SIAM J. Discrete Math.
Vol. 18, No. 3, pp. 472–478

THE RADON TRANSFORM ON $\mathbb{Z}_n^k$*

MICHELLE R. DEDEO† AND ELINOR VELASQUEZ†

Abstract. The Radon transform on $\mathbb{Z}_n^k$ averages a function over its values on a translate of a fixed subset S in $\mathbb{Z}_n^k$. We discuss invertibility conditions and computer inverse formulas based on the Moore–Penrose inverse and on linear algorithms. We expect the results to be of use in directional and toroidal time series.

Key words. Radon transform, invertibility, Fourier transform

AMS subject classifications. Primary, 44A15; Secondary, 42A38

DOI. 10.1137/S0895480103430764

1. Introduction.

Suppose G is a finite group and fix $S \subset G$. Let $C(G)$ be the space of real-valued maps on G. A finite analogue of the Radon transform may be described as follows: For all $f \in C(G)$, define the Radon transform based on translates of $S \subset G$ as

$$\overline{f}(k) = \sum_{j \in S+a} f(j).$$

Diaconis and Graham [2] discuss the cases where $G = \mathbb{Z}_2^k$, the group of binary k-tuples, and where $G = S_n$, the symmetric group on n letters, in order to provide an exposition on discrete Radon transforms which appear in applied statistics. Fill [4] examines the case $G = \mathbb{Z}_n$, the group of integers modulo n. This case arises in directional data analysis and circular time series. Other finite analogues of the Radon transform occur, but we shall restrict ourselves to the case $G = \mathbb{Z}_n^k$, the group of k-tuples of the integers modulo n, as these results are of use in k-dimensional toroidal time series.

In section 1, we use representation theory as described in DeDeo and Velasquez [1] to describe the Radon transform on $\mathbb{Z}_n^k$ and its invertibility conditions. In section 2, we discuss a specific example, the Radon transform based on a translate of a fixed $S_r \subset \mathbb{Z}_n^k$, where S_r denotes a sphere of radius r. In this situation, $\mathbb{Z}_n^k$ is associated with a Cayley graph with a Hamming metric. The injectivity of the Radon transform is seen to depend on the zeros of particular Krawtchouk polynomials. The proof of this includes a counting argument rather than computing the appropriate spherical functions for the graph. Inversion formulas are presented in section 3. First, explicit formulas are computed using the Fourier transform, its inverse, and a Moore–Penrose generalized inverse transform. Then inverse algorithms, which do not rely on the Fourier transform, are described for the Radon transform based on translates of the fixed spheres S_r in $\mathbb{Z}_n^k$.

1.1. Motivation.

This is an extension of DeDeo and Velasqeuz [1] which attempts to extend directional data and time series to discretized analogues of manifolds. Two-dimensional manifolds are homomorphically either spheres with handles

*Received by the editors July 2, 2003; accepted for publication (in revised form) April 6, 2004; published electronically December 30, 2004.
http://www.siam.org/journals/sidma/18-3/43076.html

†Department of Mathematics and Statistics, University of North Florida, Jacksonville, FL 32224 (mdedeo@unf.edu, velasque@sfsu.edu).

or spheres with crosscaps. For dimensions greater than two, the situation is more complex. In this paper we shall inspect the discrete analogue of the sphere with k-handles, i.e., the discretized k-dimensional torus denoted by $\mathbb{Z}_n^k$.

Functions relevant to time series are the maps $f : T^k \to \mathbb{R}$ or $f : \mathbb{Z}_n^k \to \mathbb{R}$, with $\mathbb{Z}_n^k$ the proposed discretization of the k-fold torus. The act of employing a certain linear filter to functions on $\mathbb{Z}_n^k$ may be considered to be the mapping of f to $\overline{f}$, its Radon transform, where

$$\overline{f}(a) = \sum_{j \in \mathbb{Z}_n^k} \varphi(j-a) f(j)$$

for some $\varphi : \mathbb{Z}_n^k \to \mathbb{R}$. If φ is the characteristic function of a fixed S in $\mathbb{Z}_n^k$, the mapping above reduces to the usual Radon transform based on translates of S in $\mathbb{Z}_n^k$.

