PACIFIC JOURNAL OF MATHEMATICS
Vol. 118, No. 2, 1985

THE RADON TRANSFORM ON $\mathbf{Z}_2^k$

PERSI DIACONIS AND R. L. GRAHAM

In memory of Ernst Straus

Suppose G is a finite group and f is a function mapping G into the set of real numbers R. For a subset $S \subseteq G$, define the Radon transform F_S of f mapping G into R by:

$$F_S(x) = \sum_{y \in S+x} f(y)$$

where $S + x$ denotes the set $\{s + x: s \in S\}$. Thus, the Radon transform can be thought of as a way of replacing f by a "smeared out" version of f. This form of the transform represents a simplified model of the kind of averaging which occurs in certain applied settings, such as various types of tomography and recent statistical averaging techniques.

A fundamental question which arises in connection with the Radon transform is whether or not it is possible to invert it, i.e., whether one can recover (in principle) the function f from knowledge of F_S.

In this paper we investigate this problem in detail for several special classes of groups, including the group of binary n-tuples under modulo 2 addition.

1. Introduction. Let X be a finite set and let Y be a class of subsets of X. For a real-valued function $f: X \to \mathbf{R}$, the Radon transform of f at $y \in Y$ is defined as

$$\check{f}(y) = \sum_{x \in y} f(x).$$

This paper investigates uniqueness of the transform when X is the group of binary k-tuples $\mathbf{Z}_2^k$ or the symmetric group S_n, and Y is the class of translates of a given set $S \subset X$.

In §2 we deal with $\mathbf{Z}_2^k$. It is shown that the transform is one-to-one when $|S|$ is odd and is not one-to-one for most sets of even cardinality. It is also shown that the problem of determining uniqueness is NP-complete so that at present no polynomial-time algorithm (in k and $|S|$) is known to exist to determine uniqueness.

In Section 3 we give explicit inversion theorems for the case where $S = \{x \in \mathbf{Z}_2^k: H(0, x) \leq 1\}$ where $H(x, y)$ is Hamming distance—the number of coordinates where x and y disagree. The transform is one-to-one

if and only if $k = 2n$ is even. Then an inversion theorem can be given as

$$f(x) = \frac{1}{(2n+1)} \sum_y \beta_n\left(\left\lfloor \frac{H(x,y)}{2} \right\rfloor\right) \bar{f}(y),$$

where

$$\beta_n(j) = (-1)^j \frac{2 \cdot 4 \cdots 2j}{(2n-1)(2n-3)\cdots(2n-2j+1)}.$$

When k is odd, a similar result holds for the transform based on translates of $S = \{x: H(0,x) = 1\}$.

In §4, X is taken to be the symmetric group on n letters and Y is taken to be the translates of $S = \{\pi \in S_n: d(id, \pi) \leq 1\}$ where $d(\pi, \eta)$ is the Cayley metric—the minimum number of transpositions required to bring π to η. Using the representation theory of the symmetric group we show that the transform is one-to-one if and only if $n \in \{1, 3, 4, 5, 6, 8, 10, 12\}$.

The program of investigating general Radon transforms was studied by Gelfand *et al.* [**11**]. They used a transform based on averages over submanifolds as a way of writing down all of the irreducible representations of certain Lie groups. We learned of this program through work of Bolker [**2**] and Guilleman-Sternberg [**12**]. They worked with the class Y generated by a combinatorial block design. They discuss many issues not treated here. For example, they give characterizations of the range of the transform in many examples. Kung [**15**] generalizes the theory based on block designs. He shows that if X is a finite set and Y is the collection of sets of rank i in a matroid on X, then the transform is one-to-one. The examples considered in the present paper do not fall into any of the previous frameworks: the class of translates of a set does not arise from matroids.

Discrete Radon transforms of the type studied here are starting to be used in applied statistics. For example, Diaconis [**4**] considers an example of data analysis of syllable counts in the books of Plato. For each sentence in a given book (e.g. Plato's Republic) the syllable pattern in the last five syllables was recorded. This gives a binary vector in $\mathbf{Z}_2^5$ (syllables being coded long or short). A function f: $\mathbf{Z}_2^5 \to \mathbf{R}$ was defined by counting the number of sentences with each pattern. This was analyzed by taking various averages, amounting to Radon transforms for various choices of Y.

It is natural to inquire if the averages considered were rich enough to characterize f. Further discussion, and many other examples, can be found in Diaconis [**5**].

In applications, we are sometimes given the *unordered set* $\{\check{f}(y)\}$. This happens when the classical Radon transform ($X = \mathbf{R}^n$, $Y =$ affine hyperplanes) is used to inspect high-dimensional data in statistics by using a "grand tour" as in Asimov [**8**]. In an important set of papers, Straus [**20**], Selfridge and Straus [**18**], and Gordon, Fraenkel and Straus [**9**] determined conditions on $|X|$ to guarantee that the set of values $\{f(x)\}$ is determined when Y is the class of all k-element sets. For example, when $k = 2$, the set of values is determined if and only if $|X| \neq 2^j$ for some j. For any other fixed $k \neq 2$, the set of values is determined for all but a finite number of values of $|X|$.

Similar questions can be considered for the transforms considered here. We can show that if two probability measures in $\mathbf{R}^n$ have compact support and the same set of projections along affine hyperplanes, then the two measures are the same up to an affine change of variables, the result being false without the support conditions. Aside from this, and Straus' results, we know nothing.

2. Uniqueness for Radon Transforms Based on Translates in $\mathbf{Z}_2^k$. Throughout this section the underlying space X is $\mathbf{Z}_2^k$. Let $f\colon \mathbf{Z}_2^k \to \mathbf{R}$ be a function, and $S \subset \mathbf{Z}_2^k$ a non-empty subset. Define

$$\check{f}(y) = \sum_{x \in S+y} f(x).$$

This includes several familiar examples:

EXAMPLE (2.1). Let $H(x) = H(0, x)$ be the number of ones in x. If $S_r^+ = \{x \in \mathbf{Z}_2^k\colon H(x) \leq r\}$, the transform becomes the nearest neighbor transform which averages f over all points of distance less than or equal to r. If $S_r = \{x \in \mathbf{Z}_2^k\colon H(x) = r\}$ the transform averages over "shells" of radius exactly r.

The next lemma connects uniqueness of the transform to the Fourier transform on $\mathbf{Z}_2^k$. Recall that if $f\colon \mathbf{Z}_2^k \to \mathbf{R}$ is a function, $\hat{f}(x) = \sum_y (-1)^{x \cdot y} f(y)$ defines the Fourier transform with inverse

$$f(y) = \frac{1}{2^k} \sum_x (-1)^{x \cdot y} f(x).$$

LEMMA 1. *The transform $f \to \check{f}$ based on the translates of a set S is one-to-one if and only if*

$$\hat{\chi}_S(x) := \sum_{y \in S} (-1)^{x \cdot y} \neq 0 \quad \textit{for any } x \in \mathbf{Z}_2^k.$$

More generally, the dimension of the vector space of functions f such that $\bar{f} \equiv 0$ is the number of x such that $\hat{\chi}_S(x) = 0$.

