

SIDON SETS WITH EXTREMAL SIDON CONSTANTS

COLIN C. GRAHAM AND L. THOMAS RAMSEY¹

ABSTRACT. A finitely supported measure μ on an l.c.a. group is said to be extremal if $\|\hat{\mu}\|_{\infty} = \|\mu\|^{1/2} = (\# \text{supp } \mu)^{1/2}$. If μ is an extremal measure and E is the support of μ , it follows that the Sidon constant of E is $(\# E)^{1/2}$, in which case E is also said to be extremal. Our results are these. (1) An "independent" union of m cosets of a finite subgroup H of G is extremal if and only if (essentially) m divides $\# H$. (2) Not all extremal subsets of abelian groups have the form described in (1). (3) For any group (abelian or not), the Sidon constant of that group is at least $(.8)(\# G)^{1/13}$.

1. Introduction. We use the notations, notions, results, and prerequisites of [GM]. For finite sets E we use $\#(E)$ for the cardinality of E . If G is an l.c.a. group and μ is a finitely-supported measure on G , we say μ is *extremal* if $\|\hat{\mu}\|_{\infty} = \|\mu\|^{1/2} = \#(\text{supp } \mu)^{1/2}$. Note that if E is the support of an extremal measure μ , then the Sidon constant of E is $(\# E)^{1/2}$. In that case we also say that E is extremal. If G is a finite abelian group, then the Sidon constant, $\alpha(G)$, is $(\# G)^{1/2}$; that is, G is extremal [GM, p. 336]. In this paper we provide an answer to the question of whether $\alpha(E) = \#(E)^{1/2}$ characterizes cosets of finite groups. That question is asked in [GM, p. 405]. The answer is "no", as we show by a general result (Theorem 2.1) and by several special examples (§3). The examples suggest that identification of all extremal sets may be difficult. In §4 we show by elementary means that the Sidon constant of any group (abelian or not) is at least $(.8)(\# G)^{1/13}$.

We conclude this first section with a lemma. It is well known but we are unable to provide a reference for it.

1.1. LEMMA. *Let μ be an extremal measure. Then (i) $|\hat{\mu}|$ is a constant and (ii) $|\mu(\{x\})| = 1$ for all x in the support of μ .*

PROOF OF 1.1. Since μ is a discrete measure on a finite set E , we may assume that G is discrete and G^{\wedge} is compact. We may then write

$$\begin{aligned} \|\hat{\mu}\|_{\infty}(\# E)^{1/2} &= \|\mu\| = \sum |\mu(\{x\})| \\ &< \left\{ \sum |\mu(\{x\})|^2 \right\}^{1/2} (\# E)^{1/2} = \left(\int_{G^{\wedge}} |\hat{\mu}|^2 \right)^{1/2} (\# E)^{1/2}. \end{aligned}$$

Received by the editors February 27, 1981.

1980 *Mathematics Subject Classification.* Primary 43A25, 43A46; Secondary 42A05, 43A70.

¹Partially supported by N.S.F. Contract MCS-7801875.

© 1981 American Mathematical Society
0002-9939/81/0000-0518/\$02.25

Thus $\|\hat{\mu}\|_\infty \leq \|\hat{\mu}\|_2$. Therefore $|\hat{\mu}|$ is constantly $\|\hat{\mu}\|_\infty$. The above chain of inequalities also gives

$$\sum |\mu\{x\}| = \left(\sum |\mu(\{x\})|^2 \right)^{1/2} (\#E)^{1/2} = \#E.$$

Thus $|\mu\{x\}| = \chi_E(x)$ for each $x \in G$. That gives (ii).

2. The independent unions of cosets. Our main result is this.

2.1. THEOREM. *Let G be a finite subgroup of the discrete abelian group H . Let $m > 1$ and $x_1, \dots, x_m \in H$ be such that $\sum_1^m n_j x_j \in G$ if and only if $n_1 x_1 = \dots = n_m x_m = 0$. Then the following hold.*

- (i) *If m divides $\#G$, then $\{x_1, \dots, x_m\} + G$ is extremal.*
- (ii) *If m is even, $m/2$ divides $\#G$ and all the x_j have order two, then $\{x_1, \dots, x_m\} + G$ is extremal.*
- (iii) *If not all x_j have order two and $\{x_1, \dots, x_m\} + G$ is extremal, then m divides $\#G$.*