2. Fourier analysis on $\mathbb{Z}_n^k$. Throughout the next two sections, we set $G = \mathbb{Z}_n^k$, the group of k-tuples with elements in $\mathbb{Z}_n$. Explicitly, $\mathbb{Z}_n^k = (\mathcal{A}, +)$, where $\mathcal{A} = \{x | x = (x_1, x_2, \ldots, x_k)^t$ for x_i in $\mathbb{Z}_n$, where $i = 1, \ldots, k\}$. Assign the natural inner product to $\mathbb{Z}_n^k$ such that, for all x and y in $\mathbb{Z}_n^k$, $x \cdot y = \sum_{i=1}^k x_i y_i$. Thus $\mathbb{Z}_n^k$ is an abelian group under addition and its group representations all have degree one since $\mathbb{Z}_n^k \cong \prod^k \mathbb{Z}_n$. We have that the characters are the homomorphisms $\chi_j : \mathbb{Z}_n^k \to \mathbb{C}^\times$, where

$$\chi_j(z) = \prod_{i=1}^k \chi_{j_i}(z_i)$$

for all $z = (z_1, z_2, \ldots, z_k)^t$ and $j = (j_1, j_2, \ldots, j_k)^t$ in $\mathbb{Z}_n^k$, $\mathbb{C}^\times$ denotes the nonzero complex numbers, and χ_j denotes the character of the jth copy of $\mathbb{Z}_n$. Recall that the characters of $\mathbb{Z}_n$ are explicitly the functions $\chi_m : \mathbb{Z}_n \to \mathbb{C}^\times$ defined by $\chi_m(y) = \omega^{m \cdot y}$ for $m \in \{0, \ldots, n-1\}$, where $\omega = e^{\frac{2\pi i}{n}}$, an nth root of unity. Thus we have that $\chi_j : \mathbb{Z}_n^k \to \mathbb{C}^\times$ defined by $\chi_j(z) = \omega^{j \cdot z}$ indexed by $j \in \mathbb{Z}_n^k$ are the inequivalent, irreducible unitary representations of $\mathbb{Z}_n^k$. We denote the Hilbert spaces of functions on $\mathbb{Z}_n^k$ and $\widehat{\mathbb{Z}_n^k}$, the space of characters of $\mathbb{Z}_n^k$, by $\mathcal{L}^2(\mathbb{Z}_n^k)$, and the space of square-differentiable functions on $\mathbb{Z}_n^k$ by $\mathcal{L}^2(\widehat{\mathbb{Z}_n^k})$.

The Fourier transform for $\mathbb{Z}_n^k$ from $\mathcal{L}^2(\mathbb{Z}_n^k) \to \mathcal{L}^2(\widehat{\mathbb{Z}_n^k})$ is

$$(\mathcal{F}f) = \widehat{f}(x) = \widehat{f}(\chi_x) = \sum_{f(y) \in \mathbb{Z}_n^k} \chi_x(y) = \sum_{f(y) \in \mathbb{Z}_n^k} f(y) \omega^{x \cdot y}$$

with the Fourier inverse from $\mathcal{L}^2(\widehat{\mathbb{Z}_n^k}) \to \mathcal{L}^2(\mathbb{Z}_n^k)$ as

$$\begin{aligned}(\mathcal{F}^{-1}\widehat{f}) = f(y) &= \frac{1}{n^k} \sum_{\widehat{f}(y) \in \widehat{\mathbb{Z}_n^k}} \chi(y^{-1}) \widehat{f}(\chi) \\ &= \frac{1}{n^k} \sum_{x \in \mathbb{Z}_n^k} \chi_x(y^{-1}) \widehat{f}(\chi_x) \\ &= \frac{1}{n^k} \sum_{x \in \mathbb{Z}_n^k} \omega^{-x \cdot y} \widehat{f}(x).\end{aligned}$$

For all functions $f \in C(\mathbb{Z}_n^k)$, the Radon transform

$$(\mathcal{R}f) = \overline{f}(a) = \sum_{j \in S+a} f(j) = \sum_{j \in \mathbb{Z}_n^k} \varphi_S(j-a) f(j),$$

where $\varphi_S(\cdot)$ is the characteristic function of S in $\mathbb{Z}_n^k$. Therefore, we can identify the Radon transform $\mathcal{R}$ with the matrix

$$(\mathcal{R})_{k,j} = \varphi_S(j-k)$$

and the finite Fourier transform $\mathcal{F}$ and its inverse with the matrices

$$(\mathcal{F})_{l,m} = \omega^{l\cdot m} \text{ and } \left(\mathcal{F}^{-1}\right)_{l,m} = \frac{1}{n^k}\,(\mathcal{F})^*_{m,l} = \frac{1}{n^k}\omega^{l\cdot m},$$

respectively, where ω is a fixed root of unity and * denotes the conjugate transpose. We wish to describe the invertibility of the Radon matrix. The group $\left(\mathbb{Z}_n^k, +\right)$ is abelian; therefore, singular value decompression via Fourier matrices results in a diagonal matrix.

