Discrete Mathematics 108 (1992) 139–147
North-Holland

Invertibility of the base Radon transform of a matroid

Anders Björner and Johan Karlander
Department of Mathematics, Royal Institute of Technology, S-100 44 Stockholm, Sweden

Received 21 March 1991

Abstract

Björner, A. and J. Karlander, Invertibility of the base Radon transform of a matroid, Discrete Mathematics 108 (1992) 139–147.

Let M be a matroid of rank r on n elements and let $\boldsymbol{F}$ be a field. Assume that either char $\boldsymbol{F}=0$ or char $\boldsymbol{F}>r$. It is shown that the point-base incidence matrix of M has rank $n-k+1$ over $\boldsymbol{F}$, where k is the number of connected components. This implies that the Radon transform on the family of bases is invertible if and only if the matroid is connected. If M is loop-free then the Radon transform on the family of m-element independent sets is invertible, for every $0<m<r$.

1. Introduction

Let E be a set of n elements and $f: E \to \boldsymbol{F}$ a function with values in a field $\boldsymbol{F}$. The Radon transform Rf of f is the $\boldsymbol{F}$-valued function on the family of subsets of E defined by

$$Rf(A) = \sum_{x \in A} f(x) \quad \text{for every } A \subseteq E.$$

If the A's belong to a specific family $\mathscr{A}$ of subsets we make the following definition:
The Radon transform is *invertible* on $\mathscr{A}$ if and only if $Rf(A) = Rg(A)$ for all $A \in \mathscr{A}$ implies that $f = g$.

The Radon transform can be expressed in a different way by the use of matrices. Suppose that the elements in E and $\mathscr{A}$ are enumerated such that $E = \{x_1, \ldots, x_n\}$ and $\mathscr{A} = \{A_1, \ldots, A_m\}$. We now define the incidence matrix $I(\mathscr{A}, E)$ by

$$I(\mathscr{A}, E) = M \iff M_{i,j} = \begin{cases} 1 & \text{if } x_j \in A_i, \\ 0 & \text{if } x_j \notin A_i. \end{cases}$$

If

$$\bar{f} = \begin{pmatrix} f(x_1) \\ \vdots \\ f(x_n) \end{pmatrix} \quad \text{and} \quad \overline{Rf} = \begin{pmatrix} Rf(A_1) \\ \vdots \\ Rf(A_m) \end{pmatrix}$$

then $\overline{Rf} = I(\mathscr{A}, E) \cdot \bar{f}$. Clearly, the $\boldsymbol{F}$-Radon transform is invertible on $\mathscr{A}$ if and only if $\mathrm{rank}_{\boldsymbol{F}}(I(\mathscr{A}, E)) = n$.

Therefore, to find out whether the Radon transform is invertible or not is a special case of the problem of finding the rank of $I(\mathscr{A}, E)$. Of course, for complicated families $\mathscr{A}$ this is not necessarily a simple problem.

In this paper we will study the case when $\mathscr{A}$ is the family of bases of a matroid on the set E. Such incidence matrices have earlier been studied from a polyhedral point of view (and hence over the field of real numbers) by Edmonds [5].

Of course, the Radon transform cannot in this case be generally invertible. The most striking counterexample is perhaps when M is the free matroid with $B = E$ as the only base. The concept of *connectivity* plays a key role in this problem. Indeed, let M be a connected matroid of rank r, and assume that either $\mathrm{char}\, \boldsymbol{F} = 0$ or $\mathrm{char}\, \boldsymbol{F} > r$. Then the Radon transform is invertible on the family $\mathscr{B}(M)$ of bases. This is our Theorem 1.

If M is not connected then E can be subdivided into k connected components. Assume that $\mathrm{char}\, \boldsymbol{F} = 0$ or that $\mathrm{char}\, \boldsymbol{F}$ is greater than the matroid rank of any component. In this case $\mathrm{rank}_{\boldsymbol{F}}(I(\mathscr{B}, E)) = |E| - k + 1$. This is our Theorem 2. The characteristic 0 case of this rank formula is implicit in Edmonds' work [5].