PROOF. (i) Suppose that m divides $\#G$. Let G_1 be a subgroup of G of order m . Let μ be a measure on G such that

$$(2.1) \quad \mu * m_{G_1} = \mu, \quad \|\mu\| = \#G \quad \text{and} \quad \|\hat{\mu}\|_\infty = (m \cdot \#G)^{1/2}.$$

Such a measure can be constructed as follows. Let ω be a measure on G/G_1 such that $\|\omega\| = \#G/m$ and $\|\hat{\omega}\|_\infty = (\#G/m)^{1/2}$ [GM, p. 336]. Then, for $y \in G$, let $\mu(\{y\}) = \omega(y + G_1)$. Verification of (2.1) is a routine matter.

Using μ we now define ν on $\{x_1, \dots, x_m\} + G$ as follows.

Let $\gamma_1, \dots, \gamma_m$ be distinct representatives of the cosets of G_1^\perp in G^* . For $g \in G$, we specify

$$(2.2) \quad \nu(\{x_j + g\}) = \langle \gamma_j, g \rangle \mu(\{g\}).$$

Let ν_j be the restriction of ν to $x_j + G$. For every $\gamma \in H^*$, there is a unique j such that $|\hat{\nu}(\gamma)| = |\hat{\nu}_j(\gamma)|$. [Note that $\gamma|_G$ must be congruent to one of $\gamma_1, \dots, \gamma_m$ modulo G_1^\perp , say to γ_j . Thus, on $x_l + G$, $l \neq j$, $\hat{\nu}_l(\gamma) = \langle -\gamma, x_l \rangle \hat{\mu}(\gamma - \gamma_l) = \langle -\gamma, x_l \rangle \cdot 0 = 0$, since $\gamma - \gamma_l \notin G_1^\perp$.] Thus $\|\hat{\nu}\|_\infty = (m \cdot \#G)^{1/2}$, and $\|\nu\| = m\|\mu\| = m(\#G)$. Thus ν is an extremal measure on $\{x_1, \dots, x_m\} + G$, and that gives us (i).

(ii) As in (i), we find a subgroup G_1 of G and a measure $\mu \in M(G)$ such that $\#G_1 = m/2$,

$$(2.3) \quad \mu * m_{G_1} = \mu, \quad \|\mu\| = \#G \quad \text{and} \quad \|\hat{\mu}\|_\infty = ((m/2)\#G)^{1/2}.$$

We let $\gamma_1, \dots, \gamma_{m/2}$ be distinct representatives of the cosets of G_1^\perp in G^* . For $g \in G$, we define for $1 \leq j \leq m/2$,

$$(2.4) \quad \nu\{x_j + g\} = \langle \gamma_j, g \rangle \mu(\{g\}) \quad \text{and} \quad \nu\{x_{j+m/2} + g\} = i \langle \gamma_j, g \rangle \mu(\{g\}).$$

Straightforward calculations using the fact $\langle \gamma, x_j \rangle = \pm 1$ for all j and all $\gamma \in G^*$ show that $\|\hat{\nu}\|_\infty = (m \cdot \#G)^{1/2}$.

(iii) Let the measure μ on $E = G + \{x_1, \dots, x_m\}$ be such that $\|\mu\| = \#E$ and $\|\mu^\wedge\|_\infty = (\#E)^{1/2}$. Then μ has the form $\mu = \sum_{j=1}^m \delta(x_j) * \mu_j$, where $\|\mu_j\| = \#G$ for $1 \leq j \leq m$. We shall then show for some $1 \leq j \leq m$ that

(2.5) If $\gamma \in G^\wedge$ and $\mu_j^\wedge(\gamma) \neq 0$, then $\mu_k^\wedge(\gamma) = 0$ for $k \neq j$.