Proposition 2.1. *$(\mathcal{F}\mathcal{R}\mathcal{F}^*)_{j,l} = \delta_{j,l} n^k \widehat{\varphi}_s(-l)$, where $\delta_{j,l} = 1$ if $j = l$ and 0 otherwise.*

Proof. We refer the reader to DeDeo and Velasquez [1]. □

We note that the Radon matrix is not invertible if $S = \mathbb{Z}_n^k$ as it leads to a matrix of all 1's, and that the matrix is always invertible if S has one element.

3. The Krawtchouk polynomial and invertibility. Consider a subset of $\mathbb{Z}_n^k$. Specifically, for a fixed $r \in \mathbb{N}$, set $S = S_r = \{x \in \mathbb{Z}_n^k | H(x) = r\} = H(x)$, where $H(x)$ is the Hamming distance of x from the origin of $\mathbb{Z}_n^k$. In other words, we associate $\mathbb{Z}_n^k$ with the graph $X = X(V, E)$ with vertex set $V = \mathbb{Z}_n^k$ and edge set $E = \{(x, y) \in V \times V | H(x, y) = 1\}$, and where $H(x)$ is the Hamming metric, the number of coordinates in which x and y differ.

Definition 3.1. *Fix the following integers r in $0, \ldots, k$ and let q be a prime. The Krawtchouk polynomial (MacWilliams and Sloane [6]) is*

$$p_r^k(\nu; q) = \sum_{l\in\mathbb{Z}_r} (-1)^l (q-1)^{k-1} \binom{\nu}{l}\binom{k-\nu}{r-l},$$

where $\binom{a}{b}$ denotes the usual binomial coefficient. Setting $q = 2$ results in the form we will be using for the remainder of the paper:

$$p_r^k(\nu) = \sum_{l\in\mathbb{Z}_r} (-1)^l \binom{\nu}{l}\binom{k-\nu}{r-l}.$$

Proposition 3.2 (DeDeo and Velasquez [1]). *For $x \in \mathbb{Z}_n^k$, $\widehat{\varphi_{S_r}}(x) = p_r^k(H(x))$.*

Proof. For $x \in \mathbb{Z}_n^k$, we have $\widehat{\varphi_{S_r}}(x) = \sum_{s\in S_r} \omega^{x\cdot s}$, where ω is a primitive nth root of unity. Since $\widehat{\varphi_{S_r}}(x)$ depends on $x = (x_1, \ldots, x_k)^t$ in $\mathbb{Z}_n^k$ only through the unordered set $\{x_1, \ldots, x_k\}$, then we may assume, without loss of generality, that $x_i \neq 0$ for $i = 1, \ldots, h$, where $h := H(x)$ and $x_i = 0$ for $i = h+1, \ldots, k$. Now

$$\widehat{\varphi_{S_r}}(x) = \sum_{l=0}^{r} \sum_{\{\alpha_1,\ldots,\alpha_l\}\subset\{1,\ldots,k\}} \sum_{s\in S_r(\{\alpha_1,\ldots,\alpha_l\})} \omega^{x\cdot s}$$

with $S_r(\{\alpha_1, \ldots, \alpha_l\}) := \{s \in S | s_i \neq 0 \text{ for } i \in \{\alpha_1, \ldots, \alpha_l\} \text{ and } s_i = 0 \text{ for } i \in \{1, \ldots, k\}/\{\alpha_1, \ldots, \alpha_l\}\}$.

