ILLINOIS JOURNAL OF MATHEMATICS
Volume 28, Number 3, Fall 1984

A CONVOLUTION THEOREM FOR PROBABILITY MEASURES ON FINITE GROUPS

BY

DAVID L. RITTER

1. Introduction

Central among phenomena studied by harmonic analysts is the smoothing caused by convolution. One manifestation of this on the circle group T is the existence of positive Borel measures μ that, for every finite $p > 1$, convolve $L^p(T)$ into $L^q(T)$ with $q > p$ dependent on μ and p. Such measures may be considered to be L^p-improving.

A remarkable example, the classical Cantor–Lebesgue measure supported by the usual middle-third Cantor set, was shown by Oberlin in [6] to be L^p-improving. To obtain that result, by using the Riesz–Thorin convexity theorem and by making a reduction based on a careful analysis of the structure of the natural discrete measures used to define the Cantor–Lebesgue measure as a limit, Oberlin revealed that it suffices to prove there is a $p < 2$ such that

$$(\#) \qquad \|\mu^* x\|_2 \leq \|x\|_p$$

for every $x \in L^p(G)$, where $G = \mathbf{Z}/3\mathbf{Z} = \{0, 1, 2\}$ is the cyclic group of integers modulo 3, the L^q-norms are those taken with respect to normalized counting measure on G, and μ is the probability measure that places a mass of 1/2 at 0 and at 2. Finally, to complete the proof, he obtained a quantitative version of $(\#)$ that, subsequently, was sharpened by W. Beckner.

Here, in the context of arbitrary finite groups, we characterize the probability measures that satisfy $(\#)$ for some $p < 2$. In addition, we show that the p appearing in $(\#)$ is well behaved with respect to compactness in the space of probability measures.

We now make that precise. Let G be a finite group with K elements, and for $p > 1$, let $L^p(G)$ be the usual Lebesgue space on G with norm $\|\cdot\|_p$ defined in terms of the Haar measure on G that assigns mass $1/K$ to each point of G. We denote the set of probability measures on G by $P(G)$ and supply $P(G)$ with the topology obtained from the total variation norm on $M(G)$, the measure algebra on G. For $\mu \in P(G)$, let $G(\mu)$ denote the subgroup of G generated by the set $\{i^{-1}j: i, j \in \text{supp}(\mu)\}$, where supp (μ) denotes the support of μ. Our main result is the theorem that follows.

Received March 8, 1982.

THEOREM 1. (a) *If $\mu \in P(G)$, where G is a finite group, then there is a $p < 2$, dependent on μ, such that*

$$\|\mu^* x\|_2 \leq \|x\|_p \tag{1}$$

for every $x \in L^p(G)$ if, and only if,

$$G(\mu) = G. \tag{2}$$

(b) *In addition, if C is a compact subset of $P(G)$ with every μ in C satisfying* (2), *then there is a $p < 2$, dependent on C, such that* (1) *is true for every $\mu \in C$ and every $x \in L^p(G)$.*

We shall prove Theorem 1 in the next section after stating and proving two essential lemmas. The last section will be devoted to some results related to Theorem 1.

2. Proof of the main theorem

In this section we do some multivariable calculus. For notation, then, we turn to [4, pp. 56–157]. In addition, unless otherwise indicated, sums will be over the group G, where we shall assume $K \geq 2$ to avoid a trivial case. Finally, we shall identify real-valued functions on G, the only type we treat in this section, with elements of R^K.

Now set

$$\begin{aligned} g(\mu, x) &= \|\mu^* x\|_2^2 - \|x\|_2^2 \\ &= K^{-1}\left[\sum_i \left[\sum_j \alpha_{ij^{-1}} x_j\right]^2 - \sum_i x_i^2\right] \end{aligned}$$

for $\mu = \sum \alpha_j \delta_j$ in $P(G)$ and x in R^K. The keystone on which the proof of Theorem 1 rests is the following simple lemma concerning $g(\mu, x)$.