Our proof of the last theorem uses the fact that $I(\mathscr{B}, E)$ can be regarded as a kind of composition of the incidence matrices corresponding to the components of M. This construction allows us to generalize Theorem 2 in a purely matrix-theoretic way. This generalization is our Theorem 3.

The finite Radon transform has previously been studied in several papers, see e.g. [2, 4, 6, 7]. From a matroid-theoretic point of view the paper of Kung [6] is particularly interesting. He proves that the family of hyperplanes of a simple matroid has invertible Radon transform, and similarly for the family of circuits of a matroid whose dual is simple.

2. Invertibility on matroids

We will assume familiarity with elementary matroid theory, see e.g. [8, 9]. Nevertheless we begin by reviewing a few basic concepts.

Let M be a matroid with E as the set of elements, $\mathscr{B}(M)$ as the family of bases, $\mathscr{I}(M)$ as the family of independent sets and $\mathscr{C}(M)$ as the family of circuits. Let A be an arbitrary subset of E. The following defines the *deletion* and *contraction* by A:

- $M \backslash A$ is the matroid with $E - A$ as elements and $\{X : X \subseteq E - A, X \in \mathscr{I}(M)\}$ as independent sets.

• M/A is the matroid with $E - A$ as elements and $\{X: X \subseteq E - A, X \cup Y \in \mathcal{I}(M)$ where Y is a basis of $A\}$ as independent sets.

We define a relation $\sim$ on the set E by

$$x \sim y \Leftrightarrow x = y \quad \text{or} \quad \exists C \in \mathcal{C}(M) \quad \text{with} \quad \{x, y\} \subseteq C.$$

The relation $\sim$ can be shown to be an equivalence relation. Its equivalence classes are called the *components* of M. If M has only one component we say that M is *connected.*

Our aim is to prove the following theorems. In all the following we assume that $\boldsymbol{F}$ is a field such that $\operatorname{char} \boldsymbol{F} = 0$ or $\operatorname{char} \boldsymbol{F} > r_{\max}$ where $r_{\max} = \max\{\operatorname{rank}(M_i)$: M_i is a component of $M\}$. If M is connected then $r_{\max} = r$.

Theorem 1. *If M is a connected matroid with $|E| \geqslant 2$ then the Radon transform is invertible on $\mathcal{B}(M)$.*

Theorem 2. *If $B = I(\mathcal{B}(M), E)$ is the base incidence matrix of a matroid M with n elements, not all loops, and if the number of components of M is k, then* $\operatorname{rank}_{\boldsymbol{F}}(B) = n - k + 1$.

As was discussed in the introduction, Theorem 1 is a restatement of the $k = 1$ case of Theorem 2. Our method of proof is to first establish Theorem 1 with the use of matroid structure, and then deduce Theorem 2 by completely general arguments. These results are in general false when $2 \leqslant \operatorname{char} \boldsymbol{F} \leqslant r_{\max}$. For instance, the columns of $I(\mathcal{B}(M), E)$ are clearly dependent over $\boldsymbol{F}$ whenever $\operatorname{char} \boldsymbol{F}$ divides r.

Corollary. *For a connected matroid M there exists an injective mapping $\phi : E \rightarrow \mathcal{B}(M)$ such that $x \in \phi(x)$ for all $x \in E$.*

Such a matching can be found by picking out n bases $\mathcal{B}'$ such that the square matrix $I(\mathcal{B}', E)$ is nonsingular, and then finding a nonzero term in the defining expansion of $\det I(\mathcal{B}', E)$.

It is a consequence that $|\mathcal{B}(M)| \geqslant |E|$ for every connected matroid M. However, this inequality is known to hold for the larger class of all matroids without isthmuses and loops, and for connected matroids much better lower bounds for $|\mathcal{B}(M)|$ are known, see e.g. [1, Propositions 7.5.1 and 7.5.4].

Since every proper truncation of a loop-free matroid is connected we can also deduce the following consequence of Theorem 1.