Proof. For any f, the Radon transform at y can be represented as the convolution of f with the indicator function of the set S:

$$\bar{f}(y) = \sum_{x \in S} f(y - x) = f * \chi_S(y).$$

Taking Fourier transforms of both sides leads to

$$\hat{\bar{f}}(x) = \hat{f}(x)\hat{\chi}_S(x).$$

If $\hat{\chi}_S(x)$ is never zero this equation specifies $\hat{f}$ and so f.

Conversely, for every z such that $\hat{\chi}_S(z) = 0$, define

$$f_z(x) = \frac{(-1)^{x \cdot z}}{2^k}.$$

The orthogonality of characters implies

$$\hat{f}_z(x) = \begin{cases} 0 & \text{if } x \neq z, \\ 1 & \text{if } x = z. \end{cases}$$

The $\hat{f}_z$ are linearly independent functions on $\mathbf{Z}_2^k$. Since the Fourier transform is an isometry, the f_z are linearly independent. Clearly $\hat{\bar{f}}_z(y) = \hat{f}_z(y)\hat{\chi}_S(y) \equiv 0$. So the f_z are non-zero independent functions with $\bar{f}_z$ zero. It is easy to see that the f_z form a basis for the space of all functions f with $\bar{f} = 0$. □

EXAMPLE 2.2. If $|S|$ is odd then the transform $f \to \bar{f}$ is one-to-one. Indeed, $\hat{\chi}_S(y)$ cannot vanish since it is a sum of an odd number of ± 1's. This implies that the nearest neighbor transform based on $S_1^+ = \{y: H(y) \leq 1\}$ is one-to-one when k is even and that the transform based on $S_1 = \{y: H(y) = 1\}$ is one-to-one when k is odd.

It is certainly not necessary that $|S|$ be odd to have unique inversion. For example, if $k = 5$ and $S = \{x: H(x) = 2\}$, then $|S| = 10$, but it follows from Example 2.3 below that the transform based on S is one-to-one. The parity restrictions on S_1^+ and S_1 are necessary and sufficient. As an example, consider

$$\hat{\chi}_S(y) = k - 2H(y).$$

If k is even, this vanishes for all vectors with $k/2$ ones. There are $\binom{k}{k/2}$ of these so the dimension of the space of functions f such that $\bar{f} \equiv 0$ is reasonably large.

REMARKS. If $\hat{\chi}_S$ has no zeros then $\hat{\chi}_{S^c}$ has no zeros because $\hat{\chi}_{\mathbf{Z}_2^k}(y) = 0$ for all non-zero y. It is easy to show the following pale version of the Wiener Tauberian Theorem holds: if $S \subset \mathbf{Z}_2^k$ then any function can be written as a linear combination of the translates of $\hat{\chi}_S$ if and only if $\hat{\chi}_S$ is never zero.

EXAMPLE 2.3. When $S = S_r = \{x: H(x) = r\}$ we have

$$\hat{\chi}_S(x) = p_r^k(H(x))$$

where for variable v, and integers $0 \le r \le k$, $p_r^k(v)$ is the Krawtchouk polynomial (see MacWilliams and Sloane [**16**], p. 130)

$$p_r^k(v) = \sum_{l=0}^{r} (-1)^l \binom{v}{l}\binom{k-v}{r-l}.$$

We see that the Radon transform based on S_r is one-to-one if and only if the Krawtchouk polynomial $p_r^k(v)$ has no integer zero in $[0, k]$. For example:

$p_0^k(v) = 1$—the transform based on S_0 is one-to-one.

$p_1^k(v) = \{k - 2v\}$—the transform based on S_1 is one-to-one iff k is odd.

$p_2^k(v) = \frac{1}{2}\{(k - 2v)^2 - k\}$—the transform based on S_2 is one-to-one iff k is not a square.

$p_3^k(v) = \frac{1}{6}(k - 2v)\{(k - 2v)^2 - 3k + 2\}$—the transform based on S_3 is one-to-one iff k is odd and $3k - 2$ is not a square.

The recurrence for the polynomials p_r^k can be used to show that when r is odd the polynomial has a factor of the form $(k - 2v)$ and so has an integer zero whenever k is even and r is odd.

MacWilliams and Sloane ([**16**], p. 153) give the identity

$$p_0^k(v) + p_1^k(v) + \cdots + p_r^k(v) = p_r^{k-1}(v - 1).$$

It follows that the transform based on $S_r^+ = \{x \in \mathbf{Z}_2^k: H(x) \le r\}$ is one-to-one if and only if the Krawtchouk polynomial $p_r^{k-1}(v)$ has no integer zeros in $[-1, k - 1]$. We do not know of any systematic study of integer zeros of Krawtchouk polynomials.

Using classical results on integer zeros of polynomials, it is straightforward to show that for r even and at least 4, the transform based on S_r is one-to-one for all but a finite number of values of k. In particular for $r = 4$ the only values of k for which this transform is not one-to-one are those k for which the (transformed) Krawtchouk polynomial

$$z^4 - 2(3k - 4)z^2 + 3k(k - 2)$$

has an integer root z_0 with $0 \le z_0 \le k$. This can be transformed by a straightforward change of variables to the diophantine equation

$$(*) \qquad 6x^2(x^2 - 1) + 9 = y^2.$$

The values of n for which the transform based on S_4 is not invertible are then given by

$$n = x^2 + 1 + y/3.$$

The known solutions to (*) together with the corresponding values of n are listed below.

TABLE 1

Values of n for which the transform of S_4 is not invertible

x	y	n
0	3	2
0	−3	0
±1	3	3
±1	−3	1
±2	9	8
±2	−9	2
±3	21	17
±3	−21	3
±6	87	66
±6	−87	8
±91	20283	15043
±91	−20283	1521

The curve of (*) can be birationally transformed to Weierstrass normal form:

$$u^2 = 4v3 - 57v + 53.$$

This elliptic curve has at least 18 rational points (derivable from the table) and so must have rational points of infinite order. Presumably, the *only* integer points on (*) are given in Table 1 but we have not been able to show this.

The following theorem shows that for many sets S, $\hat{\chi}_S(x) = 0$ for some x, so the transform is not one-to-one.

THEOREM 1. *Let $\mathscr{S}_{2t} = \{S \subset \mathbf{Z}_2^k: |S| = 2t\}$. Then, the proportion of sets S in $\mathscr{S}_{2t}$ such that $\hat{\chi}_S(x) = 0$ for some x tends to 1 as k tends to infinity uniformly in t, for $t = o(2^{k/2})$.*

We require a preparatory lemma which gives another way to decide when $\hat{\chi}_S(x)$ is zero.

