \mathbb{R}$ have the same line sums in the directions of D, then the line sums of $f - g$ in the directions of D are obviously 0. On the other hand, the line sums of f do not change if you add a function g for which all the line sums in the directions of D vanish. Thus for finding all the functions f which yield given line sums in the directions of D, it suffices to find one solution f and the set of functions for which all the line sums in the directions of D vanish. Such functions are called *switching components*.

3. Application of the Chinese Remainder Theorem

In this section we show that making a projection can be considered as computing the remainder of a division of a polynomial by a polynomial.

For a commutative ring Z we write $Z[x, y]$ for the set of polynomials $\sum_{i,j} c_{i,j} x^i y^j$ with $c_{i,j} \in Z$ for all i, j. The theorem we apply reads as follows.

Theorem 3.1. *Let $P_1(x, y), \dots, P_r(x, y) \in \mathbb{Z}[x, y]$ with P_j relatively prime to P_i for all $j \ne i$. For given $Q_1(x, y), \dots, Q_r(x, y) \in \mathbb{Z}[x, y]$ there is a unique polynomial $R_0(x, y) \in \mathbb{Z}[x, y]$ of degree less than $\sum_{i=1}^r deg(P_i)$ such that all solutions of*

$$R(x, y) \equiv Q_j(x, y) \pmod{P_j(x, y)} \quad \text{for } 1 \le j \le r \tag{3.2}$$

are given by

$$R(x, y) \equiv R_0(x, y) \left(\mathrm{mod} \prod_{j=1}^{r} P_j(x, y) \right).$$

Proof. See [Lan81] p. 63 or Exercise 3 on page 437 of [Knu81].

In the above notation let A and D be given. For $f : A \to \mathbb{R}$ let $F(x,y) = \sum_{(a,b)\in A} f(a,b)x^a y^b$. For direction (d_i, e_i) write

$$P_i(x,y) = \begin{cases} x^{d_i}y^{e_i} - 1 & \text{if } d_i > 0,\ e_i > 0, \\ x^{d_i} - y^{-e_i} & \text{if } d_i > 0,\ e_i < 0, \\ x - 1 & \text{if } d_i = 1,\ e_i = 0, \\ y - 1 & \text{if } d_i = 0,\ e_i = 1. \end{cases}$$

Put $P_D(x,y) = \prod_{i=1}^k P_i(x,y)$. The following application of Theorem 3.1 characterizes the functions $f : A \to \mathbb{R}$ which have given line sums in the directions of D. It is a simplified reformulation of Theorem 1 of Hajdu and Tijdeman [HaTi01].

Theorem 3.2. *Let $A = \{(a,b) \in \mathbb{Z}^2 : 1 \le a \le m, 1 \le b \le n\}$ and D a set of directions. If the function $g : A \to \mathbb{R}$ has the same line sums in the directions of D as $f : A \to \mathbb{R}$, then the corresponding polynomials G and F satisfy the congruence*

$$G(x,y) \equiv F(x,y) \pmod{P_D(x,y)}.$$

Note that the polynomial P_D has degree $M := \sum_{i=1}^k d_i$ in x and $N := \sum_{i=1}^k |e_i|$ in y. Therefore f is uniquely determined by its line sums if $m \le M$ or $n \le N$, as was proved by M. Katz [Kat77] in 1977. If this is the case, it is said that *the Katz condition holds* or that (A, D) is *invalid*. If, on the contrary, (A, D) is *valid*, then the polynomials corresponding to the functions $f : A \to \mathbb{R}$ with only zero line sums in the directions of D are exactly the polynomial multiples of P_D.