LEMMA 2.1. *Let $G(\mu)$ be the subgroup of G generated by*

$$D(\mu) = \{i^{-1}j \colon i, j \in \operatorname{supp}(\mu)\}.$$

Then $g(\mu, x)$ is a negative semi-definite quadratic form that vanishes precisely on the set

$$Z(\mu) = \{x \in R^K \colon x \text{ is constant on right cosets of } G(\mu)\}.$$

Proof of Lemma 2.1. That $g(\mu, x)$ is negative semi-definite is equivalent to the inequality $\|\mu^* x\|_2 \leq \|x\|_2$ being true for $x \in R^K$, and thus, is an immediate consequence of Theorem 20.12 of [5].

We next show that the set on which $g(\mu, x)$ vanishes is just $Z(\mu)$. Avoiding the trivial case where μ is a point mass δ_j, we suppose that the support of μ contains at least two points.

Now an elementary calculus argument shows that the set of points in R^K where g vanishes concides with the solution set of the system of linear equations

$$\sum_i \left[\sum_j \alpha_{ij_0^{-1}} \alpha_{ij^{-1}} x \right] - x_{j_0} = 0, \quad j_0 \in G.$$

This homogeneous system may be rewritten in a much more revealing form, namely, as

$$\sum_j c_{j_0 j^{-1}} x_j = 0, \quad j_0 \in G, \tag{3}$$

where, if e denotes the identity of G, then

$$c_e = 1 - \sum_i \alpha_i^2 \quad \text{and} \quad c_j = -\sum_i \alpha_{ij} \alpha_i \text{ for } j \neq e.$$

Evidently the solution set of (3) is the null space of the convolution operator $S(x) = v^* x$, where $v = \sum_j c_j \delta_j$. Therefore it should come as no surprise that, to complete the proof, we require the special properties of the measure v that we now enumerate:

(i) $\sum c_j = 0$; (ii) $c_e > 0$; (iii) if $j \neq e$ and $c_j \neq 0$, then $c_j < 0$; and (iv) $\operatorname{supp}(v) = D(\mu)$.

When combined with (i) and (iv), an elementary computation reveals that if $x \in R^K$ is constant on right cosets of $G(\mu)$, then x is in the null space of S. The real problem is in verifying the truth of the converse.

Before we prove that, we recall some necessary group theoretic notation. First, if A and B are subsets of G, then $AB = \{ab: a \in A \text{ and } b \in B\}$. Therefore, if $n \geq 1$, then we may define A^{n+1} recursively by $A^{n+1} = AA^n$. Consequently,

$$G(\mu) = \cup \{D(\mu)^n : n \geq 1\}.$$

Now let x be an element of the null space of S. By making a preliminary adjustment by a function constant on right cosets of $G(\mu)$, we may suppose that x is non-negative and that x vanishes at least once on each right coset. Thus, we shall be finished once we show x vanishes identically.

To do that, choose a system of representatives for the right cosets of $G(\mu)$ from the zeros of x, and suppose j_0 is such a representative. To finish, we shall use a simple induction argument to show that x vanishes on $D(\mu)^n j_0$ for each $n \geq 1$, and hence, on $G(\mu) j_0$.

That x vanishes on $D(\mu) j_0$ is obvious from (iii) and the equation

$$0 = v^* x(j_0) = \sum_{j \in D(\mu)} c_{j^{-1}} x_{j j_0}$$

since $x \geq 0$ and $x_{j_0} = 0$. Consequently, we have a basis for induction.

To make the induction step, we show that if x vanishes on $D(\mu)^n j_0$, then x vanishes on $D(\mu)^{n+1} j_0$. To do that, it suffices to see that if j_1 is any element of

$D(\mu)^n j_0$, then x vanishes on $D(\mu) j_1$. That, however, follows by making the same argument as that of the preceding paragraph with j_1 replacing j_0. Thus, we have completed the induction argument and the proof of the lemma. //

Now suppose $\mu = \sum a_j \delta_j$ is a probability measure on G. In Theorem 1, the inequality with which we must contend is

$$\left[K^{-1} \sum_i \left[\sum_j \alpha_{ij-1} x_j\right]^2\right]^{1/2} \leq \left[K^{-1} \sum_j x_j^p\right]^{1/p}, \tag{4}$$

where x is any non-negative function on G. Of course to study (4), we resort to the usual tactic of defining a suitable function and studying its behavior.

