JOURNAL OF COMBINATORIAL THEORY, Series A 44, 168-171 (1987)

Note

The Radon Transform on Abelian Groups

P. FRANKL

CNRS, Paris, France

AND

R. L. GRAHAM

AT&T Bell Laboratories, Murray Hill, New Jersey 07974

Communicated by Managing Editors

Received July 15, 1986

The Radon transform on a group A is a linear operator on the space of functions $f: A \to \mathbb{C}$. It is shown that if $A = \mathbb{Z}_p^n$ then the Radon transform with respect to a subset $B \subset A$ is not invertible if and only if B has the same number of elements in every coset of some maximal subgroup of A. The same does not hold in general for arbitrary finite abelian groups.

INTRODUCTION

Let A be a finite group and $B \subset A$, a subset. For every function $f: A \to \mathbb{C}$ one defines the function $F_B: A \to \mathbb{C}$, the *Radon transform of f with respect to B* by

$$F_B(a) = \sum_{b \in B} f(ab). \tag{1}$$

The principal problem we address here is: for which subsets B is the Radon transform invertible, i.e., knowledge of the function F_B determines f uniquely. Such sets are called *unique inversion* sets. Unique inversion sets were investigated in Diaconis and Graham [1], where particular attention is given to the case $A = \mathbb{Z}_2^n$.

The main result of this note gives a combinatorial description of unique inversion sets in $\mathbb{Z}_p^N$ when p is a prime.

Let us say that B is *uniformly distributed* modulo the subgroup $A_0 < A$ if $|B \cap aA_0|$ is the same for all $a \in A$. Note that this implies $|A : A_0|$ divides $|B|$.

0097-3165/87 $3.00

THEOREM 1.1. *A subset $B \subset A = \mathbb{Z}_p^n$ is not a unique inversion set if and only if B is uniformly distributed modulo some maximal subgroup $A_0 < A$.*

Remark. Most subsets B of $\mathbb{Z}_p^n$ have size close to $p^n/2$. Since $\mathbb{Z}_p^n$ has $(p^n-1)/(p-1)$ maximal subgroups, for such B, the problem whether B is a unique inversion set can be decided in time polynomial in $|B|$. On the other hand, in [1] it is shown that the existence of a polynomial time algorithm for general $B \subset \mathbb{Z}_2^n$ implies $P = NP$.

Proof of Theorem 1.1. One can look at (1) as a system of $|A|$ linear equations in the $|A|$ unknowns $\{f(a): a \in A\}$. Therefore B is a unique inversion set if and only if the coefficient matrix $M(B)$ of (1) is nonsingular.

If A is abelian and $K(A)$ denotes the character matrix of A, then it is easy to check that the Hermitian matrix $K(A)/\sqrt{|A|}$ can be used to bring $M(B)$ into diagonal form, i.e., the matrix $K(A)M(B)K(A)^*/|A|$ is diagonal. This leads to the following.

PROPOSITION 2.1 (Frobenius, cf. [2]). *Let $\{\psi_d : d \in A\}$ be the set of irreducible characters of the abelian group A. Then the eigenvalues of $M(B)$ are the numbers $\psi_d(B) = \sum_{b \in B} \psi_d(b)$.*

Let us now use this formula to prove Theorem 1.1. Suppose that $B \subset \mathbb{Z}_p^n$ is not a unique inversion set. Then there exists an element $d \in A$ so that $\sum_{b \in B} \psi_d(b) = 0$. Since the statement is trivially true for $B = \emptyset$, we may assume that B is non-empty. Consequently, $d \neq 1$ and thus $A_0 = \{a \in A : \psi_d(a) = 0\}$ is a maximal subgroup. For $0 < j < p$, let us define $A_j = \{a \in A : \psi_d(a) = e^{2\pi i j/p}\}$. Then $A = A_0 \cup A_1 \cup \cdots \cup A_{p-1}$ is the decomposition of A into cosets of A_0.

Setting $b_j = |B \cap A_j|$ for $0 \leqslant j < p$, and $x = e^{2\pi i/p}$ we obtain

$$0 = \psi_d(B) = \sum_{j=0}^{p-1} b_j x^j.$$

Therefore the minimal polynomial $1 + x + \cdots + x^{p-1}$ of $e^{2\pi i/p}$ must divide $b(x) = \sum_{j=0}^{p-1} b_j x^j$. Since $\deg b(x) \leqslant p-1$, $b(x) = c(1 + x + \cdots + x^{p-1})$ follows for some constant c. This proves $b_0 = b_1 = \cdots = b_{p-1} = c$, as desired.