Corollary. *If M is a loop-free matroid of rank r then the $\boldsymbol{F}$-Radon transform is invertible on the family $\mathcal{I}_k(M)$ of k-element independent subsets, for every* $0 < k < r$.

The following lemma, due to Crapo [3], will be of crucial importance for the proof.

Lemma. *Let M be a connected matroid and e an arbitrary element. Then $M\backslash e$ or M/e is connected.*

We will also make use of the following observation: If e is an element in a connected matroid M (actually we only need that e is neither a loop nor an isthmus) then there exist bases $B_1, B_2 \in \mathcal{B}(M)$ such that $e \in B_1$ and $e \notin B_2$.

Proof of Theorem 1. We use induction on the size of $|E|$. When $E = \{x, y\}$ the only possible connected matroid over E is generated by the bases $B_1 = \{x\}$, $B_2 = \{y\}$. Obviously, the Radon transform is invertible on B_1, B_2.

Suppose the theorem is true for $|E| \leq n$. Let M be a connected matroid with $|E| = n + 1$ and let $Rf : \mathcal{B}(M) \to \boldsymbol{F}$ be the known Radon transform of a function f. We then must show that $f(x)$ can be uniquely determined for all $x \in E$. We choose an element $e \in E$ and make use of the lemma. There are two cases to consider.

Case 1: *$M\backslash e$ is connected.*

Since $\mathcal{B}(M\backslash e) = \{B' : B' \in \mathcal{B}(M) \text{ and } e \neq B'\}$ the Radon transform $Rf(B')$ is known for every $B' \in \mathcal{B}(M\backslash e)$. By induction, it is possible to determine $f(x)$ for all $x \in E - \{e\}$ and, since there exists a $B \in \mathcal{B}(M)$ with $e \in B$, $f(e)$ can be calculated by

$$f(e) = Rf(B) - \sum_{x \in B - \{e\}} f(x).$$

We conclude that Rf is invertible on $\mathcal{B}(M)$.

Case 2: *M/e is connected.*

In this case, $\mathcal{B}(M/e) = \{B' : B' = B - \{e\},\ B \in \mathcal{B}(M),\ e \in B\}$. Let $f(e) = t$. Then

$$Rf(B') = Rf(B) - t.$$

By induction, the Radon transform is invertible on the sets B', and since it is a linear transform we can express $f(x)$ on the form

$$f(x) = a_x + b_x t,$$

where a_x and b_x are known elements of $\boldsymbol{F}$, depending only on x.

We now show that t can indeed be determined and thereby all $f(x)$. If there exists a B' with $\sum b_x \neq -1$, where $x \in B'$, then t can be found by solving the equation

$$Rf(B' \cup e) = t + \sum_{x \in B'} (a_x + b_x t).$$

On the other hand, suppose that $\sum b_x = -1$ for all $B' = \mathcal{B}(M/e)$. Define a function g on $E - \{e\}$ by $g(x) = b_x$. The Radon transform of g on $\mathcal{B}(M/e)$ is $Rg(B') = -1$ for all $B' \in \mathcal{B}(M/e)$. Let $m = r - 1$ be the common cardinality of the bases B' and define a function h by $h(x) = -1/m$ for all $x \in E - \{e\}$. Then $Rh(B') = -1$ for all B', i.e.,

$$Rg(B') = Rh(B') \quad \text{for all} \quad B' \in \mathcal{B}(M/e).$$

By the invertibility of the Radon transform we find that $g = h$, so $b_x = -1/m$ for all $x \in E - \{e\}$. Now, let B_0 be a base of M not containing e. Then t is given by the equation

$$Rf(B_0) = \sum_{x \in B_0} (a_x + b_x t) = \sum_{x \in B_0} (a_x - t/m) = \sum_{x \in B_0} a_x - t(m+1)/m.$$

Note that we have used that both m and $m + 1$ are invertible in $\boldsymbol{F}$, which follows from the assumption that $\operatorname{char} \boldsymbol{F} = 0$ or $\operatorname{char} \boldsymbol{F} > r = m + 1$.