To begin, set

$$\Delta = \{x \in R^K \backslash \{0\} : x_j \geq 0 \text{ for each } j \in G\}.$$

Then define f on $P(G) \times \Delta \times [1, 2]$ by

$$f(\mu, x, p) = \left[\sum_i \left[\sum_j a_{ij-1} x_j\right]^2\right]^{1/2} \Big/ \left[\sum_j x_j^p\right]^{1/p},$$

where $\mu = \sum \alpha_j \delta_j$.

Evidently inequality (4) is equivalent to

$$f(\mu, x, p) \leq K^{1/2 - 1/p} \tag{5}$$

holding for $x \in \Delta$;

it will be in this form that we shall treat (4) in proving (b) of Theorem 1.

Now to prove Theorem 1, we require one more lemma, a lemma that concerns the behavior of f near $x_0 = (1/K, \ldots, 1/K)$.

LEMMA 2.2 *Let C be a compact subset of $P(G)$ with every μ in C satisfying (2), and let $\sigma = \{x \in R^K : x_j \geq 0$ for every j, and $\sum x_j = 1\}$ be the simplex in R^K spanned by the canonical basis. Then there is a $p_1 < 2$, dependent on C, and there is an open neighborhood U about x_0, such that (5) holds when $(\mu, x, p) \in C \times [U \cap \sigma] \times [p_1, 2]$.*

Proof of Lemma 2.2. Instead of considering f as a function defined on

$$P(G) \times \Delta \times [1, 2],$$

we now think of f as a family of functions defined on Δ and indexed in a continuous way by $P(G) \times [1, 2]$. Evidently every member of the family is C^∞ on the interior of Δ. Consequently, we shall obtain the proof of the lemma by studying the second degree Taylor expansion of the family.

First, it is easy to see that the ray $\{(t, \ldots, t) : t > 0\}$ is a set of critical points for each member of the family. Set $x_0 = (1/K, \ldots, 1/K)$. Then, since

$f(\mu, x_0, p) = K^{1/2-1/p}$, there is a closed ball B centered at the origin of R^K so that $x_0 + B$ is contained in the interior of Δ, and so that

$$(6) \qquad f(\mu, x_0 + h, p) - K^{1/2-1/p} = q(\mu, h, p) + R_2(\mu, h, p)$$

for $h \in B$ and $(\mu, p) \in P(G) \times [1, 2]$, where

$$\begin{aligned} q(\mu, h, p) &= (1/2)D_h^2 f(\mu, x_0, p) \\ &= (1/2)(h_1 D_1 + \cdots + h_K D_K)^2 f(\mu, x_0, p), \end{aligned}$$

and

$$R_2(\mu, h, p) = (1/6)D_h^3 f(\mu, x_0 + \tau(\mu, h, p) \cdot h, p)$$

with $\tau(\mu, h, p) \in (0, 1)$.

A routine computation reveals that $q(\mu, h, 2) = (K/2)g(\mu, h)$. Thus, by Lemma 2.1, $q(\mu, h, 2)$ is negative semi-definite and vanishes only on the line $L = \{t, \ldots, t): t \in R\}$ whenever μ is in C.

Conveniently enough, the orthogonal complement of L with respect to the usual inner product on R^K is $T_{x_0} = \{x \in R^K: \sum x_j = 0\}$, the tangent space of σ at x_0. This means that $q(\mu, h, 2)$ is bounded away from zero for $\mu \in C$ and $h \in S_{x_0} = T_{x_0} \cap S^{K-1}$, where $S^{K-1} = \{x \in R^K: |x| = 1\}$ is the unit sphere in R^K defined by the usual quadratic norm. From continuity, then, there is an $m < 0$ and a compact neighborhood of 2 in $[1, 2]$, say $[p_1, 2]$, such that

$$(7) \qquad q(\mu, h, p) \leq m$$

for $(\mu, h, p) \in C \times S_{x_0} \times [p_1, 2]$.

