EXTREME VALUES FOR THE SIDON CONSTANT

DONALD I. CARTWRIGHT, ROBERT B. HOWLETT AND JOHN R. McMULLEN

ABSTRACT. Let $G$ be a compact group and let $\phi \neq P \subseteq \hat{G}$. We consider the inequalities $1 < \kappa(P) < (\sum_{\sigma \in P} d_{\sigma}^2)^{1/2}$, where $\kappa(P)$ denotes the Sidon constant of $P$. The condition $\kappa(P) = 1$ essentially characterizes an example of Figà-Talamanca and Rider. The condition $\kappa(P) = (\sum_{\sigma \in P} d_{\sigma}^2)^{1/2}$ for finite $P$ is equivalent to the existence of certain interesting functions on $G$. We show that $\kappa(G) = |G|^{1/2}$ for a very large class of finite groups $G$, and this implies the existence of "$G$-circulant" unitary matrices whose entries all have modulus $|G|^{-1/2}$.

Let $G$ be a compact group and let $P$ be any nonempty subset of $\hat{G}$, the dual hypergroup of $G$. We denote by $S_P(G)$ the space of trigonometric polynomials $f$ on $G$ whose Fourier transforms $\hat{f}$ vanish off $P$. The point of departure of this article is the easily proved pair of inequalities

$$1 < \kappa(P) < \left( \sum_{\sigma \in P} d_{\sigma}^2 \right)^{1/2}$$

(see Proposition 1), in which $\kappa(P)$ denotes the Sidon constant of $P$, defined by

$$\kappa(P) = \sup \left\{ \| f \|_1 = \sum_{\sigma \in P} d_{\sigma} \| \hat{f}(\sigma) \|_{\Phi}, f \in S_P(G), \| f \|_{\infty} < 1 \right\},$$

and where, as usual, $d_{\sigma}$ denotes the degree of the representation $\sigma$ in $\hat{G}$, and $\| \|_{\Phi}$ denotes the trace-class norm.

We investigate conditions under which $\kappa(P)$ takes one of the two bounding values in (1). For the case $\kappa(P) = 1$ we give a complete answer. Indeed, we show that the example of Figà-Talamanca and Rider [1] of a Sidon set $P$ constructed using the projections on the various factors of a product of unitary groups gives essentially the only situation in which $\kappa(P) = 1$ can occur.

We give in Proposition 3 various necessary and sufficient conditions for $\kappa(P) = (\sum_{\sigma \in P} d_{\sigma}^2)^{1/2}$ to hold. In Theorem 2 and its corollary, we show that this is the case whenever $P = \hat{G}$ and $G$ belongs to a large class of finite groups. This special case permits construction of certain generalized circulant Hadamard matrices, or equivalently certain elements of the group algebra $CG$. It also strongly generalizes the result of Graham [2], who established this when $G$ is a finite abelian group.

Finally, we show by example that there exist two finite groups $A$ and $B$, a hypergroup isomorphism $\phi: \hat{A} \rightarrow \hat{B}$, and a set $P \subseteq \hat{A}$ such that $\kappa(P) \neq \kappa(\phi(P))$. Thus the result of Vrem [7], that whether a subset $P$ of $\hat{G}$ is a central Sidon set
depends only on the hypergroup $\hat{G}$ and not on the compact group $G$ giving rise to it, is unlikely to hold sway for general Sidon sets.

Unexplained notation will be that of Hewitt and Ross [3].

1. The basic inequalities. Henceforth when $P \subseteq \hat{G}$ we use the notation $\|P\| = \sum_{a \in P} d_a^2$. Then using [3, (D.51) and (28.43)] and the Cauchy-Schwarz inequality it is easy to obtain

Proposition 1. Let $G$ be a compact group and let $P \subseteq \hat{G}$ be a finite nonempty set. Then for each $f \in \mathcal{G}_p(G)$ we have

$$\|f\|_\infty < \|\hat{f}\|_1 < \|P\|^{1/2}\|f\|_\infty,$$

and hence

$$1 < \kappa(P) < \|P\|^{1/2}. \quad (1')$$

2. Sets $P$ with $\kappa(P) = 1$. Let $G = \prod_{a \in \Lambda} G_a$ be a Cartesian product in which each factor $G_a$ is a unitary group. Let $\text{pra}$ denote the projection on the factor $G_a$, and for each $a \in \Lambda$ let $\sigma_a \in \hat{G}_a$ be the self-representation. In [1], Figà-Talamanca and Rider showed that $P = \{\sigma_a \circ \text{pra} | a \in \Lambda\}$ is a Sidon set. In fact it is plain that $\kappa(P) = 1$. The following theorem characterizes situations of this kind.

