THE SIDON CONSTANT OF A FINITE ABELIAN GROUP

COLIN C. GRAHAM

ABSTRACT. It is shown that the Helson constant of a finite abelian group, G, is exactly \((\text{Card } G)^{1/2}\).

The purpose of this note is to prove the following theorem.

THEOREM. Let \(G\) be a finite abelian group of cardinality \(n\). Then there exists a nonzero measure \(\mu\) on \(G\) such that \(\|\mu\|/\|\hat{\mu}\|_\infty = n^{1/2}\).

The Sidon (or Helson) constant \(\alpha(E)\) of a finite set \(E\) of a locally compact abelian group is the supremum of the ratio \(\|\mu\|/\|\hat{\mu}\|_\infty\) as \(\mu\) ranges over nonzero measures concentrated on \(E\). The Sidon constant for \(E\) is at most \((\text{Card } E)^{1/2}\) (see [K, p. 34]). Thus, the theorem establishes the claim of the abstract.

This result is a qualitative improvement of previous results. For example, [LR, pp. 78-80] shows that the Sidon constant of a finite abelian group is at least \((\text{Card } G/2e \log \text{Card } G)^{1/2}\). For a finite cyclic group, Shapiro-Rudin polynomials can be used to show that the Sidon constant of \(G\) is at least \(2^{-3/2}(\text{Card } G)^{1/2}\) [K, p. 35]. Neither of these results can be improved by modification of the techniques used to obtain them.

PROOF OF THEOREM. It will be sufficient to prove the theorem in case that \(G\) is a finite cyclic group. Indeed, if the theorem holds for finite cyclic groups, and \(G\) is a finite product of cyclic groups, then the product of the measures "that work" for the factors of \(G\) has the required property.

We now exhibit the measure that has the required property in case that \(G\) is a finite cyclic group of order \(n\). We identify \(G\) with the integers \(1, 2, \ldots, n\) with addition modulo \(n\).

If \(n\) is even, we let \(\mu\) be the measure on \(G\) that has mass \(j\) given by

\[
\mu(j) = \exp(2\pi i j^2/2n), \quad \text{for } 1 < j < n.
\]

Obviously \(\|\mu\| = n\). We need to show that \(\|\hat{\mu}\|_\infty = n^{1/2}\). Since \(\|(\mu \ast \hat{\mu})\|_\infty = \|\hat{\mu}\|_\infty\), it will suffice to show that \(\mu \ast \mu = n\delta\) where \(\delta\) is the point mass at the identity. We calculate. The following formulae are easily established. (Recall that addition is mod \(n\).)
\(\mu(-j) = \mu(n-j) = \mu(j)\).

(3) \(\tilde{\mu}(j) = \exp(-2\pi i j^2/2n)\).

We then have, for \(1 < k < n\),

\[
\mu \ast \tilde{\mu}(k) = \sum_{j=1}^{n} \mu(k - j) \tilde{\mu}(j) = \sum_{j=1}^{n} \exp(2\pi i [(k - j)^2 - j^2]/2n) = \exp(2\pi i k^2/2n) \sum_{j=1}^{n} \exp(2\pi i (-kj/n)).
\]

Of course, when \(1 < k < n\), the last sum is zero. Thus, \(\mu \ast \mu = n\delta\).

For odd \(n\), we use \(\mu(j) = \exp(2\pi i j^2/n)\). Then \(\tilde{\mu}(j) = \exp(-2\pi i j^2/n)\) and

\[
\mu \ast \tilde{\mu}(k) = \exp(2\pi i k^2/n) \sum_{j=1}^{n} \exp(2\pi i 2kj/n).
\]

Since, for odd \(n\), \(2k \equiv 0 \pmod{n}\) if and only if \(k \equiv 0 \pmod{n}\), the last sum is zero when \(1 < k < n\). Thus, \(\mu \ast \tilde{\mu} = n\delta\).

**Remark.** The corresponding problem for arithmetic progressions is much more difficult. It is not known if \(\lim a(\{1, 2, \ldots, n\})/n^{1/2} = 1\). See [N] for a discussion.

**References**


Department of Mathematics, Northwestern University, Evanston, Illinois 60201