Assume that (2.5) holds for some j . Define A_j to be $\{\gamma \in G^\wedge \mid \mu_j^\wedge(\gamma) \neq 0\}$. Then, by Lemma 1.1 and the Plancherel Theorem, we have

$$(2.6) \quad \begin{aligned} \|\mu_j\|_2 &= (\#A_j/\#G)^{1/2} \|\mu_j^\wedge\|_\infty = (\#A_j/\#G)^{1/2} \|\mu^\wedge\|_\infty \\ &= (\#A_j)^{1/2} (\|\mu^\wedge\|_\infty / (\#G)^{1/2}), \end{aligned}$$

whereas $\|\mu_j\|_2 = (\#G)^{1/2}$. Since $\|\mu^\wedge\|_\infty = (\#E)^{1/2} = m^{1/2}(\#G)^{1/2}$, we obtain

$$(2.7) \quad m^{1/2}(\#A_j)^{1/2} = \|\mu_j^\wedge\|_2 = \|\mu_j\|_2 = (\#G)^{1/2}.$$

Evidently m divides $(\#G)$. (2.5) remains to be established.

We shall show that if $2x_j \neq 0$ for some j , then (2.5) holds for that j . We may assume that $2x_1 \neq 0$.

Suppose that there exists $\gamma \in G^\wedge$ such that $\mu_1^\wedge(\gamma) \neq 0$ and such that there exists $1 \leq j_1 < j_2 < \dots < j_k < m$ for which $\mu_{j_i}^\wedge(\gamma) \neq 0$ for all i , and $\mu_j^\wedge(\gamma) = 0$ for $j \notin \{1, j_1, \dots, j_k\}$. We shall derive a contradiction, thus establishing (2.5).

Because $x_1, x_{j_1}, \dots, x_{j_k}$ are independent, we may specify extensions λ_r of γ to H such that $\sum_{i=1}^k \langle -\lambda_r, x_{j_i} \rangle \mu_{j_i}^\wedge(\gamma)$ has a nonzero value, independent of r , and such that $\langle \lambda_r, x_1 \rangle = e^{2\pi i r/q}$, for $1 \leq r \leq q$, where $q \geq 3$ is the order of x_1 . (If x_1 has infinite order, we may choose $\lambda_1, \lambda_2, \lambda_3$ so that $\langle \lambda_r, x_1 \rangle = e^{2\pi i r/3}$.)

Since $\mu^\wedge(\lambda_r) = \langle -\lambda_r, x_1 \rangle \mu_1^\wedge(\gamma) + \sum \langle -\lambda_r, x_{j_i} \rangle \mu_{j_i}^\wedge(\gamma)$ and the first factor of the first term varies among at least three distinct roots of unity, $|\mu^\wedge(\lambda_r)|$ is not a constant function of r . That contradicts Lemma 1.1, and therefore (2.5) holds. That ends the proof of Theorem 2.1.

3. Examples.

3.1. PROPOSITION. (i) *Each of the following three element sets is extremal in the group indicated.*

Z_3 in Z_3 ,

$\{0, 1, 2\}$ in Z_4 .

(ii) *Every three element extremal set can be obtained from one of the above by the operations of group automorphism, passing to a subgroup, and translation.*

3.2. PROPOSITION. (i) *Each of the following four element sets is extremal in the group indicated.*

Z_4 in Z_4 ,

$\{0, 1, 2, 3\}$ in Z_5 ,

$\{0, 1, 2, 4\}$ in Z_7 ,

$\{0, x, y, x + y\}$ where $2x = 0$, in any group (union of two cosets),

$\{(0, 0), (1, 0), (3, 1), (0, 1)\}$ in $Z_4 \times Z_2$.

(ii) *Every four element extremal set can be obtained from one of the above by the operations of group automorphism, passing to a subgroup, and translation.*

3.3. PROPOSITION. (i) *Each of the following five element sets is extremal in the group indicated.*

Z_5 in Z_5 ,

$\{0, 1, 2, 3, 4\}$ in Z_6 ,

$\{0, 1, 2, 5, 10\}$ in Z_{12} ,

$\{(0, 0), (2, 0), (0, 1), (2, 1), (1, 0)\}$ in $Z_4 \times Z_2$,

$\{(0, 0), (1, 0), (2, 0), (3, 0), (0, 1)\}$ in $Z_4 \times Z_2$,

$\{(0, 0, 0), (1, 0, 0), (0, 1, 0), (0, 0, 1), (1, 1, 0)\}$ in $Z_2 \times Z_2 \times Z_2$.

(ii) *Every five element extremal set can be obtained from one of the above by the operations of group automorphism, passing to a subgroup, injection of one of the groups above, and translation.*

3.4. REMARKS. (i) The proofs of 3.1–3.3 are tedious calculations involving elimination of cases; that of 3.3 currently occupies some two hundred pages of manuscript.