Then

$$\begin{aligned}\sum_{s\in S_r(\{\alpha_1,\ldots,\alpha_l\})}\omega^{x\cdot s} &= \binom{k-h}{r-l}\sum_{S_{\alpha_1}\neq 0}\cdots\sum_{S_{\alpha_l}\neq 0}\omega^{\sum_{j=1}^{l}x_{\alpha_j}\cdot s_{\alpha_j}}\\ &= \binom{k-h}{r-l}\prod_{j=1}^{l}\left[\sum_{s=1}^{k}\omega^{x_{\alpha_j}\cdot s}\right]\\ &= \binom{k-h}{r-l}\prod_{j=1}^{l}\left[0-\omega^{x_{\alpha_j}\cdot 0}\right]\\ &= (-1)^l\binom{k-h}{r-l}\end{aligned}$$

since ω is a primitive root of unity and $x_{\alpha_j}\neq 0$.

Hence $\widehat{\varphi_{S_r}}(x)=\sum_{l=0}^{r}\binom{H(x)}{l}(-1)^l\binom{k-H(x)}{r-l}=p_r^k(H(x))$. □

4. Inversion algorithms. We now consider the case of an invertible Radon matrix along with a typically noninvertible Radon matrix. Inversion formulas using standard Fourier methods are constructed. Then follows an exposition of inversion algorithms which do not use Fourier transforms.

DEFINITION 4.1. *If T is a finite-dimensional matrix, let the Moore–Penrose generalized inverse matrix of T be the unique matrix U satisfying* (1) $TUT=T$; (2) $UTU=U$; (3) $(TU)^*=TU$; (4) $(UT)^*=UT$, *where* * *is the conjugate transpose of* T.

We shall denote U by $T^{\div}$.

PROPOSITION 4.2 (DeDeo and Velasquez [1]). *Suppose $f\in C(\mathbb{Z}_n^k)$. Then we have the following.*

i. *If $\varphi_S(x)\neq 0$ for all $x\in\mathbb{Z}_n^k$, then, for all $z\in\mathbb{Z}_n^k$,*

$$f(x)=\sum_{z\in\mathbb{Z}_n^k}\overline{f}(z)\cdot\frac{1}{n^k}\sum_{y\in\mathbb{Z}_n^k}\frac{\omega^{(z-x)\cdot y}}{\widehat{\varphi_{S_r}}(-y)}.$$

ii. *If $\varphi_S(x)=0$ for some $x\in\mathbb{Z}_n^k$, let matrix Λ be given by*

$$(\Lambda)_{j,l}=\delta_{jl}n^k\sum_{s\in S}\omega^{-l\cdot s},$$

which implies that

$$(\Lambda^{\div})_{jl}=\delta_{jl}\lambda_l^{\div} with \lambda_l^{\div}=\begin{cases}\frac{1}{n^k}\left(\sum_{s\in S}\omega^{-l\cdot s}\right)^{-1} & if \sum_{s\in S}\omega^{-l\cdot s}\neq 0.\\ 0 & otherwise\end{cases}$$

Then $f=\mathcal{R}^{\div}\overline{f}$ with $\mathcal{R}^{\div}\equiv\mathcal{F}^*\Lambda^{\div}\mathcal{F}$. In other words, the reconstruction of $f\in C(\mathbb{Z}_n^k)$ for $\widehat{\varphi_S}(x)$ is

$$f(x)\overset{def}{=}\mathcal{R}^{\div}(\overline{f}(x))=\frac{1}{n^k}\sum_{y,z\in\mathbb{Z}_n^k}\lambda_y^{\div}\omega^{y\cdot(z-x)}\overline{f}(x).$$

Fill [4] estimates the possibility of the accurate reconstruction of a function by a least squares error discussion. This argument is completely valid for $\mathbb{Z}_n^k$. Hence, we provide a brief sketch here and refer the reader to Fill [4] for the details.

Given g in $C(\mathbb{Z}_n^k)$, we need to redefine the residual vector $E(f)$ for all f in $C(\mathbb{Z}_n^k)$ such that

$$E(f) = g - \mathcal{R}f \text{ in } C(\mathbb{Z}_n^k).$$

Then

$$\|E(f)\|^2 = \|g - \mathcal{R}f\|^2 = \sum_{x \in \mathbb{Z}_n^k} |g(x) - (\mathcal{R}f)(x)|^2 .$$

If $f_0 = \mathcal{R}^{\div}\overline{f}$ and $f = f_0 + h$, where $h \in C(\mathbb{Z}_n^k)$, then the least squares error is

$$\|E_0\|^2 = \|f - f_0\|^2 = \left\|(I - \mathcal{R}\mathcal{R}^{\div})g\right\|,$$

where I is the identity transform.