Theorem 1. Let $G$ be a compact group, and let $P$ be any subset of $\hat{G}$. Let $\phi_p$ denote the homomorphism $\prod_{a \in P} \sigma$ of $G$ into $\mathfrak{U}_p = \prod_{a \in P} \mathfrak{U}(H_a)$. Then $\kappa(P) = 1$ holds if and only if every element of $\mathfrak{U}_p$ can be written $\lambda \phi_p(x)$, with $\lambda \in \mathbb{T}$ and $x \in G$. In particular, if $P = \{1\} \cup Q$ with $1 \notin Q$, then the condition becomes: $\phi_Q: G \to \mathfrak{U}_Q$ is a surjection.

The proof requires the following technical lemma.

Lemma. Let $G$ be a compact group, let $P \subseteq \hat{G}$ be finite, and let $U_\tau \in \mathfrak{U}(H_\tau)$ be given for each $\tau \in P$. Then there exist $x_1, \ldots, x_n \in G$ and $\mu_1, \ldots, \mu_n \in \mathbb{C}$ such that $\sum |\mu_\tau| = 1$ and such that $U_\tau = \kappa(P) \sum_{a=1}^{n} \mu_a \sigma(x_\tau)$, for each $\tau \in P$. Indeed $\kappa(P)$ is the smallest constant with this property.

The lemma follows from the bipolar theorem applied to the inclusion $A \subseteq \kappa(P)B^{00}$, in which $B = \{\bigoplus_{a \in P} \sigma(x)| x \in G\}$ and $A = \{\bigoplus_{a \in P} U_a| \sigma \in \mathfrak{U}(H_\sigma)\}$ for all $\sigma \in P$ are regarded as subsets of $\mathfrak{E}(\bigoplus_{a \in P} H_\sigma)$, and the absolute bipolars are taken with respect to the pairing $\langle T, S \rangle = \text{trace}(TS)$. (Notice that the circled convex hull $\Gamma(B)$ of $B$ is closed, since $B$ is compact and $\mathfrak{E}(\bigoplus_{a \in P} H_\sigma)$ is finite-dimensional.)

Now the assertion of the theorem for finite $P$ follows immediately from the lemma, since $\mathfrak{U}(H)$ is the set of extreme points of the unit ball of $\mathfrak{E}(H)$ (see [5, Theorem 1.6.4]). The case of infinite $P$ then follows by a routine compactness argument.

Remark. If $G = \mathbb{T}$, then Theorem 1 shows that a subset $P$ of $\mathbb{Z}$ whose Sidon constant is 1 has at most two elements, since $\phi_p(G)$ has dimension at most one as a submanifold of $\mathfrak{U}_p$, while the latter has dimension card $P$. Similarly, if $G$ is a
compact Lie group of dimension \( n \) and if \( P \subseteq \hat{G} \) with \( \kappa(P) = 1 \), then \( P \) may contain at most \( n + 1 \) elements.

Before leaving this topic we record without proof a curious geometric interpretation of the Sidon constant afforded by the above lemma. We let \( d(, ) \) denote the metric obtained from the operator norm on \( \mathcal{E}(\bigoplus_{\sigma \in P} H_\sigma) \), and define \( \rho(P) = \sup\{ d(U, \Gamma(B)) | U \in A \} \) where \( B, \Gamma(B) \) and \( A \) are defined as in the proof of the lemma. Thus for a single \( \sigma \in P \) we have

\[
\rho(\sigma) = \sup\{ d(U, \Gamma(\sigma(G))) | U \in \mathcal{U}(H_\sigma) \}.
\]

**Proposition 2.** \( \kappa(P) = \left(1 - \rho(P)\right)^{-1} \) for any finite \( P \subseteq \hat{G} \). □

### 3. Sets \( P \) with \( \kappa(P) = \|P\|^{1/2} \)

**Proposition 3.** Let \( G \) be a compact group and let \( P \subseteq \hat{G} \) be nonempty and finite. Then \( \kappa(P) = \|P\|^{1/2} \) holds if and only if there exists a complex-valued function \( f \) on \( G \) satisfying one of the following equivalent conditions:

(a) \( f \in \mathcal{T}_P(G) \), \( \|\hat{f}\|_1 = \|P\|^{1/2} \) and \( \|f\|_\infty < 1 \).