Sketch of the proof of Theorem 3.2. The polynomial $F(1,y) =: \sum_{j=1}^n r_j y^j$ has coefficients $r_j = \sum_{i=1}^m f(i,j)$ for $j = 1, \dots, n$. Therefore, if $(1,0) \in D$, then $F(x,y) - G(x,y)$ is divisible by $x - 1$. Similarly, if $(0,1) \in D$, then $F(x,y) - G(x,y)$ is divisible by $y - 1$. If $de \neq 0$ and

$$\sum_{(a,b)\in A,\ ea-db=h} f(a,b) = \sum_{(a,b)\in A,\ ea-db=h} g(a,b)$$

for all $h \in \mathbb{Z}$, then

$$F(x^e, x^{-d}) = \sum_{(a,b)\in A} f(a,b)x^{ea-db} = \sum_{h\in\mathbb{Z}} \left(\sum_{(a,b)\in A,\ ea-db=h} f(a,b) \right) x^h$$

$$= \sum_{h\in\mathbb{Z}} \left(\sum_{(a,b)\in A,\ ea-db=h} g(a,b) \right) x^h = G(x^e, x^{-d}).$$

It follows that $F(x,y) - G(x,y)$ is divisible by $x^d y^e - 1$ if $d > 0, e > 0$ and by $x^d - y^{-e}$ if $d > 0, e < 0$. Hence, by Theorem 3.1 with $R_0(x) \equiv F(x,y)$ and pairwise coprimality of $P_1, \dots, P_k$, we obtain that $G(x,y) - F(x,y)$ is divisible by $P_D(x,y)$.

Remark 3.1. Theorem 3.2 has various generalizations. The original formulation was for polynomials in $Z[x,y]$ where $Z[x,y]$ is a unique factorization domain. Stolk and Batenburg [StoBat10] extended the theory to finite, convex sets A in place of rectangles A and to commutative rings Z in place of unique factorization domains Z. See also [HaTi13]. Generalizations to higher dimensions can be found in [Sto11, HaTi07].

4. Good choices for the directions

In this section we show that the width of the beam used to compute a line sum in practice induces a bound for the directions which can be considered.

Let again $A = \{(a,b) \in \mathbb{Z}^2 : 0 < a \le m,\ 0 < b \le n\}$ for given (m,n). The larger the entries of a direction are, the more information the line sums provide. However, there is a natural boundary for the selectable directions. The beam measuring the line sum has a certain width and directions should be chosen in such a way that a beam meets only the pixels on the line and no others. This induces an upper bound for the length of a usable direction (d,e). If the width of the beam is w times the distance between neighbouring pixels, then $\sqrt{d^2+e^2}$ should be less than $1/w$ so that no pixels outside the considered line are in the beam. See Figure 1.

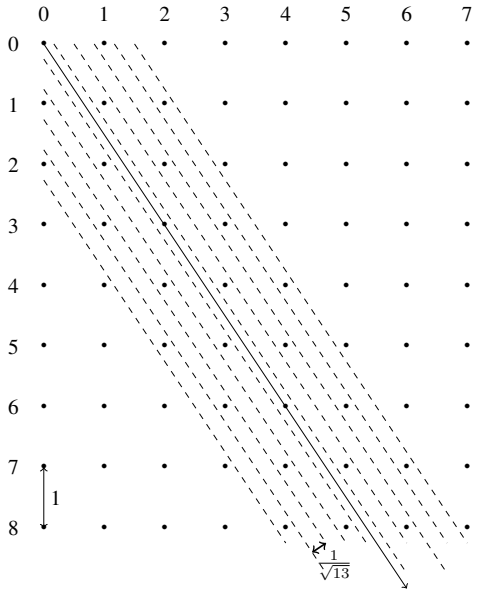

Figure 1: Maximal beams of lines in the direction (2,3). The distance between consecutive lines is $1/\sqrt{2^2+3^2} = 1/\sqrt{13}$.

For an optimal choice of the primitive directions, we have to determine the primitive directions (d,e) with $d^2+e^2 < C$ for some $C \le 1/w$. In order to determine these directions we use the following numbertheoretical result.