We now consider inversion algorithms based on a linear equations approach rather than the use of Fourier transforms. Diaconis and Graham [2] consider algorithms for shells and balls of Hamming radius 1. We shall consider shells to indicate the general scheme.

Proposition 4.3. *Suppose f is in $C(\mathbb{Z}_n^k)$. For $m \in \{0, \ldots, k\}$, define*

$$g(m) = \sum_{H(x)=m} f(x) \quad \textit{and} \quad \overline{g}(m) = \sum_{H(x)=m} \overline{f}(x),$$

where $\overline{f}$ is the Radon transform of f on translates of a shell of Hamming radius 1. Then

$$\overline{g}(m) = (n-1)(k-m+1) \cdot g(m-1) + (n-2)m \cdot g(m) + (m+1) \cdot g(m+1)$$

with $\overline{g}(-1) \equiv \overline{g}(k+1) \equiv 0$.

Proof. Given $f \in C(\mathbb{Z}_n^k)$, note that the Radon transform of f on a shell of radius 1 is

$$\overline{f}(x) = \sum_{y \in S_1 + x} f(y) = \sum_{y: H(x,y)=1} f(y).$$

Given x in $\mathbb{Z}_n^k$, we examine y in $\mathbb{Z}_n^k$ such that $H(x, y) = 1$. Suppose $x \in S_m \overset{def}{=} \{x \in \mathbb{Z}_n^k | H(x) = m\}$. Then there are three possible radii for $y : H(y) = m-1, m$, or $m+1$. We shall consider each case separately.

First, we discuss some notation. Fix $m \in \{0, \ldots, k\}$ and consider $w = w_{i_1} \ldots w_{i_m}$ in S_m. Then w has m nonzero coordinates w_{i_α} for $\alpha \in \{1, \ldots, m\}$. We choose $\{i_\alpha\}_1^m \subset \{j\}_1^k$.

1. $H(y) = m - 1$. Let $x = x_{i_1} \ldots x_{i_m} \in S_m$. It is clear that there exists a y in S_{m-1} such that $y = x_{i_1} \ldots x_{i_{m-1}}$. For a fixed y, partition S_m into subsets where

$$\mathcal{F}_y = \{x_{i_1} \ldots x_{i_{m-1}} x_{i_m} | y = x_{i_1} \ldots x_{i_{m-1}}\}.$$

Since x_{i_m} has $k - (m-1)$ possible coordinate positions in the k-tuple and $n - 1$ possible nonzero values to assume at each position, we have that the cardinality of $\mathcal{F}_y$ is $(k-m+1)(n-1)$ for a fixed y. It is also clear that there is a one-to-one correspondence between the $y \in S_m$ and $\mathcal{F}_y$.

2. $H(y) = m$. Let $x = x_{i_1} \dots x_{i_m} \in S_m$. Each x_{i_a} has some value in $\mathbb{Z}^\times$. Thus each coordinate is a map $x_{i_\nu} : \mathcal{A} \subset \mathbb{Z}_n^k \to \mathbb{Z}_n^\times$, where $x_{i_\nu} \to x_{i_\nu}(\beta_\nu) \equiv x_{i_\nu}^{\beta_\nu}$ for $\nu = 1, \dots, m$. Fix x_0 in S_m. Then x_0 looks like $x_{i_1}^{\alpha_1} \dots x_{i_m}^{\alpha_m}$ for fixed coordinate positions $\{i_\nu\}_1^m$ and fixed values $\{\alpha_\nu\}_1^m$. If $y \in S_m \cap \{y | H(x,y) = 1\}$, then y can have the forms

$$x_{i_1}^{\beta_1} x_{i_2}^{\alpha_2} x_{i_3}^{\alpha_3} \dots x_{i_m}^{\alpha_m}, \quad x_{i_1}^{\alpha_1} x_{i_2}^{\beta_2} x_{i_3}^{\alpha_3} \dots x_{i_m}^{\alpha_m}, \dots, \quad x_{i_1}^{\alpha_1} \dots x_{i_{m-1}}^{\alpha_{m-1}} x_{i_m}^{\beta_m},$$