LEMMA 2. *Let* $S = \{s_i\}_{i=1,\ldots,|S|}$ *where* $s_i = (s_{i1},\ldots,s_{ik})$. *Let the columns of the matrix* (s_{ij}) *be* c_j, $1 \le j \le k$. *Then for* $x = (x_1,\ldots,x_k)$,

$$\hat{\chi}_S(x) = 0 \quad \textit{if and only if} \quad H\Big(\sum_j x_j c_j\Big) = \frac{|S|}{2}.$$

REMARKS. The proof of the lemma follows at once from the definitions. The lemma implies that instead of checking for $\hat{\chi}_S(x) = 0$, one can check if there is a word of weight $|S|/2$ in the vector space (over $\mathbf{Z}_2$) spanned by the columns of the matrix (s_{ij}).

Proof of Theorem 1. Let

$$\begin{bmatrix} s_{11} & s_{12} & \cdots & s_{1k} \\ \vdots & & & \\ s_{2t,1} & & \cdots & s_{2t,k} \end{bmatrix}$$

be a random $2t \times k$ matrix with entries s_{ij} that are independent, identically distributed (iid) with $p(s_{ij} = 1) = p(s_{ij} = 0) = 1/2$. Let $c_1, c_2,\ldots,c_k$ be the columns of the matrix. For $z \in \mathbf{Z}_2^k$ define $X_z = \sum_{\{i:z_i=1\}} c_i$ where the sum is taken coordinate-wise modulo 2. It is easy to see that the $\{X_z\}_{z\in\mathbf{Z}_2^k}$ are pairwise independent random vectors. For fixed $z \neq 0$, the coordinates of X_z are iid coin-tossing. Define

$$W_z = \begin{cases} 1 & \text{if } H(X_z) = t, \\ 0 & \text{otherwise.} \end{cases}$$

Thus, the W_z are pairwise independent and, for $z \neq 0$, the central limit theorem for coin-tossing implies that

$$P\{W_z = 1\} = \frac{\theta_1(t)}{\sqrt{t}}, \qquad \operatorname{Var}(W_z) = \frac{\theta_2(t)}{\sqrt{t}} \tag{2.1}$$

where $\theta_1(t)$, $\theta_2(t)$ tend to positive constants as t tends to infinity. Let

$$S = \sum_{z\neq 0} W_z.$$

Thus S counts the number of times a vector in the column space of (s_{ij}) has weight t. Using (2.1) and the pairwise independence yields

$$\mu := E(S) = \frac{(2^k-1)\theta_1(t)}{\sqrt{t}}, \qquad \sigma^2 := \operatorname{Var}(S) = \frac{(2^k-1)\theta_2(t)}{\sqrt{t}}. \tag{2.2}$$

Now Chebyshev's inequality gives

$$P\{(S-\mu)^2 > a\} \leq \sigma^2/a^2.$$

It follows from this and (2.2) that $P\{S > 0\}$ tends to 1 as k tends to infinity, uniformly in t when $0 \leq t < 2^k$.

To complete the argument, observe that the probability that the rows $(s_{i1},\ldots,s_{ik})$ are all distinct is

$$\prod_{i=1}^{2t-1}\left(1-\frac{i}{2^k}\right).$$

This tends to 1 for $t = o(2^{k/2})$. The theorem follows. □

As noted above, if $\hat{\chi}_S$ has a zero, $\hat{\chi}_{S^c}$ has a zero. Thus the theorem implies that most sets of cardinality $2^k - 2t$, for $0 < 2t \ll 2^{k/2}$ are not sets of uniqueness for the Radon transform.

R. Chen, A. M. Odlyzko and L. A. Shepp have recently shown that Theorem 1 can be strengthened to hold uniformly in $0 \leq 2t \leq 2^k$.

Similar theorems can be proved on other Abelian groups. For example, on $X = \mathbf{Z}_n$, with Y taken as all translates of a fixed subset S with $|S| = k$, the transform is one-to-one for most sets S as n and k tend to infinity. Peter Frankl has sharper results for general Abelian groups.

The final result of this section shows that, at present, there is no reasonable algorithm to apply to a set $S \subset \mathbf{Z}_2^k$ which decides if the Radon transform, based on translates of S, is unique. We will argue that the following problem is *NP*-complete.

Problem 1. *Input*: A subset $S \subset \mathbf{Z}_2^k$.
Property: Every function $f\colon \mathbf{Z}_2^k \to \mathbf{R}$ is determined by the Radon transform

$$f \mapsto \bar{f}(y) = \sum_{x \in S} f(x+y).$$

The result implies that any polynomial-time algorithm (in k and $|S|$) for Problem 1 could be used to provide polynomial-time algorithms for solving literally thousands of problems that have also been shown to be *NP*-complete. For background on *NP*-completeness see Garey and Johnson (1978).

We will find it convenient to use the language of coding theory. A *code* is a vector space over $\mathbf{Z}_2$. Vectors in a code are called *codewords*. The *weight* of a codeword, $W(v)$, is the number of ones in v. If M is a binary matrix, $\langle M\rangle$ denotes the code generated by the rows of M. The *length* of $V \in \langle M\rangle$ is the number of columns of M.

With this notation, Lemma 1 provides a second problem clearly equivalent to Problem 1:

Problem 2. *Input*: A binary matrix T with distinct columns.
Property: The vector space T over $\mathbf{Z}_2$ generated by the rows of T contains a vector V with weight $(V) = \frac{1}{2}$ length (V).

The following problem has been shown to be *NP*-complete by Berlekamp, McEliece, and Van Tilborg [**1**]:

Problem 3. *Input*: A binary matrix A and a nonnegative integer t.
Property: There is a binary vector x with weight t such that $xA = 0$.

If C is a code, the *dual code* to C is the set of all binary vectors orthogonal to every codeword in C where the dot product modulo 2 is used. Problem 3 says that the dual code to the code generated by the columns of A contains a codeword of weight t. Given a matrix M whose columns are used to generate a code, it is easy to construct a matrix M' whose rows generate the dual code using the Gram-Schmidt algorithm. The size of M' is polynomially bounded by the size of M'. Thus, the following problem in *NP*-complete.

Problem 4. *Input*: A binary matrix B and a nonnegative integer t.
Property: The code generated by the rows of B contains a codeword of weight t.

In what follows, we will show that Problems 2 and 4 are polynomially equivalent. The differences between the problems are that Problem 4 has a free variable t in its input while in Problem 2 the matrix has distinct columns. The following proof is due to Rob Calderbank and Peter Shor.

THEOREM 2. *Problems* 2 *and* 4 *are polynomially equivalent.*

Proof. Clearly any algorithm that solves Problem 4 can be used to solve Problem 2 after computing the number of columns of the input matrix T.

Conversely, we will now construct a matrix T, given B and t, such that the dimensions of T are polynomially bounded by the dimensions of B, T has distinct rows, and such that the algorithm for Problem 2 applied to T provides an answer to Problem 4.