The second implication of the theorem holds even for general groups. Let $A_0, A_1, \ldots, A_{m-1}$ be the left cosets of A_0 in A in some order and suppose that for some b, $|B \cap A_j| = b$ holds for $0 \leqslant j < m$. Consider the function $f(a)$ defined by

$$f(a) = \begin{cases} 1 & a \in A_0, \\ -1 & a \in A_1, \\ 0 & \text{otherwise.} \end{cases}$$

It is easily checked that $F_B(a) = \sum_{ab \in A_0, b \in B} 1 - \sum_{ab \in A_1, b \in B} 1 = b - B = 0$, i.e., $F_B(a)$ is identically zero. ∎

Let us now investigate in more detail the case of general (abelian) groups. The simplest example of a nonunique inversion set is probably an arbitrary subgroup. Indeed, if $B < A$ then the Radon transform F_B is constant on each left coset of B. Thus the space of the functions F_B has dimension at most $n/|B|$.

The same also holds if B is the disjoint union of right cosets of B.

PROPOSITION 2.2. *Suppose that $D_1, ..., D_r$ are subgroups of A satisfying $\sum_{i=1}^{r} 1/|D_i| < 1$ and B is the disjoint union of some right cosets of $D_1, ..., D_r$. Then B is not a unique inversion set.*

Proof. Let B_i be the subset of B which is the union of the right cosets of D_i. Let V_i denote the vector space of functions F_{B_i}. As we showed before $\dim V_i \leqslant n/|D_i|$. Consequently $V_1, V_2, ..., V_r$ generate a subspace, say W, of dimension less than n. Since F_B is contained in W, the statement follows. ∎

Remark. If $r \geqslant 2$, then the preceding conclusion holds even if $\sum_{i=1}^{r} 1/|D_i| = 1$, since the constant function is contained in each of the V_i. Thus, the simplest group for which Theorem 1.1 fails is $\mathbb{Z}_{p^2}$, taking as B the cyclic subgroup of order p in it.

For abelian groups one can actually compute $\dim V_i$ as follows.

PROPOSITION 2.3. *Suppose that B is a coset of a subgroup D of the abelian group A. Then the dimension of the vector space of the functions $F_B(a)$ is $n/|D|$.*

Proof. In view of Proposition 2.1 the dimension in question is simply the number of characters ψ_d with $\psi_d(B) \neq 0$. Now $|\psi_d(B)| = |B| \neq 0$ if $D \leqslant \operatorname{Ker} \psi_d$, i.e., for all $n/|D|$ characters of A/D. Otherwise $\psi = \psi_{d|D}$ is a non-trivial irreducible character of D, and consequently $(\psi, 1_D) = 0$, which implies $\psi_d(B) = 0$.

Using Proposition 2.2 we can get examples of groups of square-free order for which Theorem 1.1 fails. For example, in $\mathbb{Z}_{30}$ the group of integers $(\text{mod } 30)$ take $B = \{0, 1, 11, 15, 21\} = \{0, 15\} \cup \{1, 11, 21\}$. Then the corresponding Radon transform has only dimension 20.

However, by the Chinese remainder theorem, this approach cannot work for cyclic groups of order pq, p and q being distinct primes. Nevertheless, if A is slightly larger, e.g., if A has a non-trivial subgroup A_0 with $A/A_0 \cong \mathbb{Z}_{pq}$ then we do not have to worry about disjointness. Suppose that $B \subset A$ is such that the elements of B considered modulo A_0 form the union of one coset of $\mathbb{Z}_p$ and one of $\mathbb{Z}_q$. In particular, $|B| = p + q$. Then B is not a unique inversion set in view of Proposition 2.2, and in most cases it is not uniformly distributed modulo any maximal subgroup of A (a simple sufficient condition is $(p+q, |A|)=1$). In this way we can show that Theorem 1.1 fails for all abelian groups except $\mathbb{Z}_p^n$ and $\mathbb{Z}_{pq}$.

PROBLEM 2.4. Does Theorem 1.1 hold for $A=\mathbb{Z}_{pq}$? One can easily check that the answer is "yes" for $\mathbb{Z}_{pq}$. In general, a positive answer to the problem is equivalent to a negative one to the following.

PROBLEM 2.5. Let $\phi(x)$ be the pqth cyclotomic polynomial, i.e., $\phi(x)=(x-1)(x^{pq}-1)/(x^p-1)(x^q-1)$. Is there a polynomial $g(x)=\sum_{i=0}^{pq-1} \varepsilon_i x^i$ with $\varepsilon_i=0, 1$ so that $\phi(x)$ divides $g(x)$ but neither $x^{p-1}+\cdots+x+1$ nor $x^{q-1}+\cdots+x+1$ divides $g(x)$.

Note added in proof. Peter Cameron has just shown that Theorem 1.1 does indeed hold for $A=\mathbb{Z}_{pq}$.

REFERENCES

1. P. DIACONIS AND R. L. GRAHAM, The Radon transform on $\mathbb{Z}_2^k$, *Pacific J. Math.* **118** (1985), 323–345.
2. T. HAWKINS, *Arch. Hist. Exact Sci.* **7** (1970/71), 142–170; **8** (1971/72), 243–287; **12** (1974), 217–243.

Printed in Belgium