We conclude that Rf is invertible on $\mathcal{B}(M)$. □

Proof of Theorem 2. First, suppose that M contains a set of loops E_0. In that case every loop l forms a component with l as its only element. The columns in B corresponding to E_0 contain only zeroes. If we let $M' = M \backslash E_0$ we get a matroid with $n' = n - |E_0|$ elements and $k' = k - |E_0|$ components. Let B' be the new base incidence matrix. If the theorem is true for B' then

$$\operatorname{rank}(B) = \operatorname{rank}(B') = n' - k' + 1 = n - k + 1.$$

Therefore, we may assume that M does not contain any loops.

Now, enumerate the components $M_1, M_2, \ldots, M_k$. Every component forms a connected matroid with a set of bases. Let these bases be enumerated so that $A_{i,j}$ means base j in M_i. Obviously, A is a base in M if and only if

$$A = A_{1,j_1} \cup A_{2,j_2} \cup \cdots \cup A_{k,j_k},$$

where $1 \leq j_p \leq m_p$ and m_p is the number of bases in M_p. By r_p we shall mean the cardinality of the bases in M_p. Let

$$\bar{\lambda} = \begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_n \end{pmatrix}.$$

We will show that $B\bar{\lambda} = \bar{0}$ if and only if there is a vector

$$\bar{\mu} = \begin{pmatrix} \mu_1 \\ \vdots \\ \mu_k \end{pmatrix}$$

such that $x_i, x_j \in M_p$ implies $\lambda_i = \lambda_j = \mu_p$ for all i, j and $\mu_1 r_1 + \cdots + \mu_k r_k = 0$.

Indeed, let $B\bar{\lambda} = \bar{0}$ and let $x_i, x_j \in M_p$. There exist m_p bases of the form

$$A_{1,1} \cup A_{2,1} \cup \cdots \cup A_{p,q} \cup \cdots \cup A_{k,1}, \quad \text{where} \quad 1 \leq q \leq m_p.$$

Let $\alpha = \sum \lambda_s$ where the summation runs over all s such that

$$x_s \in A_{1,1} \cup A_{2,1} \cup \cdots \cup A_{p-1,1} \cup A_{p+1,1} \cup \cdots \cup A_{k,1}.$$

If H_p is the incidence matrix of the family $\{A_{p,q}\}$ and $\bar{\lambda}'$ is the vector $\bar{\lambda}$ restricted to M_p then

$$H_p\bar{\lambda}' = -\begin{pmatrix} \alpha \\ \vdots \\ \alpha \end{pmatrix}.$$

Since char $\boldsymbol{F} = 0$ or char $\boldsymbol{F} > r_p$ we can use Theorem 1 to find that there is only one solution to this equation, namely

$$\bar{\lambda}' = -\frac{\alpha}{r_p}\begin{pmatrix} 1 \\ \vdots \\ 1 \end{pmatrix}.$$

(This is of course also true when the size of the component is 1.)

We can now set $\mu_p = -\alpha/r_p$. Since

$$H_p\mu_p\begin{pmatrix} 1 \\ \vdots \\ 1 \end{pmatrix} = \mu_p r_p\begin{pmatrix} 1 \\ \vdots \\ 1 \end{pmatrix} \quad \text{for all } p,$$

we get

$$B\bar{\lambda} = (\mu_1 r_1 + \cdots + \mu_k r_k)\begin{pmatrix} 1 \\ \vdots \\ 1 \end{pmatrix}.$$

Then, $B\bar{\lambda} = \bar{0}$ implies that $\mu_1 r_1 + \mu_2 r_2 + \cdots + \mu_k r_k = 0$.

Conversely, it is obvious that every vector $\bar{\lambda}$ with $\lambda_i = \lambda_j = \mu_p$ if $x_i, x_j \in M_p$ and $\mu_1 r_1 + \mu_2 r_2 + \cdots + \mu_k r_k = 0$ satisfies $B\bar{\lambda} = \bar{0}$.