(b) \( |f| \equiv 1 \), and \( |P|^{1/2} f(\sigma) \) vanishes for \( \sigma \not\in P \) and \( f \) is unitary for \( \sigma \in P \).

(c) \( |f| \equiv 1 \), and \( f \ast f^* = \|P\|^{-1} \sum_{\sigma \in P} d_{\sigma} \chi_\sigma \).

**Proof.** Since \( \mathcal{T}_P(G) \) is finite-dimensional, the mapping \( f \mapsto \|\hat{f}\|_1 \) attains its maximum on \( \{ f \in \mathcal{T}_P(G) : \|f\|_\infty < 1 \} \). Thus \( \kappa(P) = \|P\|^{1/2} \) if and only if a function \( f \) exists satisfying (a). When proving Proposition 1 one sees that for equality to hold in the inequality \( \|\hat{f}\|_1 < \|P\|^{1/2} \|f\|_\infty \) it is necessary and sufficient that \( |f| \) be constant and that for some \( c > 0 \) independent of \( \sigma \), \( c\hat{f}(\sigma) \) is unitary for all \( \sigma \in P \). This shows the equivalence of (a) and (b). The equivalence of (b) and (c) is easily seen by taking Fourier transforms. □

It will be convenient to write \( \delta_P \) for the function \( \|P\|^{-1} \sum_{\sigma \in P} d_{\sigma} \chi_\sigma \) appearing in (c). In a special situation, \( \delta_P \) assumes a simple form:

**Proposition 4.** Let \( N \) be an open normal subgroup of the compact group \( G \). Let \( \rho \in \hat{N} \) be \( G \)-invariant (i.e. the representation \( \rho^*: N \mapsto \rho(x^{-1}nx) \) is equivalent to \( \rho \) for each \( x \in G \)). Let \( P = \rho^G \), where we define \( \rho^G = \{ \sigma \in \hat{G} : \rho \) is a component of \( \sigma|_N \} \). Then \( P \) is finite, \( \|P\| = \|G : N\|d_\rho^2 \), and

\[
\delta_P(x) = \begin{cases} 0 & \text{if } x \not\in N, \\ \frac{\chi_\rho(x)}{d_\rho} & \text{if } x \in N. \end{cases}
\]

**Proof.** Put

\[
g(x) = \begin{cases} 0 & \text{if } x \not\in N, \\ \chi_\rho(x) & \text{if } x \in N. \end{cases}
\]

If \( \sigma \in P \) we see that \( \hat{g}(\sigma) = [G : N]^{-1} \int_N \chi_\rho(n)\sigma(n^{-1}) \, dn \) so that by Clifford’s theorem \( \hat{g}(\sigma) = [G : N]^{-1} d_{\rho}^{-1} \mathcal{I}_{H_\sigma} \). If \( \sigma \not\in P \) then \( \rho \) is not a component of \( \sigma|_N \) and therefore \( \hat{g}(\sigma) = 0 \). From this we see that the equation \( d_{\rho}[G : N]g = \sum_{\sigma \in P} d_{\sigma} \chi_\sigma \) holds, as both members are continuous functions and their Fourier transforms agree. Evaluation at the identity yields \( [G : N]d_{\rho}^2 = \|P\| \) and hence \( d_{\rho} \delta_P = g \) follows. □
Our next theorem implies that \( \kappa(P) = \|P\|^{1/2} \) holds for sets \( P \) of the form \( \rho^G \), at least when \( G \) is a finite solvable group and \( d_\rho = 1 \).