where $\beta_j \neq \alpha_j$ for $j = 1, \dots, m$. Outputting other x's of the form

$$x_{i_1}^{\gamma_1} x_{i_2}^{\alpha_2} x_{i_3}^{\alpha_3} \dots x_{i_m}^{\alpha_m}, \quad x_{i_1}^{\alpha_1} x_{i_2}^{\gamma_2} x_{i_3}^{\alpha_3} \dots x_{i_m}^{\alpha_m}, \dots, x_{i_1}^{\alpha_1} \dots x_{i_{m-1}}^{\alpha_{m-1}} x_{i_m}^{\gamma_m},$$

where $\gamma_j \neq \alpha_j$, results in the y's associated with each outputted x. For example, consider $x_{i_1}^{\gamma_1} x_{i_2}^{\alpha_2} x_{i_3}^{\alpha_3} \dots x_{i_m}^{\alpha_m}$, where $\gamma_1 \neq \alpha_1$. We already know that the associated y's are

$$\begin{gathered} x_{i_1}^{\beta_1 \neq \gamma_1} x_{i_2}^{\beta_2 = \alpha_2} x_{i_3}^{\beta_3 = \alpha_3} \dots x_{i_m}^{\beta_m = \alpha_m}, \\ x_{i_1}^{\beta_1 = \alpha_1} x_{i_2}^{\beta_2 \neq \alpha_2} x_{i_3}^{\beta_3 = \alpha_3} \dots x_{i_m}^{\beta_m = \alpha_m}, \\ \dots, x_{i_1}^{\beta_1 = \alpha_1} \dots x_{i_{m-1}}^{\beta_{m-1} = \alpha_{m-1}} x_{i_m}^{\beta_m \neq \alpha_m} \end{gathered}$$

for β_δ in $1, \dots, d-1$ if $\delta = 1, \dots, m$ unless stated otherwise. We need only examine y in $\{x_{i_1}^{\beta_1 \neq \gamma_1} x_{i_2}^{\beta_2 = \alpha_2} x_{i_3}^{\beta_3 = \alpha_3} \dots x_{i_m}^{\beta_m = \alpha_m}\}_{\beta_1 = 1}^{\beta_1 = d-1}$. This set has cardinality $d - 2$ and contains a unique y_0 such that $y_0 = x_{i_1}^{\alpha_1} \dots x_{i_m}^{\alpha_m}$. In other words, there exists β_1 such that $\beta_1 = \alpha_1 \neq \gamma_1$ for some β_1 in $1, \dots, d-1$. For each fixed γ_1, we can find a copy of x_0 which we denote as y_0. Thus there are $d - 2$ copies of x_0 among the y associates if we output x in S_m such that $x = x_{i_1}^{\gamma_1} x_{i_2}^{\alpha_2} x_{i_3}^{\alpha_3} \dots x_{i_m}^{\alpha_m}$ for all $\gamma_1 = 1, \dots, d-1$, where $\gamma_1 \neq \alpha_1$.
If we output all forms of x as described above, we get $(d-2) * m$ copies of x_0. No more repetitions of x_0 can occur amongst the y associates because we have exhausted all possible forms of x with which to compute y associates. Since x_0 was arbitrary, outputting all x from S_m results in $(d-2) * m$ copies of each y in S_m.
3. $H(y) = m + 1$. Fix y_0 in S_{m+1}. Then $y_0 = y_{i_1}^{\alpha_1} y_{i_2}^{\alpha_2} \dots y_{i_{m+1}}^{\alpha_{m+1}}$ for fixed coordinate positions $\{i_\nu\}_1^{m+1}$ and fixed values $\{\alpha_\nu\}_1^{m+1}$. Partition S_m into families which are projections of y in S_{m+1}. (For example, y_0 has the projection $\mathcal{F}_{y_0} = \{y_{i_1}^{\alpha_1} y_{i_2}^{\alpha_2} \dots y_{i_m}^{\alpha_m}, y_{i_1}^{\alpha_1} y_{i_2}^{\alpha_2} \dots y_{i_{m-1}}^{\alpha_{m-1}} y_{i_{m+1}}^{\alpha_{m+1}}, \dots, y_{i_2}^{\alpha_2} y_{i_3}^{\alpha_3} \dots y_{i_{m+1}}^{\alpha_{m+1}}\}$.) Then given y in S_{m+1}, the cardinality of $\mathcal{F}_{y_0}$ is $m + 1$. It is clear that there exists a one-to-one correspondence between y in S_{m+1} and $\mathcal{F}_{y_0}$ as a subset of S_{m+1}. ☐