Since all $r_i \neq 0$, the choice of the μ_i's is restricted to $k-1$ degrees of freedom, i.e., the kernel of B is of dimension $k-1$.

We conclude that $\text{rank}(B) = n - k + 1$. □

3. Composition of matrices

Let $M_1, M_2, \ldots, M_k$ be a set of matrices with entries from a given field $\boldsymbol{F}$, which in this section may be of arbitrary characteristic. We assume that the size of M_i is $m_i \times n_i$. Now, we define a $(m_1 \cdots m_k) \times (n_1 + \cdots + n_k)$-matrix $M = M_1 \vee M_2 \vee \cdots \vee M_k$ in the following way: Let W be the set of vectors $w =$

$(a_1, a_2, \ldots, a_k)$ where $a_i \in \{1, \ldots, m_i\}$. Given $w \in W$ we let $r(w)$ be the $(n_1 + \cdots + n_k)$-vector obtained by concatenating the rows $a_1, \ldots, a_k$ of $M_1, \ldots, M_k$. The $m_1 \cdots m_k$ vectors thus obtained will be ordered lexicographically. Let M be the matrix with the rows $r(w_1), \ldots, r(w_{m_1 \cdots m_k})$.

We will now establish the connection between the matrix ranks of the M_is and the rank of M over F. To this end we will need the following definition.

Definition. A matrix A is said to be *balanced* if there exists a vector $\bar{x}$ such that

$$A\bar{x} = \begin{pmatrix} 1 \\ \vdots \\ 1 \end{pmatrix}.$$

Theorem 3. *If* $M = M_1 \vee M_2 \vee \cdots \vee M_k$ *then* $\operatorname{rank}_F(M) = \sum_{i=1}^{k} \operatorname{rank}_F(M_i) - \max(p, 1) + 1$, *where p is the number of balanced matrices M_i.*

Proof. To the row number i in M we have a corresponding vector w_i. If $w_i = (a_1, \ldots, a_k)$ we let $p(w_i)$ be a $(m_1 + \cdots + m_k)$-vector with 1 in the positions $m_1 + \cdots + m_{j-1} + a_j$, $1 \leq j \leq k$, and 0 in all other positions. Let J be the $(m_1 \cdots m_k) \times (m_1 + \cdots + m_k)$-matrix with the vectors $p(w_i)$ as rows.

Next, we define a $(m_1 + \cdots + m_k) \times (n_1 + \cdots + n_k)$-matrix M' in the following way:

$$M' = \begin{pmatrix} M_1 & 0 & 0 & \cdots & 0 \\ 0 & M_2 & 0 & \cdots & 0 \\ 0 & 0 & M_3 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & M_k \end{pmatrix},$$

i.e., the diagonal consists of the matrices M_i and the rest of M' of zeroes. Obviously, $\operatorname{rank}(M') = \sum \operatorname{rank}(M_i)$. Furthermore, it is easily realized that $M = J \cdot M'$.

The null space $\mathcal{N}(J) = \{\bar{x} : J\bar{x} = \bar{0}\}$ has dimension $k - 1$. Indeed, suppose $J\bar{x} = \bar{0}$. We can enumerate the components of $\bar{x}$ such that $x_{i,j}$ is the component in position $m_1 + \cdots + m_{i-1} + j$. For every i, j_1, j_2 such that

$$1 \leq i \leq k, \qquad 1 \leq j_1, j_2 \leq m_i$$

we can deduce the equation $x_{i,j_1} - x_{i,j_2} = 0$, i.e., there exists y_i such that

$$x_{i,j} = y_i, \qquad 1 \leq j \leq m_i, \quad 1 \leq i \leq k.$$

Therefore the equations in $J\bar{x} = \bar{0}$ are all equal to $y_1 + y_2 + \cdots + y_k = 0$, which implies that $\mathcal{N}(J)$ is $(k-1)$-dimensional.