**Theorem 2.** Let \( N \) be a normal subgroup of a finite solvable group \( G \), and let \( \rho \) be a linear character of \( N \) satisfying \( \rho(x^{-1}nx) = \rho(n) \) for all \( x \in G \) and \( n \in N \). Then there exists a function \( f: G \to \mathbb{C} \) satisfying

(i) \( |f(x)| = 1 \) for all \( x \in G \).
(ii) \( f(xn) = f(x)p(n) \) for all \( x \in G \) and \( n \in N \).
(iii) \( f \ast f^* = 0 \) off \( N \).

Note. (i) and (ii) entail \( f \ast f^*|_N = \rho \).

**Proof.** The key idea is lifting \( f \) from a subgroup \( M_1 \) to a subgroup \( M_3 \), where \( M_1 < M_2 < M_3 \) and \( [M_2 : M_1] = [M_3 : M_2] = p \) a prime. Straightforward lifting of \( f \) from \( M_1 \) to \( M_3 \) fails, in general.

Assuming the theorem is false, let \( G \) be a counterexample of minimal order. Choose \( N \lhd G \) and a \( G \)-invariant linear character \( \rho \) of \( N \) for which no function \( f \) exists with the desired properties. We obtain a contradiction by means of several steps.

1. \( \rho \) is faithful. Since \( \rho \) is \( G \)-invariant, \( H = \ker \rho \) is a normal subgroup of \( G \). Let \( \hat{\rho} \) be the character of \( \hat{N} = \ker \rho \) induced by \( \rho \). If \( H \neq \{1\} \), then by minimality of \( G \) there exists \( \hat{f}: G/H \to \mathbb{C} \) satisfying (i), (ii) and (iii) with \( G \) replaced by \( G/H \) and \( N \) by \( N/H \) and \( \rho \) by \( \hat{\rho} \). Define \( f: G \to \mathbb{C} \) by \( f(x) = \hat{f}(xH) \) and it is easy to see that \( f \) has the desired properties. This contradiction shows that \( H = \{1\} \).

2. \( N \) is contained in the centre of \( G \). This follows from step 1 since \( \rho(x^{-1}nx) = \rho(n) \) for all \( x \in G \) and \( n \in N \).

3. There do not exist proper subgroups \( G_1/N, \ldots, G_r/N \) of \( G/N \) such that each \( \xi \in G/N \) is uniquely expressible as a product \( \xi_1 \xi_2 \cdots \xi_r \) with \( \xi_j \in G_j/N \) for each \( j \). Suppose \( G/N \) has such subgroups. Since \( |G_j| < |G| \) for each \( j \), there exist functions \( f_j: G_j \to \mathbb{C} \) satisfying (i), (ii) and (iii) (with \( G \) replaced by \( G_j \)). Our hypotheses and step 2 show that each \( x \in G \) may be expressed in the form \( x_1 x_2 \cdots x_r \) (with \( x_j \in G_j \) for all \( j \)) in exactly \( |N|^{-r-1} \) ways. Property (ii) of the functions \( f_j \) shows that a function \( f: G \to \mathbb{C} \) is well defined if we set \( f(x) = f_1(x_1)f_2(x_2) \cdots f_r(x_r) \) for any such decomposition of \( x \). It is clear that \( f \) satisfies properties (i) and (ii). To see that (iii) holds, notice that \( f = (|G|/|N|)^{r-1} \hat{f}_1 \ast \cdots \ast \hat{f}_r \), where

\[
\hat{f}_j(x) = \begin{cases} 0 & \text{if } x \in G \setminus G_j, \\ f_j(x) & \text{if } x \in G_j.
\end{cases}
\]

Notice also that \( \hat{f}_j \ast \hat{f}_j^* = [G : G_j]^{-1} \delta \), that \( \delta \ast \delta = [G : N]^{-1} \delta \), where

\[
\delta(x) = \begin{cases} 0 & \text{if } x \in G \setminus N, \\ \rho(x) & \text{if } x \in N,
\end{cases}
\]

and that \( \delta \) is central in \( \mathcal{F}(G) \) (\( \delta = \delta_p \) in the notation of Proposition 4). This completes step 3.