Finally, the third order partials are bounded for

$$(\mu, x, p) \in P(G) \times [x_0 + B] \times [1, 2].$$

Thus, the limit,

$$\lim_{h \to 0} R_2(\mu, h, p)/|h|^2 = 0,$$

is uniform with respect to $\mu \in P(G)$ and $p \in [1, 2]$. Hence, there is an open ball U, centered at x_0, such that if $x_0 + h \in U$, then

$$(8) \qquad |R_2(\mu, h, p)|/|h|^2 < -m/2$$

for each $\mu \in P(G)$ and each $p \in [1, 2]$. That is the last step, for when $x_0 + h \in U \cap \sigma$, we have $h \in T_{x_0}$. Thus, Lemma 2.2 follows from (6), (7), and (8). //

With all the tools in hand, we now get down to the business of proving Theorem 1.

Proof of the necessity of $G(\mu) = G$ *in Theorem* 1 (a). We prove the contrapositive. Suppose $G(\mu) \neq G$, and let K_0 be the number of elements in the space of right cosets of $G(\mu)$, $G/G(\mu)$. Then, for non-negative x in $Z(\mu)$, (4) assumes the form

$$\left[K_0^{-1}\sum_{j\in G/G(\mu)} x_j^2\right]^{1/2} \leq \left[K_0^{-1}\sum_{j\in G/G(\mu)} x_j^p\right]^{1/p},$$

and since $K_0 \geq 2$, there is a single non-negative x in $Z(\mu)$ such that this inequality fails for every $p < 2$. That completes the proof of necessity. //

To prove the sufficiency of the condition $G(\mu) = G$ in (a) of Theorem 1, it evidently suffices to establish (b). That is our last task.

Proof of Theorem 1 (b). First, f is continuous, and for fixed μ and p, $f(\mu, \cdot, p)$ is homogeneous of degree zero, that is, purely directional. For our set of directions, then, we shall use the simplex σ of Lemma 2.2.

Thus, set

$$M = \max\{f(\mu, x, 2)\colon \mu \in C,\, x \in \sigma\backslash U\},$$

where U is the open neighborhood about $x_0 = (1/K, \ldots, 1/K)$ given by Lemma 2.2.

We claim $M < 1$. To see this, note that if $\mu \in C$, then $G(\mu) = G$. It follows from Lemma 2.1, then, that $f(\mu, \cdot, 2)$ assumes its maximum, 1, only on the ray $\{(x, \ldots, x)\colon x > 0\}$. Thus, $f(\mu, x, 2) < 1$ for $x \in \sigma\backslash U$, and the claim is true.

An immediate consequence of the inequality $M < 1$ is that there is a $p_2 < 2$ such that

$$M \leq K^{1/2-1/p} \leq 1 \tag{9}$$

for $p \in [p_2, 2]$. That is just what we need in order to make the local result, Lemma 2.2, yield the global one, the theorem.

Set $p_0 = \max(p_1, p_2)$. Then $p_0 < 2$, and, in fact, (5) holds for all (μ, x, p) in $C \times \Delta \times [p_0, 2]$. To see this, it suffices to observe that (5) holds when (μ, x, p) is in $C \times \sigma \times [p_0, 2]$. Now, on the one hand, if $x \in U \cap \sigma$, then (5) follows from Lemma 2.2. If, on the other hand, $x \in \sigma\backslash U$, then we have $f(\mu, x, p) \leq f(\mu, x, 2) \leq M$, for, fixed μ and x, $f(\mu, x, \cdot)$ is either constant or strictly increasing. This time (5) follows from (9). That, however, completes the proof of (b), and thus the proof of the theorem. //

3. Related results

We first point out that the Riesz–Thorin convexity theorem implies a more general version of Theorem 1, where we initially take $p > 1$ and then replace 2 by q with $q > p$. We leave the precise statement of this variant of Theorem 1 and its proof to the reader. Consequently, we now direct our attention to the form Theorem 1 can be made to assume when G is abelian, for then we have the use of the Fourier transform.