(ii) That there is but “one” two element extremal set is obvious.

(iii) We do not know about the six element case, or even if $\{0, 1, 2, 3, 4, 5\}$ is extremal in Z_7 . We do know that $\{0, 1, 2, 3, 4, 5, 6\}$ is extremal in Z_8 .

3.5. Some specific questions. (i) Can the implication 2.1(ii) be reversed? That is, if all x_j have order two and $\{x_1, \dots, x_m\} + G$ is extremal, must either m divide $\#G$ or m be even and $m/2$ divide $\#G$?

(ii) Is $\{0, 1, 2, \dots, n-2\}$ always extremal in Z_n ?

(iii) If $\|\mu^{\pm n}\| = o(\log|n|)$, is μ trivial? This is a question of Kahane. In view of the trivial fact that if μ is supported on a finite coset and $\|\mu^{\pm n}\| = o(\log|n|)$, then $\|\mu^{\pm n}\| = O(1)$, and our examples in §2, “trivial” should be interpreted as “concentrated on a finite coset”. Kahane’s question seems ripe for solution.

4. The nonabelian case. The Sidon constant of a closed subset of a nonabelian group is defined to be the supremum of the fractions $\|\mu\|/\|\mu\|_0$, where $\|\mu\|$ denotes the measure norm, $\|\mu\|_0$ denotes the norm of μ as an operator (by convolution) on $L^2(G)$, and the supremum is taken over all nonzero measures supported on the set in question.

Cartwright, Howlett and McMullen [C] have shown that a solvable group (and some others) has Sidon constant equal to the square root of its cardinality. By simpler means, we prove the following weaker (but more general) result.

4.1. PROPOSITION. *Let G be a finite group. Then the Sidon constant of G is at least $(.8)(\#G)^{1/13}$.*

PROOF. We leave most of the details to the reader.

We claim that if $k < \log_3 \#G$, then there exist $x_1, \dots, x_k \in G$ such that

$$(4.1) \quad \#(\{1, x_1\} \cdots \{1, x_k\}) = 2^k.$$

The proof of the claim is straightforward.

Straightforward calculations show that if $k \geq 2$ and x_1, x_2 and G satisfy (4.1), then the measure

$$(4.2) \quad \mu = \delta_1 + \delta_{x_1} + \delta_{x_2} - \delta_{x_1 x_2}$$

has norms $\|\mu\| = 4$ and $\|\mu\|_0 = \|(\mu * \tilde{\mu})^2\|_0^{1/4} \leq \|(\mu * \tilde{\mu})^2\|^{1/4} \leq (124)^{1/4}$. [In the sum for $(\mu * \tilde{\mu})^2$, the terms involving masses at $x_1, x_1^{-1}, x_1x_2^2, x_2^{-2}x_1^{-1}, x_2^2x_1^{-1}, x_1x_2^{-2}, x_2^2$ and x_2^{-2} all cancel.]

On taking $k = [(\log_3 \# G)/2]$ products of the form (4.2), we see that

$$\begin{aligned} \alpha(G) &> (4/(124)^{1/4})^k \\ &> [(124)^{1/4}/4][\# G]^{(\log 2 - (1/8)\log 124)/\log 3} > [.834](\# G)^{1/13}. \end{aligned}$$

[Use of $\|\mu * \tilde{\mu}\|_0 \leq 12$ yields $\alpha(G) > (.866)(\# G)^{1/16}$. More sophisticated choices of μ in (4.2) and higher powers of $\mu * \tilde{\mu}$ may yield somewhat larger bounds for $(\# G)$.]

REFERENCES

- [C] D. I. Cartwright, R. B. Howlett and J. R. McMullen, *Extreme values for the Sidon constant*, Proc. Amer. Math. Soc. **81** (1981), 531–537.
 [GM] C. C. Graham and O. C. McGehee, *Essays in commutative harmonic analysis*, Springer-Verlag, Berlin and New York, 1979.

DEPARTMENT OF MATHEMATICS, NORTHWESTERN UNIVERSITY, EVANSTON, ILLINOIS 60201

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF HAWAII, HONOLULU, HAWAII 96822