We use the results of Proposition 4.2 to describe the system of equations $\bar{g}(p) = (G)_{m,p} g(m)$ for $0 \leq m, p \leq k$ and

$$G \overset{def}{=} (G)_{m,p} \overset{def}{=} \begin{cases} (n-1) \cdot (k - m + 1) & \text{when } m = p - 1, \\ (n-2) \cdot m & \text{when } m = p, \\ m + 1 & \text{when } m = p + 1, \\ 0 & \text{otherwise.} \end{cases}$$

Then G is a singular, nonsymmetric tridiagonal matrix. (Note that when $r \geq 1$, G is a singular, nonsymmetric band-limited matrix with bandwidth proportional to r.)

Therefore, in order to describe the system of equations $g(m) = ((G)_{m,p})^{-1}\bar{g}(p)$, we need to set $(G)^{-1} \equiv G^{+}$, the generalized Moore–Penrose inverse of G.

PROPOSITION 4.4. *Suppose f is in $C(\mathbb{Z}_n^k)$. If $\widehat{\chi}_{S_1} \not\equiv 0$, then*

$$f(y) = \sum_{H(x,y)=0}^{k} (G^{+})_{1,H(x,y)}\overline{f}(x),$$

where

$$\overline{f}(x) = \sum_{H(x,y)=1} f(y)$$

and G^{+} is the Moore–Penrose inverse of G.

Proof. We note that from DeDeo and Velasquez [1], the inversion problem has become one of inverting singular, nonsymmetric band-limited matrices. For $r = 1$, band-limited means inverting the tridiagonal matrix G computed in Proposition 4.2. Using the definitions and results from Proposition 4.2, we have that

$$g(0) = \sum_{\beta=0}^{k}(G^{+}(s,t))_{1,\beta}g(\beta)$$

with $(G^{+}(s,t))_{\alpha,\beta} = G^{+}(s,t)$, the Moore–Penrose inverse of $G = G(s,t)$. Then, since $f(0) = g(0)$, we have that

$$f(0) = \sum_{H(x)=0}^{k} (G^{+}(s,t))_{1,H(x,y)}\overline{f}(x)$$

and, by a shift action,

$$f(y) = \sum_{H(x,y)=0}^{k} (G^{+}(s,t))_{1,H(x,y)}\overline{f}(x)\ . \qquad \square$$

REFERENCES

[1] M. R. DeDeo and E. Velasquez, *An introduction to the Radon transform on $\mathbb{Z}_2^k$*, Congr. Numer., 156 (2002), pp. 201–209.

[2] P. Diaconis and R. Graham, *The Radon transform on $\mathbb{Z}_2^k$*, Pacific J. Math., 118 (1985), pp. 323–345.

[3] C. Dunkel, *A Krawtchouk polynomial addition theorem and wreath products of symmetric groups,* Indiana Univ. Math. J., 25 (1976), pp. 335–358.

[4] J. A. Fill, *The Radon transform on $\mathbb{Z}_n$*, SIAM J. Discrete Math., 2 (1989), pp. 262–283.

[5] G. M. L. Gladwell and N. B. Williams, *A discrete Gel'fand-Levitan method for band-matrix inverse eigenvalue problems*, Inverse Problems, 5 (1989), pp. 165–279.

[6] J. MacWilliams and N. J. A. Sloane, *The Theory of Error Correcting Codes*, North Holland, Amsterdam, 1977.

[7] P. Rózsa, R. Bevilacqua, F. Romani, and P. Favati, *On band matrices and their inverses*, Linear Algebra Appl., 150 (1991), pp. 287–295.

[8] D. Stanton, *Orthogonal polynomials and Chevalley groups*, in Special Functions: Group Theoretical Aspects and Applications, R. A. Askey et al., eds., D. Reidel, Boston, MA, 1984, pp. 87–128.

[9] D. Stanton, *An introduction to group representations and orthogonal polynomials*, in Orthogonal Polynomials, P. Nevai, ed., Kluwer Academic, Norwell, MA, 1990, pp. 419–433.