Let G be a finite abelian group, let Γ be its dual, and let 0 denote the identity of Γ. We take as the Haar measure on Γ ordinary counting measure. This means we have the Plancherel theorem at our disposal, and thus we may write

$$g(\mu, x) = \sum_{\gamma \in \Gamma} (|\hat{\mu}(\gamma)|^2 - 1)|\hat{x}(\gamma)|^2,$$

where $\hat{x}$ and $\hat{\mu}$ are the transforms of x and μ, respectively. When g is written in this form, the set of functions where it vanishes is particularly transparent. Consequently, Theorem 1 may be formulated in terms of the Fourier transform as follows.

THEOREM 2. (a) *If $\mu \in P(G)$, where G is a finite abelian group with dual group Γ, then there is a $p < 2$, dependent on μ, such that* (1) *holds for every $x \in L^p(G)$ if, and only if, $|\hat{\mu}(\gamma)| \neq 1$ for $\gamma \in \Gamma \backslash \{0\}$.*

(b) *For $1 > \delta > 0$, there is a $p < 2$, dependent on δ, such that* (1) *holds for each x in $L^p(G)$ and each μ in $P(G)$ with $|\hat{\mu}(\gamma)| \leq \delta$ for $\gamma \in \Gamma \backslash \{0\}$.*

The results of Theorem 1 and Theorem 2 may be construed as a qualitative answer to an analog for finite groups of the problem raised by Stein in [8] of characterizing positive measures that convolve L^p into L^q with $q > p$. A quantitative answer here would evidently shed some light on Stein's problem, but even in the context of finite cyclic groups, to obtain quantitative results appears to be difficult. A few special cases are known. For instance, when $G = \mathbf{Z}/2\mathbf{Z} = \{0, 1\}$, precise results are known; see [3], [1], and [9]. The general problem for $\mathbf{Z}/k\mathbf{Z}$ appears to be unsolved, however. Finally, to give an idea of how Theorem 1 itself applies to Stein's problem, we note that it may be used to show that the Cantor–Lebesgue measures on the circle constructed on Cantor sets built with constant rational ratio of dissection are L^p-improving [7].

Remark. Using quite different methods from ours, W. Beckner, S. Janson, and D. Jerison have independently obtained a variant of Theorem 1 valid for finite abelian groups [2]. By private communication, D. Jerison has pointed out to us that the general interpolation theorem that is the key to the proof of the variant in [2] actually yields our Theorem 1.

REFERENCES

1. W. BECKNER, *Inequalities in Fourier Analysis*, Ann of Math., vol. 102 (1975), pp. 159–182.
2. W. BECKNER, S. JANSON AND D. JERISON, *Convolution inequalities on the circle* (preprint).
3. A. BONAMI, *Etude des coefficients de Fourier des fonctions de $L^p(G)$*, Ann. Inst. Fourier (Grenoble), vol. 20 (1970), fasc. 2, pp. 335–402.
4. C. H. EDWARDS, *Advanced calculus of several variables*, Academic Press, New York, 1973.
5. E. HEWITT AND K. A. ROSS, *Abstract harmonic analysis*, volumes I and II, Springer-Verlag, New York, 1963 and 1970.

6. D. OBERLIN, *A convolution property of the Cantor–Lebesgue measure* (preprint).
7. D. L. RITTER, *Some singular measures on the circle which improve L^p-spaces*, Ph.D. Dissertation, Louisiana State University, 1981.
8. E. M. STEIN, "Harmonic analysis on R^n" in *Studies in harmonic analysis*, MAA Studies in Math., vol. 13, Mathematical Association of America, Washington, D.C., 1976.
9. F. B. WEISSLER, *Two-point inequalities, the Hermite semigroup, and the Gauss–Weierstrass semigroup*, J. Functional Analysis, vol. 32 (1970), pp. 102–121.

FLORIDA INTERNATIONAL UNIVERSITY
MIAMI, FLORIDA