The construction uses two special codes:

(2.3) $\mathscr{C}$—a 2-weight code—has length $n = 2^{2r-1} - 2^{r-1}$, with 2^{r-1} codewords. It has the property that the only weights that occur are 0,

$$w_1 = 2^{2r-2} - 2^{r-1} = \frac{n}{2} - 2^{r-2} \quad \text{and}$$

$$w_2 = 2^{2r-2} = \frac{n}{2} + 2^{r-2}.$$

Calderbank and Kantor [3] discuss this code. It follows from this work that $\mathscr{C}$ exists for any $r \geq 2$. Further, $\mathscr{C}$ can be generated by the rows of an $r - 1$ by n matrix C with distinct columns.

(2.4) $\mathscr{S}$—the simplex code—has length 2^r. It is generated by an $r \times 2^r$ matrix S having as columns the distinct binary r-tuples (arranged in lexicographically increasing order). It has the property that each nonzero codeword has weight 2^{r-1}. The simplex code is discussed in MacWilliams and Sloane (1977). For example, when $r = 3$, the generator matrix is

$$\begin{array}{ccccccc} 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 0 & 1 \end{array}$$

Note that if t columns of $\mathscr{S}$ are removed to form a matrix S', then each nonzero codeword of the code generated by the rows of S' has weight contained in $[2^{r-1} - t, 2^{r-1}]$.

Now, suppose we are given a matrix B with rows of length b and a nonnegative integer $t \leq b$. We may assume that none of the rows of B are all zero. We first argue that without loss of generality we may assume

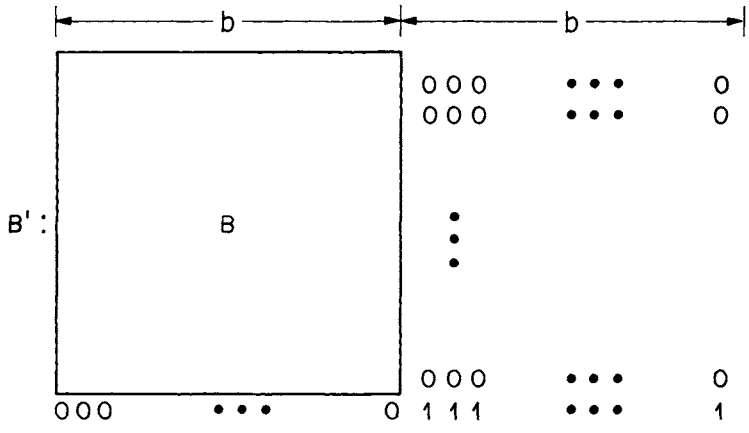

FIGURE 1

$t \leq b/2$. If $t > b/2$, construct a new matrix B' from B as shown in Fig. 1. Thus B' has $b' = 2b$ columns and one more row than B. Furthermore, $\langle B' \rangle$ has a codeword of weight t if and only if $\langle B \rangle$ has a codeword of weight t, since any sum of rows containing the last row of B' has weight $> b \geq t$. Hence, by passing to a new matrix if necessary, we may assume $t \leq b/2$.

Next, form a matrix D by adjoining at most $m = [(\log b)/(\log 2)]$ rows to the top of B so as to make all the columns of D distinct. The matrix $\hat{B}$ we put on top of B has the form

$$\hat{B} = \begin{bmatrix} \overbrace{0 & 0 & 0 & 0 & \cdots}^{b} \\ 0 & 0 & 0 & 0 & \cdots \\ \cdot & \cdot & \cdot & \cdot & \cdots \\ 0 & 0 & 1 & 1 & \cdots \\ 0 & 1 & 0 & 1 & \cdots \end{bmatrix} \Big\} m$$

Let r be determined by $b < 2^{r-2} \leq 2b$. From (2.3), $n = 2^{2r-1} - 2^{r-1}$. Set $\varepsilon = b - 2t$. Notice that

$$\frac{b - \varepsilon}{2} < 2^{r-2}. \tag{2.5}$$

Form the matrix T as shown in Figure 2.

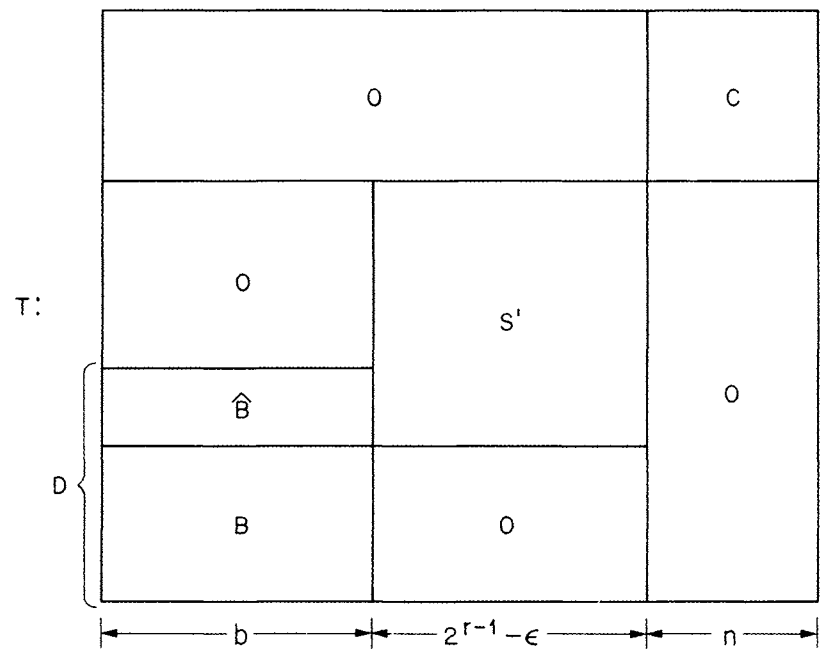

FIGURE 2

It will now be shown that T has a codeword of weight half its length if and only if B has a codeword of length t. Let v be a codeword in T. The weight of v is

$$W(v) = W_D(v) + W_{S'}(v) + W_C(v)$$

where $W_D(v)$ denotes the weight of the portion of v formed from the first b rows arising from D, etc.

The possible values of these subweights are:

$$0 \le W_D(v) \le b, \tag{2.6}$$

$$W_{S'}(v) = 0 \quad \text{or} \quad 2^{r-2} - \varepsilon \le W_{S'}(v) \le 2^{r-2},$$

$$W_C(v) = 0 \quad \text{or} \quad W_C(v) = \frac{n}{2} \pm 2^{r-2}.$$

The length of E is $n + 2^{r-1} - \varepsilon + b$.