Let $\mathscr{R}(M)$ be the range of M, i.e., $\mathscr{R}(M) = \{M\bar{x}\}$. Our objective is to find $\operatorname{rank}(M) = \dim \mathscr{R}(M)$. Since $M = J \cdot M'$, we have $\mathscr{R}(M) = J \cdot \mathscr{R}(M')$. If we let $\mathscr{N}' = \mathscr{R}(M') \cap \mathscr{N}(J)$ and make use of the dimension theorem of linear algebra we get

$$\dim \mathscr{R}(M) + \dim \mathscr{N}' = \dim \mathscr{R}(M'),$$

that is

$$\operatorname{rank}(M) = \sum_i \operatorname{rank}(M_i) - \dim \mathscr{N}'.$$

If $\bar{x}$ is a vector in $\mathscr{N}(J)$ then $\bar{x}$ can be represented by the numbers y_i, $1 \leqslant i \leqslant k$. We find that

$$\bar{x} \in \mathscr{R}(M') \iff y_i = 0 \quad \text{for every } M_i \text{ which is not balanced.}$$

Therefore, if $p \geqslant 1$ is the number of balanced M_i's, we get

$$\dim \mathscr{N}' = k - 1 - (k - p) = p - 1.$$

On the other hand, if $p = 0$ then $\dim \mathscr{N}' = 0$.

We conclude that

$$\operatorname{rank}(M) = \sum_i \operatorname{rank}(M_i) - \max(p, 1) + 1. \qquad \square$$

Theorem 3 has the following application to set families. Suppose that $\mathscr{B}_i$ is a collection of r_i-element subsets of E_i, for $1 \leqslant i \leqslant k$, and let $M_i = I(\mathscr{B}_i, E_i)$. In this case all the M_i's are balanced. Furthermore, let M be the incidence matrix of the set family $\{A_1 \cup \cdots \cup A_k : A_i \in M_i, 1 \leqslant i \leqslant k\}$. Assume that the ground sets E_i are pairwise disjoint. Then the theorem gives that

$$\operatorname{rank}(M) = \sum_i \operatorname{rank}(M_i) - k + 1.$$

Theorem 2 is a special case.

Note added in proof. We have subsequently extended Theorem 2 to all fields. The result for a field $\boldsymbol{F}$ of characteristic p (p a prime number or $p = 0$) is that

$$\operatorname{rank}_{\boldsymbol{F}}(B) = \begin{cases} n - k & \text{if } p \text{ divides } \operatorname{rank}(M_i) \text{ for all components } M_i, \\ n - k + 1, & \text{otherwise.} \end{cases}$$

This shows that Theorem 1 is valid for all fields whose characteristic does not divide $\operatorname{rank}(M)$.

The details will appear elsewhere.

Acknowledgement

We want to thank Bernt Lindström for very helpful suggestions.

References

[1] A. Björner, The homology and shellability of matroids and geometric lattices, in: N. White, ed., Matroid Applications (Cambridge Univ. Press, Cambridge, 1991) 226–283.
[2] E.D. Bolker, The finite Radon transform, in: Integral Geometry (Brunswick, Maine, 1984), Contemp. Math. 63 (1987), Amer. Math. Soc., Providence, RI, 27–50.
[3] H.H. Crapo, A higher invariant for matroids, J. Combin. Theory 2 (1967) 406–417.
[4] P. Diaconis and R.L. Graham, The Radon transform on Z_2^k. Pacific J. Math. 118 (1985) 323–345.
[5] J. Edmonds, Submodular functions, matroids, and certain polyhedra, in: Combinatorial Structures and their Applications, Proceedings Calgary 1969 (Gordon and Breach, New York, 1970) 69–87.
[6] J.P.S. Kung, The Radon transforms of a combinatorial geometry, J. Combin. Theory, Ser. A 26 (1979) 97–102.
[7] J.P.S. Kung, Matchings and Radon transforms in lattices. I. Consistent lattices, Order 2 (1985) 105–112.
[8] D.J.A. Welsh, Matroid Theory (Academic Press, London, 1976).
[9] N. White, ed., Theory of Matroids (Cambridge Univ. Press, Cambridge, 1986).