4. \( G/N \) is a \( p \)-group for some prime \( p \). If \( G/N \) is not a \( p \)-group, then being solvable it has nontrivial proper Hall subgroups \( G_1/N \) and \( G_2/N \) corresponding to
complementary sets of prime divisors of $|G/N|$. Since $G/N = G_1/N \cdot G_2/N$ and $G_1/N \cap G_2/N = \{1\}$, step 3 yields a contradiction.

5. If $|N| > 1$ then $\rho$ does not extend to a character of $G$. Suppose that $|N| > 1$ and that $\rho$ extends to a character $\tilde{\rho}$ of $G$. By minimality of $G$ there exists a function $\tilde{f}: G/N \to \mathbb{C}$ satisfying (i), (ii) and (iii) (with $G$ replaced by $G/N$, $N$ by the trivial subgroup of $G/N$ and of course $\rho$ by the trivial representation). Define $f: G \to \mathbb{C}$ by $f(x) = \tilde{f}(xN)\tilde{\rho}(x)$ and clearly a contradiction is obtained.

6. $G$ is not abelian. If $G$ is abelian, then $N = \{1\}$ by step 5. But then the set $P$ of Proposition 4 is the whole dual group $\hat{G}$ and so $\kappa(P) = ||P||^{1/2} (= |G|^{1/2})$ (see Graham [2]). Hence a function $f$ exists satisfying (i), (ii) and (iii).

7. For the $p$-group $G/N$ we have $p = 2$. By steps 2 and 6 we have $N \nsubseteq G$, and so there is a subgroup $M$ of $G$ with $N \subset M$, $M/N \subseteq Z(G/N)$ and $[M : N] = p$. Then $M$ is abelian and normal. Let $\Lambda = \{\lambda \in \hat{M} : |\lambda| = p\}$, and fix any $\lambda_0 \in \Lambda$. Then $\Lambda = \{\lambda_0^v : v \in N^0\}$, where $N^0$ denotes the subgroup of $\hat{M}$ whose elements are trivial on $N$. Now $G$ acts on $\Lambda$ and fixes $N^0$ elementwise. Let $H_0$ be the stabilizer of $\lambda_0$. Since $|\Lambda| = p$ we must have $H_0 = G$ or $[G : H_0] = p$. Since $M$ is abelian, we have $M \subseteq H_0$ and $M \neq G$. Hence there is a subgroup $H$ of $G$ with $[G : H] = p$ and $M \subseteq H \subseteq H_0$. Since $|H| < |G|$ there is for each $\lambda \in \Lambda$ a function $f_\lambda: H \to \mathbb{C}$ satisfying (i), (ii) and (iii) with $G$ replaced by $H$, $N$ replaced by $M$, and $\rho$ replaced by $\lambda$. Choose coset representatives $\{x_\lambda : \lambda \in \Lambda\}$ for $H$ in $G$ (note that $|\Lambda| = [G : H] = p$) and define $f: G \to \mathbb{C}$ by $f(x_\lambda h) = f_\lambda(h)$ for $\lambda \in \Lambda$ and $h \in H$. Clearly $f$ satisfies (i) and (ii), and one calculates that

$$(f \ast f^*)(x) = \begin{cases} 0 & \text{if } x \not\in M, \\ \frac{1}{p} \sum_{\lambda \in \Lambda} \lambda(x^{-1}xx_\lambda) & \text{if } x \in M. \end{cases}$$

(Note that $\lambda^H \cap \lambda'^H = \emptyset$ when $\lambda, \lambda' \in \Lambda$ are distinct, since $\lambda$ is the only component of $\sigma|_M$ if $\sigma \in \lambda^H$. Therefore $f_\lambda \ast f_\lambda = 0$ if $\lambda \neq \lambda'$, taking the convolution over $H$ here, since $f_\lambda \in \mathcal{S}_Q(H)$ with $Q = \lambda^H$.)