If

$$W(v) = \frac{1}{2} \cdot \text{length}(v) = \frac{n}{2} + 2^{r-2} + \frac{b - \varepsilon}{2},$$

then we cannot have $W_C(v) \le n/2 - 2^{r-2}$. For then,

$$W(v) \le b + 2^{r-2} + \frac{n}{2} - 2^{r-2} < \frac{n}{2} + 2^{r-2} + \frac{b - \varepsilon}{2}.$$

Therefore it must be that $W_C(v) = n/2 + 2^{r-2}$. But this together with (2.6) and the definitions imply that $W_{S'}(v) = 0$. Thus, none of the rows of S' can be used to form v, and only rows intersecting B are involved. Therefore, $W(v) = \frac{1}{2} \cdot \text{length}(v)$ implies

$$W_D(v) = W_B(v) = \frac{b - \varepsilon}{2} = t.$$

Conversely, if there is $v \in \langle B \rangle$ of weight t then certainly $\langle T \rangle$ contains a codeword of weight

$$\frac{n}{2} + 2^{r-2} + \frac{b - \varepsilon}{2} = \frac{n}{2} + 2^{r-2} + t. \qquad \square$$

REMARK. Theorems 1 and 2 combine to leave us in the following interesting situation. On the one hand, most sets S of even order are not sets of uniqueness. On the other hand, there is at present no effective way to decide uniqueness.

3. Inversion Formulas for Nearest Neighbor Transforms on $\mathbf{Z}_2^k$. When the Radon transform $f \mapsto \bar{f}$ is one-to-one, there is still the question of developing an explicit inversion formula. In this section, inversion formulas are given for the transform based on balls and shells of radius 1.

THEOREM 3. *Given* $f\colon \mathbf{Z}_2^{2m+1} \to \mathbf{R}$, *let*

$$\bar{f}(x) = \sum_{y:\, H(x,y)=1} f(y).$$

Then

$$f(y) = \frac{1}{2m+1} \sum_{x:\, H(x,y) \text{ is odd}} \beta_m\left(\frac{H(x,y)-1}{2}\right)\bar{f}(x).$$

where

$$\beta_m(k) = \frac{(-1)^k 2 \cdot 4 \cdots 2k}{(2m-1)\cdots(2m-2k+1)}.$$

THEOREM 4. *Given* $f\colon \mathbf{Z}_2^{2m} \to \mathbf{R}$, *let*

$$\bar{f}(x) = \sum_{y:\, H(x,y)\le 1} f(y).$$

Then

$$f(y) = \frac{1}{2m+1} \sum_x \beta_m\left(\left\lfloor \frac{H(x,y)}{2} \right\rfloor\right)\bar{f}(x).$$

Proof of Theorem 3. For $0 \le k \le 2m+1$, define

$$g(k) := \sum_{H(x)=k} f(x), \qquad \bar{g}(k) := \sum_{H(x)=k} \bar{f}(x). \tag{3.1}$$

By counting how often each $f(x)$ occurs when computing $\bar{g}(k)$ we have the relation

$$\bar{g}(k) = (k+1)g(k+1) + (2m-k+2)g(k-1) \qquad \text{for } 0 \le k \le 2m+1 \tag{3.2}$$

where by definition $g(-1) = g(2m+2) = 0$.

Note also that

$$g(0) = f(0).$$

We will derive an expression for $f(0)$ in terms of $\bar{f}(x)$. The corresponding expression for $f(x)$ follows after shifting everything by x. We proceed by solving the linear system (3.2) for $g(0)$. A matrix for (3.2) appears as shown in Fig. 3. Thus, for example,

$$\bar{g}(2m+1) = 0 \cdot g(2m+1) + 1 \cdot g(2m) + 0 \cdot g(2m-1),$$
$$\bar{g}(2m) = (2m+1)g(2m+1) + 2g(2m-1), \quad \text{etc.}$$

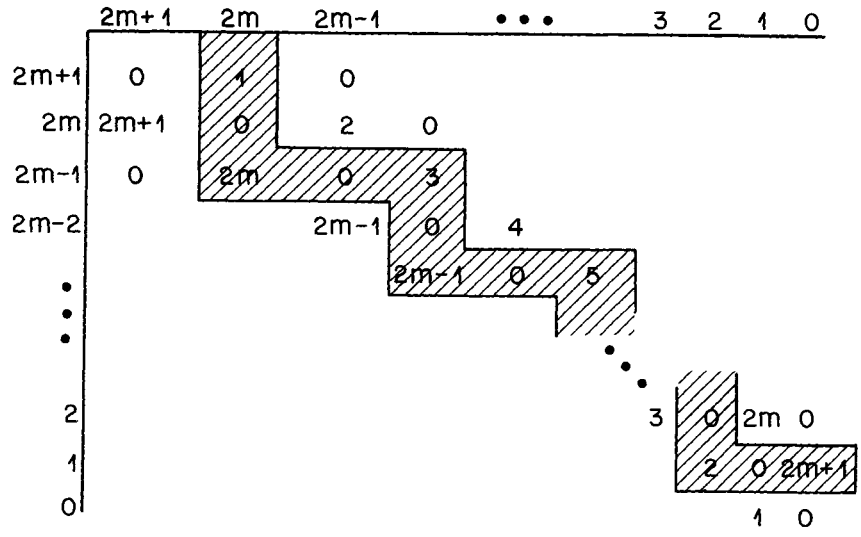

FIGURE 3

The system can be inverted by following the shaded path as follows:

$$\bar{g}(2m+1) = g(2m) \quad \text{so } g(2m) = \bar{g}(2m+1)$$

$$\bar{g}(2m-1) = 2mg(2m) + 3g(2m-2)$$

$$\text{so } g(2m-2) = \frac{1}{3}\bar{g}(2m-1) - \frac{2m}{3}\bar{g}(2m+1).$$

Continuing in this way, we obtain

$$\begin{aligned} g(0) &= \frac{1}{2m+1}\bar{g}(1) - \frac{2}{(2m-1)(2m+1)}\bar{g}(3) \\ &\quad + \frac{2\cdot 4}{(2m-3)(2m-1)(2m+1)}\bar{g}(5) \\ &\quad + \cdots + (-1)^m \frac{2\cdot 4\cdot 6\cdots 2m}{1\cdot 3\cdot 5\cdots(2m+1)}\bar{g}(2m+1) \\ &= \frac{1}{(2m+1)}\sum_{k=0}^{m} \beta_m(k)\bar{g}(2k+1) \end{aligned}$$

where

$$\beta_m(k) = \frac{(-1)^k 2\cdot 4\cdots 2k}{(2m-2k+1)(2m-2k+3)\cdots(2m-1)}.$$

Finally, recalling the definition of $\bar{g}$ in terms of $\bar{f}$,

$$f(0) = g(0) = \frac{1}{2m+1}\sum_{H(x)\text{odd}} \beta_m\left(\frac{H(x)-1}{2}\right)\bar{f}(x). \qquad \square$$