Theorem 4.1. *If d and e are positive integers with $\gcd(d,e) = 1$ and $d^2+e^2 = N = 2^m p_1^{m_1} \cdots p_r^{m_r}$ where $p_1, \ldots, p_r$ are odd distinct primes, then $m \le 1$ and $p_1, \ldots, p_r$ are all $\equiv 1 \pmod 4$. On the other hand, if N is of this form, then the number of ways N can be written as d^2+e^2 with $(d,e) = 1, d > 0, e > 0$ equals 2^r.*

Proof. See Theorem 7.5 of [Lev56].

Observe that among 24 consecutive positive integers at most 6 can be written as sum of two coprime squares, viz. the numbers $\equiv$ 1,2,5,10,13,17 (mod 24). All others are divisible by 4 or by a prime $\equiv 3 \pmod 4$.

Let $(d_1,e_1), \ldots, (d_k,e_k)$ be the primitive directions with largest lengths $< C$ and $d_j > e_j$ for $j = 1, \ldots, k$ and $d_1 \ge d_2 \ge \cdots \ge d_k$, $e_1 \le e_2 \le \cdots \le e_k$ such that $\sum_{j=1}^{k}(d_j+e_j) > C/2$. We call

such a set of directions *doubly monotonic*. We suggest to take as directions

$$\begin{aligned} D &= \{(d_1,-e_1),(d_2,-e_2),\ldots,(d_k,-e_k),(e_k,-d_k),\ldots,(e_1,-d_1),\\ &\quad (d_1,e_1),(d_2,e_2),\ldots,(d_k,e_k),(e_k,d_k),\ldots,(e_1,d_1)\}. \end{aligned}$$

Subsequently some directions may be removed provided that after removal D is still invalid for A.

Example 4.1. Suppose A is a 70×60 square and $C = 50$. Then following Theorem 4.1 and the remark thereafter we find $k = 2$, $50 = 7^2 + 1^2, 41 = 5^2 + 4^2, 37 = 6^2 + 1^2, 34 = 5^2 + 3^2$. Therefore we choose, omitting $(7, \pm 1)$ and $(6, \pm 1)$,

$$\begin{aligned} D &= \{(5,-3),(5,-4),(4,-5),(3,-5),(1,-6),(1,-7),\\ &\quad (5,3),(5,4),(4,5),(3,5),(1,6),(1,7)\}. \end{aligned}$$

We have $\sum_{h=1}^{12} e_h = 60 = n$, hence we have an invalid case.

Example 4.2. Suppose A is a 90×90 square and $C = 90$. Then Theorem 4.1 yields $89 = 8^2 + 5^2, 85 = 9^2 + 2^2 = 7^2 + 6^2, 82 = 9^2 + 1^2$. Here we choose, omitting $(9, \pm 1)$ and $(9, 2)$,

$$\begin{aligned} D &= \{(9,-2),(8,-5),(7,-6),(6,-7),(5,-8),(2,-9),(1,-9),\\ &\quad (8,5),(7,6),(6,7),(5,8),(2,9),(1,9),\}. \end{aligned}$$

We have $\sum_{h=1}^{13} e_h = 90 = n$, hence we have an invalid case.

Remark 4.1. We claim that if the directions (d_i, e_i) all satisfy

$$C \geq d_i^2 + e_i^2 \geq C - 2\sqrt{C} + 1,$$

then the directions (d_j, e_j) can be ordered such that they are doubly monotonic. Otherwise, there would be $(d_i, e_i), (d_j, e_j)$ such that $d_i > d_j$ and $e_i > e_j$. This would imply

$$\begin{aligned} d_j^2 + e_j^2 &\leq (d_i - 1)^2 + (e_i - 1)^2 = (\sqrt{d_i^2 + e_i^2} - 1)^2 + 2\sqrt{d_i^2 + e_i^2} - 2d_i - 2e_i + 1\\ &\leq (\sqrt{d_i^2 + e_i^2} - 1)^2 < (\sqrt{C} - 1)^2 = C - 2\sqrt{C} + 1. \end{aligned}$$

Observe that in Example 4.2 the sums of squares are all between 90 and $90 - 2\sqrt{90} + 1 < 73$ and therefore result in doubly monotonic directions. In Example 4.1 one sum of squares is smaller than $50 - 2\sqrt{50} + 1 > 36$, but nevertheless the resulting directions are doubly monotonic.