If the coset representatives $x_\lambda$ are chosen so that the characters $\{\lambda^x : \lambda \in \Lambda\}$ are distinct, then the sum in (3) is simply $\Sigma_{\lambda \in \Lambda} \lambda(x)$ and so $f$ satisfies (iii). (Such a choice of $x_\lambda$'s is achieved as follows: Suppose first that $H_0 \neq G$. Pick $x \in G \setminus H_0$. Thus $\lambda_0^x = \lambda_0^v$ for some nontrivial $v \in N^0$. The powers $\nu^k$ of $\nu$ for $k = 0, \ldots, p - 1$ are distinct, and so $\lambda_0^{\nu^k}$ runs through all of $\Lambda$. For each $k$ we have $(\lambda_0^{\nu^k})^{x^k} = \lambda_0^{\nu^{2k}}$, and if $p \neq 2$ the characters $\nu^{2k}$, $k = 0, \ldots, p - 1$, are all distinct. Hence if we set $x_\lambda = x^k$ whenever $\lambda = \lambda_0^{\nu^k}$, we have achieved our aim. In the case $H_0 = G$, we have $\lambda^x = \lambda$ for all $x \in G$ and $\lambda \in \Lambda$, and any choice of $x_\lambda$'s will do. Hence $p \neq 2$ leads to a contradiction.

8. $G/N$ is not a 2-group. The argument used in step 7 breaks down if the two extensions $\lambda_1$ and $\lambda_2$ of $\rho$ to $M$ are interchanged by some $x \in G$. Assume then that this is the case, so that $H = H_0$ in the above notation. If $H$ is the only maximal subgroup of $G$ containing $M$, then $G/H$ is cyclic, and since $M/N \subseteq Z(G/N)$, $G/N$ is abelian. But then $G/N$ is cyclic by step 3 and the structure theory of abelian groups. But this and $N \subseteq Z(G)$ shows that $G$ is abelian, contradicting step 6. So let $K$ be another maximal subgroup of $G$ containing $M$, and let $L = H \cap K$. 

License or copyright restrictions may apply to redistribution; see http://www.ams.org/journal-terms-of-use
Pick any \( x \in K \setminus H \). Then \( K = L \cup Lx \), and \( x \) interchanges \( \lambda_1 \) and \( \lambda_2 \). Let \( g_1, g_2 : L \to C \) satisfy (i), (ii) and (iii) with \( L \) replacing \( G \), \( M \) replacing \( N \), and \( \lambda_1 \) (resp. \( \lambda_2 \)) replacing \( \rho \). Define \( f_1, f_2 : K \to C \) by \( f_1(l) = g_1(l) \) for \( l \in L \), \( f_1(lx) = g_2(l) \), \( f_2(lx^{-1}) = -g_2(l) \). Then \( f_1 \) and \( f_2 \) satisfy (i) and (iii) (but not (ii)) with \( K \) replacing \( G \), \( M \) replacing \( N \) and \( \lambda_1 \) (resp. \( \lambda_2 \)) replacing \( \rho \). Also \( f_1 \ast f_2 = 0 \), taking the convolution over \( K \). The calculations needed here are not difficult. For example, if \( \xi \in Lx \), write \( \xi = l_0x \) with \( l_0 \in L \), and we have

\[
\frac{1}{|K|} \sum_{k \in K} f_1(k) f_1(\xi^{-1}k) = \frac{1}{|K|} \sum_{l \in L} \left\{ f_1(l) f_1(x^{-1}l_0^{-1}l) + f_1(lx) f_1(x^{-1}l_0^{-1}lx) \right\} = \frac{1}{|K|} \sum_{l \in L} \left\{ g_1(l) g_1(x^{-1}l_0^{-1}lx) + g_1(lx) g_1(x^{-1}l_0^{-1}lx) \right\} = \frac{1}{|M||K|} \sum_{l \in L, m \in M} \left\{ g_1(lm) g_1(x^{-1}l_0^{-1}lmx^{-1}) + g_1(lm) g_1(x^{-1}l_0^{-1}lmx) \right\} = 0,
\]

using the property (ii) for \( g_1 \) and the fact that \( x \) interchanges \( \lambda_1 \) and \( \lambda_2 \).

Now pick any \( y \in H \setminus K \). Then \( G = K \cup yK \), and we may define \( f : G \to C \) by \( f(k) = f_1(k) \) and \( f(yk) = f_2(k) \) if \( k \in K \). It is routine to check that \( f \) satisfies properties (i), (ii) and (iii). \( \square \)

**Corollary.** Let \( G \) be a finite group having solvable subgroups \( G_1, \ldots, G_r \) (\( r > 1 \)) so that each \( x \in G \) is uniquely expressible as a product \( x_1 \cdots x_r \) with \( x_j \in G_j \) for each \( j \). Then \( \kappa(\hat{G}) = \|\hat{G}\|^{1/2} = |G|^{1/2} \).