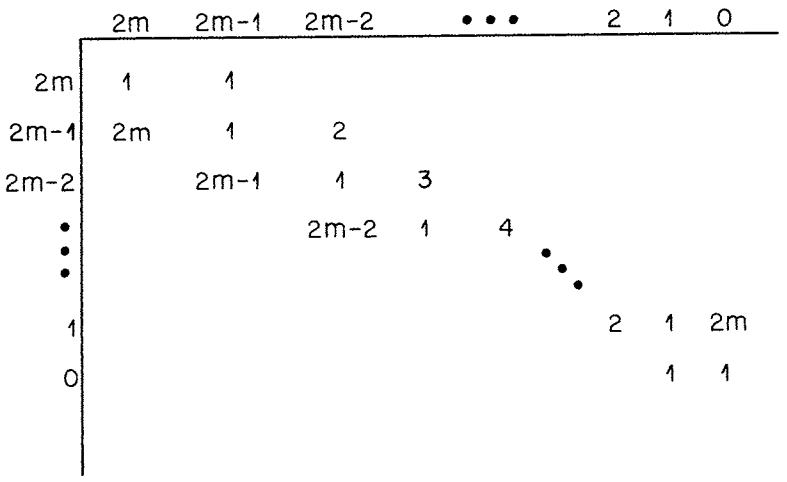

FIGURE 4

Proof of Theorem 4. For $0 \leq k \leq 2m$, define $g(k)$ and $\bar{g}(k)$ by (3.1). These functions satisfy

$$\bar{g}(k) = (k+1)g(k+1) + g(k) + (2m-k+1)g(k-1) \quad \text{for } 0 \leq k \leq 2m \tag{3.3}$$

where by definition $g(-1) = g(2m+1) = 0$.

Again $f(0) = g(0)$, and we need only solve for $g(0)$, since the general case follows by shifting. The matrix for (3.3) appears as shown in Fig. 4. Now, when solving for g in terms of $\bar{g}$, all the terms contribute, rather than only those of odd weight as in Theorem 3. The result is

$$g(0) = \frac{1}{2m+1}\left\{\bar{g}(0) + \bar{g}(1) - \frac{2}{2m-1}\bar{g}(2) - \frac{2}{2m-1}\bar{g}(3) + \frac{2\cdot 4}{(2m-3)(2m-1)}\bar{g}(4) + \frac{2\cdot 4}{(2m-3)(2m-1)}\bar{g}(5) + \cdots\right\}. \qquad \square$$

REMARKS. It is instructive to compare the formula of Theorems 3 or 4 to the result of direct use of the Fourier inversion theorem. Arguing as in §2,

$$\bar{f}(x) = f * k(x) \text{ with } k(x) = \begin{cases} 1 & \text{if } H(x) = 1, \\ 0 & \text{otherwise.} \end{cases}$$

Fourier transforming, and using $\hat{k}(y) = (2m + 1 - 2H(y))$ leads to

$$\hat{f}(y) = \hat{\bar{f}}(y)/(2m+1-2H(y)).$$

Now the Fourier inversion theorem gives

$$f(x) = \frac{1}{2^{2m+1}} \sum_y (-1)^{x \cdot y} \hat{f}(y) \tag{3.4}$$

$$= \frac{1}{2^{2m+1}} \sum_z \bar{f}(z) \sum_y \frac{(-1)^{(x+z)y}}{(2m+1-2H(y))}.$$

Equating coefficients with the formula in Theorem 3 gives an identity for inverse sums of the Krawtchouk polynomials $p_1^{2m+1}(v) = (2m+1-2v)$:

$$\frac{1}{2^{2m+1}} \sum_y \frac{(-1)^{z \cdot y}}{2m+1-2H(y)} \tag{3.5}$$

$$= \begin{cases} 0 & \text{if } H(z) \text{ is even,} \\ \dfrac{1}{2m+1} \beta_m\left(\dfrac{H(z)-1}{2}\right) & \text{if } H(z) \text{ is odd.} \end{cases}$$

Of course, the coefficients of $\bar{f}(z)$ on the right side of (3.4) provide an explicit inversion, but the forms presented in Theorems 3 and 4 are easier to think about. As an example, let us investigate the stability of the inversion: To compute $f(0)$, values of $\bar{f}(y)$ are needed for all vectors y, not just vectors y which are close to zero. Examining the coefficients $\beta_m(k)$ one sees that the largest weight in the inversion is on points furthest away, the next largest weight on points distance one away, the relative size of the weights continue alternating back and forth to the center.

We should point out here that J. A. Morrison [17] has recently given a very thorough discussion of the problem of inverting f: $\mathbf{Z}_2^n \to \mathbf{R}$ for the general case that

$$\bar{f}(x) = \sum_{k=0}^{n} \alpha_k \sum_{y:\, H(x,y)=k} f(y),$$

for arbitrary constants α_k. He derives explicit inversion formulas for $\bar{f}$ by first expanding the corresponding linear combination of Krawtchouk polynomials (which occur in the Fourier inversion formula) by partial fractions and then applying ingenious analytical techniques.

For example, for the case $n \neq t^2$ and

$$\bar{f}(x) = \sum_{y:\, H(x,y)=2} f(y)$$

it can be shown that the inversion formula (for $f(0)$) can be written in the form

$$f(0) = \sum_{k=0}^{m} c_k \bar{g}(k)$$

where

$$\bar{g}(k) = \sum_{H(x)=k} \bar{f}(x)$$

and

$$c_{2r+1} = 0,$$

$$c_{2r} = \frac{2(-1)^{n+r+1}}{\sqrt{n}\,\sin(\sqrt{n}\pi)} \int_0^{\pi} \cos(\sqrt{n}\,x)\cos^{n-2r}x \sin^{2r}x\,dx.$$

4. Other Groups. Versions of the Radon transform can be introduced in other groups or homogeneous spaces. Indeed, this was Gelfand's original motivation for studying generalizations of the classical transform. In this section we show how the relations between Radon transforms and Fourier analysis carry over to non-commutative groups. We carry out the analysis carefully for the nearest neighbor transform on the symmetric group with the Cayley distance as a metric. This defines the distance between two permutations as

$$d(\pi_1, \pi_2) := \text{the minimum number of transpositions required to bring } \pi_1 \text{ to } \pi_2.$$

This metric is discussed in Knuth ([**14**], p. 134), Diaconis and Graham [**6**] and Diaconis ([**5**], §8). It is shown that the Cayley distance is bi-invariant $d(\pi_1\eta, \pi_2\eta) = d(\eta\pi_1, \eta\pi_2) = d(\pi_1, \pi_2)$. The distance is easy to compute because of a relation discovered by Cayley: $d(\pi_1, \pi_2) = n$ − number of cycles in $\pi_1\pi_2^{-1}$. Our analysis will show that the nearest neighbor transform based on the Cayley distance is only one-to-one for certain small values of n.

Let G be a finite group. Let $d(g_1, g_2)$ be a bi-invariant metric on G. The nearest neighbor transform takes a function $f\colon G \to \mathbf{R}$ into

$$\bar{f}(t) = \sum_{s:\, d(s,t)\le 1} f(s).$$

Similarly, one can define transforms based on averaging over larger balls or shells. If $S_1^+ = \{(s\colon d(id, s) \le 1)\}$ then clearly

$$\bar{f}(t) = \sum_{s \in S_1^+ \cdot t} f(s) = \sum_{s \in t \cdot S_1^+} f(s).$$

A wide variety of bi-invariant metrics is described in Section 8 of Diaconis [**5**].