5. Reconstruction

Many papers have been written on the actual reconstruction of the scanned object. If there is no nontrivial function with zero line sums in the directions of D, unique reconstruction is possible. Otherwise there is the possibility to reconstruct the function on certain parts of A and to find a good approximation on the remaining part of A or, depending on additional data, even to reconstruct the original function f completely. In general reconstruction is time-consuming and methods from linear algebra have been developed to do it relatively quickly. See e.g. [BatSi11].

Under certain conditions, in particular if D is invalid for A, the reconstruction can be done in time linear in the number mn of pixels. In the valid case this can be achieved for the complement of the convex hull of the union of the switching components. See [PaTi].

In some cases the function f can be written down explicitly as an expression in terms of the line sums, for example in the so-called Mojette case where A is a p by p square for p prime and the directions are $(1,0),(1,1),\ldots,(1,p-1)$ and $(0,1)$. See e.g. [GBB95].

References

[BatSi11] K.J. Batenburg, J. Sijbers, DART: A practical reconstruction algorithm for discrete tomography, *IEEE Transactions Image Processing* **20** (2011), 2542-2553.

[DaHaTi13] B. E. van Dalen, L. Hajdu, R. Tijdeman, Bounds for discrete tomography solutions, *Indag. Math.* **24** (2013), 391-402.

[GBB95] J.-P. Guédon, D. Barba, N. Burger, Psychovisual image coding via an exact discrete Radon transform, *Proc. SPIE*, vol. 2501, 1995, pp. 562-572.

[GN95] J.-P. Guédon, N. Normand, The Mojette transform: The first ten years, *Discrete Geometry for Computer Imagery*, LNCS 3429, Springer-Verlag, 1995, pp. 79-91.

[HaTi01] L. Hajdu, R. Tijdeman, Algebraic aspects of discrete tomography, *J. Reine Angew. Math.* **534** (2001), 119-128.

[HaTi07] L. Hajdu, R. Tijdeman, Algebraic discrete tomography, *Advances in Discrete Tomography and its Applications*, G.T. Herman, A. Kuba (eds.), Birkhäuser, 2007, pp. 55-81.

[HaTi13] L. Hajdu, R. Tijdeman, Bounds for approximate discrete tomography solutions, *SIAM J. Discrete Math.* **27** (2013), 1055-1066.

[HerKu99] *Discrete tomography, Foundations, algorithms, applications*, G.T. Herman, A. Kuba (eds.), Birkhăuser, Boston, 1999.

[HerKu07] *Advances in discrete tomography and its applications*, G.T. Herman, A. Kuba (eds.), Birkhăuser, Boston, 2007.

[Kat77] M. Katz, *Questions of uniqueness and resolution in reconstruction from projections*, Springer Verlag, 1977.

[Knu81] D.E. Knuth, *The Art of Computer Programming Vol.2 / Seminumerical Algorithms*, Addison-Wesley, Reading MA, 2nd ed., 1981.

[Lan81] S. Lang, *Algebra*, Addison-Wesley, Reading MA, 7th ed., 1977.

[Lev56] W.J. Leveque, *Topics in Number Theory I*, Addison-Wesley, 1956.

[Nat01] F. Natterer, *The mathematics of computerized tomography*, SIAM, Philadelphia, 2001.

[PaTi] S. Pagani, R. Tijdeman, Algorithms for fast reconstruction by discrete tomography, to appear.

[Sto11] A.P. Stolk, *Discrete tomography for integer-valued functions*, PhD-thesis, Leiden University, 2011.

[StoBat10] A.P. Stolk and K. J. Batenburg, An algebraic framework for discrete tomography, *SIAM J. Discrete Math.*, **24** (2010), 1056-1079.

Rob Tijdeman
Mathematical Institute
Leiden University
2300 RA Leiden, P.O. Box 9512
The Netherlands
e-mail: tijdeman@math.leidenuniv.nl