**Proof.** When \( G \) is solvable this follows from Theorem 2 above, taking \( N \) to be the trivial subgroup. The general case follows from the solvable case as in step 3 of the proof. \( \square \)

**Remark.** We conjecture that every finite group can be decomposed in the above manner. If this conjecture is true, then \( \kappa(\hat{G}) = |G|^{1/2} \) and Theorem 2 are valid for every finite group \( G \).

4. **Circulant matrices.** Let \( G \) be a finite group. We will say that a matrix \( (\xi_{ij})_{i,j=1}^n \) is \( G \)-**circulant** if there is an enumeration \( x_1 = e, x_2, \ldots, x_n \) of \( G \) and a function \( h : G \to C \) such that \( \xi_{ij} = h(x_i^{-1}x_j) \) (\( 1 < i, j < n \)). If \( G = (a^k)_{k=0}^{n-1} \) is cyclic and if \( x_j = a^{j-1} \) for \( j = 1, 2, \ldots, n \) and if we put \( m_j = \xi_{ij} \) then such a matrix takes the form

\[
M = \begin{bmatrix}
  m_1 & m_2 & \cdots & m_{n-1} & m_n \\
  m_n & m_1 & m_2 & \cdots & m_{n-1} \\
  \vdots & \vdots & \ddots & \vdots & \vdots \\
  m_2 & m_3 & \cdots & m_n & m_1
\end{bmatrix}
\]

and is circulant in the usual sense.
THEOREM 3. Let $G$ be any finite group of order $n$. Then there exists a unitary matrix which is $G$-circulant, and whose entries all have modulus $n^{-1/2}$, if and only if $\kappa(\hat{G}) = n^{1/2}$.

PROOF. Apply Propositions 3 and 4 with $N$ the trivial subgroup of $G$. If $f$ is a function satisfying (c) of Proposition 3, then the matrix $(\xi_{ij})$ with $\xi_{ij} = n^{-1/2}f(x^{-1}y)$ has the desired properties. □

The proof of Theorem 2 shows that the matrix in Theorem 3 can be chosen to have the form $A/\sqrt{n}$, where the entries of $A$ are roots of unity. For cyclic $G$, this matrix is real-valued if and only if $A$ is an $n \times n$ circulant Hadamard matrix. Such matrices $A$ are known not to exist for $5 < n < 12100$. For $A$ to have $\pm 1, \pm i$ as entries, $n$ is still very restricted (see, e.g. [6]).

5. A small example. Let $D$ and $Q$ denote respectively the dihedral and quaternion groups of order 8, presented by $D = \langle a, b|a^4 = 1 = b^2, b^{-1}ab = a^{-1}\rangle$ and $Q = \langle a, b|a^4 = 1, b^2 = a^2, b^{-1}ab = a^{-1}\rangle$. Then $\hat{D}$ and $\hat{Q}$ are isomorphic as hypergroups (see McMullen and Price [4]), each consisting of four linear representations, and a two-dimensional representation. Denote the two-dimensional representation of $D$ by $\sigma_1$ and that of $Q$ by $\sigma_2$. Then explicit calculations reveal that $\kappa(\{1, \sigma_1\}) = 2$ but $\kappa(\{1, \sigma_2\}) = \sqrt{5}$. The set $P_2 = \{1, \sigma_2\} \subseteq \hat{Q}$ therefore satisfies the equality $\kappa(P) = ||P||^{1/2}$, while $P_1 = \{1, \sigma_1\} \subseteq \hat{D}$ does not. Thus the Sidon constant is not preserved by hypergroup isomorphisms. We also note that $P_2$ is not of the special form $\rho^G$ introduced in Proposition 4.

REFERENCES


DEPARTMENT OF MATHEMATICS, UNIVERSITY OF SYDNEY, SYDNEY, N.S.W. 2006, AUSTRALIA