The first lemma relates uniqueness of nearest neighbor transforms to the representation theory of G. A convenient reference for the elementary facts of group representations is Serre [**19**].

LEMMA 3. *Let G be a finite group. Let S be a subset of G. For $f\colon G \to \mathbf{R}$ define*

$$\bar{f}(t) = \sum_{s \in S \cdot t} f(s).$$

The transform $f \to \bar{f}$ is one-to-one if and only if for every irreducible representation ρ of G, the matrix

$$\hat{\chi}_{S^{-1}}(\rho) := \sum_{s \in S} \rho(s^{-1})$$

is invertible.

Proof. If χ_S is the indicator function of the set S, then

$$\begin{aligned} (4.1)\quad \bar{f}(t) &= \sum_{r \in S} f(rt) = \sum_{r \in G} \chi_S(r) f(rt) \\ &= \sum_r \chi_{S^{-1}}(r^{-1}) f(rt) = \sum_r \chi_{S^{-1}}(tr^{-1}) f(r) = \chi_{S^{-1}} * f(t). \end{aligned}$$

Thus,

$$(4.2)\qquad \hat{\bar{f}}(\rho) = \hat{\chi}_{S^{-1}}(\rho) \hat{f}(\rho)$$

so that if $\hat{\chi}_{S^{-1}}(\rho)$ is invertible then f can be determined from (4.2), the known transform of $\bar{f}$, and the Fourier inversion formula (Theorem 7.2 of Serre [**19**]).

Conversely, if for some ρ_0, $\hat{\chi}_{S^{-1}}(\rho_0)$ is non-invertible then there is a nonzero vector v_0 such that $\hat{\chi}_{S^{-1}}(\rho_0) v_0 = 0$. Define a function $\tilde{f}$ through its Fourier transform at irreducible representations as $\hat{\tilde{f}}(\rho) = 0$ if $\rho \neq \rho_0$, and $\hat{\tilde{f}}(\rho_0)$ is the projection along the direction of v_0. With this choice $\hat{\chi}_{S^{-1}}(\rho) \hat{\tilde{f}}(\rho) = 0$ for all irreducible representations. Thus, the associated function f is a non-zero function with $\bar{f} \equiv 0$. □

The next lemma records a key fact that allows analysis of nearest neighbor transforms based on bi-invariant metrics: the Fourier transform of $\chi_{S^{-1}}$ is a computable constant times the identity. This lemma is also at the heart of Diaconis and Shahshahani [7]. For a proof, see Theorem 7 of Serre [**19**].

LEMMA 4. *If $f\colon G \to \mathbf{R}$ is constant on conjugacy classes, so that $f(sts^{-1}) = f(t)$, then for any irreducible representation ρ of dimension d with character χ,*

$$\hat{f}(\rho) = cI \quad \text{where } c = \frac{1}{d} \sum f(g) \chi_\rho(g).$$

COROLLARY 1. *Let* $S_1 = \{\pi \in S_n\colon\ d(id, \pi) = 1\}$, $S_1^+ = \{\pi \in S_n\colon\ d(id, \pi) \leq 1\}$ *where d is the Cayley metric. Then*

$$S_1^{-1} = S_1, \qquad (S_1^+)^{-1} = S_1^+$$

and

$$\hat{\chi}_{S_1^+}(\rho) = \left(1 + \binom{n}{2} r(\rho)\right) I = (\hat{\chi}_{S_1} + 1) I$$

with

$$r(\rho) = \frac{\chi_\rho(\tau)}{d_\rho}$$

where $\chi_\rho(\tau)$ *is the character of the irreducible representation* ρ *at the transposition* τ *and* d_ρ *is the dimension of the irreducible representation.*

Proof. Because the Cayley metric is bi-invariant, both χ_{S_1} and $\chi_{S_1^+}$ are constant on conjugacy classes. The result now follows from Lemma 3. □

COROLLARY 2. *The nearest neighbor transform based on* S_1 *is not one-to-one for any* $n \geq 3$.

Proof. The irreducible representations of the symmetric group are indexed by partitions of n. Partitions are often represented by their Young diagrams; thus 3, 2, 1, 1 is represented by the diagram shown in Fig. 5. The conjugate partition is defined by forming the transpose of the diagram. Theorem 6.6 of James [**13**] implies that if λ_1 and λ_2 are conjugate partitions and τ is any transposition, then

$$\chi_{\lambda_1}(\tau) = -\chi_{\lambda_2}(\tau).$$

If $\lambda_1 = \lambda_2$ then both characters are zero. Since self-conjugate partitions exist for all $n \geq 3$, the assertion follows. □

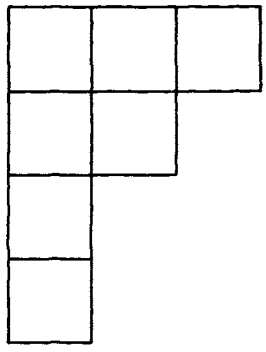

FIGURE 5

Analysis for S_1^+ is more complex. We show:

THEOREM 5. *The nearest neighbor transform*

$$f \mapsto \bar{f}(\pi) = \sum_{d(\pi,\eta)\le 1} f(\eta),$$

with d the Cayley metric on the symmetric group on n letters is one-to-one if and only if $n \in \{1, 3, 4, 5, 6, 8, 10, 12\}$.

Proof. In what follows, the characters and dimensions of irreducible representations corresponding to the partition λ: $\lambda_1 \ge \lambda_2 \ge \cdots \ge \lambda_m \ge 1$, $\Sigma\lambda_k = n$, will be denoted $\chi_\lambda(\tau)$ and d_λ. According to Corollary 1 we *cannot* invert the transform based on S_1^+ if and only if

$$\frac{\binom{n}{2}\chi_\lambda(\tau)}{d_\lambda} = -1. \tag{4.3}$$

Frobenius derived an explicit formula for this expression, as discussed in Lemma 5 of Diaconis and Shahshahani [**6**]. This yields that (4.3) is equivalent to the existence of a partition satisfying

$$\frac{1}{2}\sum_{j=1}^{m}\{(\lambda_j - j)(\lambda_j - j + 1) - j(j-1)\} = -1$$

i.e.,

$$\sum_{j=1}^{m}\left\{\binom{\lambda_j - j + 1}{2} - \binom{j}{2}\right\} = -1.$$

Make the change of variables: $\mu_j = \lambda_j - j + 1$. Thus, if there are m integers μ_i satisfying

$$\mu_1 > \mu_2 > \cdots > \mu_m \ge 2 - m$$

and

$$\sum_{j=1}^{m}\binom{\mu_j}{2} = \sum_{j=1}^{m}\binom{j}{2} - 1 = \binom{m+1}{3} - 1$$

then the value

$$n = \mu_1 + \cdots + \mu_m + \sum_{j=1}^{m}(j-1) = \mu_1 + \cdots + \mu_m + \binom{m}{2}$$

does not have a one-to-one nearest neighbor transform. We break the analysis into two cases.

Case I. *n odd*. Consider the choice for $m \geq 3$,

$$\mu_1 = m, \quad \mu_2 = 1, \quad \mu_3 = 0, \quad \mu_t = 2 - t, \qquad 4 \leq t \leq m.$$

Then

$$\binom{\mu_1}{2} = \binom{m}{2}, \quad \binom{\mu_2}{2} = 0, \quad \binom{\mu_3}{2} = 0, \quad \mu_t = \binom{t-1}{2}, \qquad 4 \leq t \leq m.$$

Thus

$$\sum_{j=1}^{m} \binom{\mu_j}{2} = \sum_{j=3}^{m} \binom{j}{2} = \binom{m+1}{3} - 1$$

and

$$n = \sum_{j=1}^{m} \mu_j + \binom{m}{2} = m + 2 - \binom{m-1}{2} + \binom{m}{2} = 2m + 1.$$

Therefore, all values $n = 2m + 1$, $m \geq 3$, are eliminated.

Case II. *n even*. Consider the choice for $m \geq 7$,

$$\mu_1 = m, \quad \mu_2 = 4, \quad \mu_3 = 3, \quad \mu_4 = -1, \quad \mu_5 = -2, \quad \mu_6 = -3$$

and

$$\mu_t = 2 - t, \quad 7 \leq t \leq m.$$

Then

$$\binom{\mu_1}{2} = \binom{m}{2}, \quad \binom{\mu_2}{2} = 6, \quad \binom{\mu_3}{2} = 3, \quad \binom{\mu_4}{2} = 1,$$

$$\binom{\mu_5}{2} = 3, \quad \binom{\mu_6}{2} = 6$$

and

$$\binom{\mu_t}{2} = \binom{t-1}{2}, \qquad 7 \leq t \leq m.$$

Thus

$$\sum_{j=1}^{m} \binom{\mu_j}{2} = \binom{m+1}{3} - 1$$

and

$$n = \sum_{j=1}^{m} \mu_j + \binom{m}{2} = m + 11 - \binom{m-1}{2} + \binom{m}{2} = 2m + 10.$$

Therefore, all values $n = 2m + 10$, $m \geq 7$, are eliminated. Furthermore the choices shown below eliminate further values of n:

$(4,1,0,-2)$	eliminates $n = 14$
$(5,3,1,0,-3)$	eliminates $n = 16$
$(5,4,1,0,-2)$	eliminates $n = 18$
$(7,3,1,-1,-2,-3)$	eliminates $n = 20$
$(6,3,2,1,0)$	eliminates $n = 22$

Also, note that $\bar{\mu} = (1,0)$ eliminates $n = 2$.

Character tables show that indeed, for the remaining values $n = 1$, 3, 4, 5, 6, 8, 10, 12, we can invert. (For $n \leq 10$ the tables in James and Kerber [**13a**] were used; for $n = 12$, the table in M. Zia-ud-Din [**21**] was used.) □

Consider the weighted transform

$$\tilde{f}(\pi) = sf(\pi) + \sum_{\eta:\, d(\eta,\pi)=1} f(x).$$

Corollary 1 dealt with $s = 0$ and Theorem 5 dealt with $s = 1$. A similar but somewhat more complicated argument can be given which shows that we cannot invert for any fixed integer s once $n \geq \frac{1}{2}s^3 + O(s)$.

Acknowledgements. We wish to thank Ethan Bolker, Rob Calderbank, Jim Fill, Jeff Lagarias, Andew Odlyzko, Mehrdad Shahshahani, Larry Shepp, Peter Shor, John Stembridge and Shlomo Sternberg for useful discussions of the problems here.

References

[1] E. Berlekamp, R. McEliece, and Van Tilborg, *On the inherent intractability of certain coding problems*, IEEE Trans. Information Theory, **24** (1978).

[2] E. Bolker, *The finite Radon transform*, Proc. of the AMS Summer Conference on Integral Geometry (Bowden, Aug. 84) to appear.

[3] A. R. Calderbank and W. M. Kantor, *The geometry of two-weight codes*, (1983), to appear, Proc. London Math. Soc.

[4] P. Diaconis, *Projection Pursuit for Discrete Data*, Technical Report No. 148, (1983), Stanford University, Department of Statistics.

[5] _____, *The use of group representations in probability and statistics*, (1985), Institute of Mathematical Statistics.

[6] P. Diaconis and R. L. Graham, *Spearman's footrule as a measure of disarray*, J. Roy. Statist. Soc. B, **39** (1977), 262–268.

[7] P. Diaconis and M. Shahshahani, *Generating a random permutation by random transpositions*, Z. Wahrscheinlichkeitstheorie Verw. Gebiete, **67** (1981), 159–179.

[8] D. Asimov, *The grand tour*, SIAM J. Scientific and Statistical Comp., (1985).
[9] A. S. Fraenkel, B. Gordon and E. J. Straus, *On the determination of sets by sets of sums of a certain order*, Pacific J. Math., **12** (1962), 187–196.
[10] M. Garey and D. J. Johnson, *Computers and Intractability: A Guide to the Theory of NP-Completeness*, (1978), Freeman, San Francisco.
[11] I. M. Gelfand, M. I. Graev and N. Ya. Vilenkin, *Generalized Functions*, Vol. 5, (1966), Academic Press, New York.
[12] V. Guilleman and S. C. Sternberg, *Notes on the Radon transform*, (1979), unpublished manuscript.
[13] G. D. James, *The Representation Theory of the Symmetric Groups*, Springer-Verlag Lecture Notes in Mathematics 682, (1978), Springer-Verlag, Berlin.
[13a] G. D. James and A. Kerber, *The Representation Theory of the Symmetric Groups*, (1981), Addison-Wesley, Reading, Mass.
[14] D. Knuth, *The Art of Computer Programming*, Vol. 3, (1973), Addison-Wesley, Reading, MA.
[15] J. Kung, *The Radon transform of a combinatorial geometry I*, J. Combinatorial Theory Series A, (1974), 97–102.
[16] J. MacWilliams and N. J. A. Sloane, *The Theory of Error Correctin Codes*, (1977), North Holland, Amsterdam.
[17] J. A. Morrison, *Weighted averages of Radon transforms on* $\mathbf{Z}_2^k$, (to appear).
[18] J. L. Selfridge and E. G. Straus, *On the determination of numbers by their sums of a fixed order*, Pacific J. Math., **8** (1958), 847–856.
[19] J.-P. Serre, *Linear Representations of Finite Groups*, (1977), Springer-Verlag, New York.
[20] E. G. Straus, *Real analytic functions as ratios of absolutely monotonic functions*, in *Spline Functions and Approximation Theory*, (1973), Birkhauser, Basel.
[21] M. Zia-ud-Din, *The Character tables of the symmetric group of degrees* 12 *and* 13, Proc. London Math. Soc., Ser. 2, **42** (1936), 340–355.

Received September 24, 1984.

STANFORD UNIVERSITY
STANFORD, CA 94305

AND

AT & T BELL LABORATORIES
MURRAY HILL, NJ 07974