Europ. J. Combinatorics (1992) **13**, 401–407

An Uncertainty Inequality for Groups of Order *pq*

ROY MESHULAM

We are concerned with some relations between the support of a function defined on a finite group and the support of its Fourier transform. Let $D_{p,q}$ be the non-commutative group of order pq, where p, q are primes, and $p \mid q-1$. We prove an uncertainty-type inequality for $D^N_{p,q} = \{(x_1, \ldots, x_N): x_i \in D_{p,q}\}$, which has the following application: If H is a subgroup of $D^N_{p,q}$ and $x_1 \cdots x_N = 1$ for all $(x_1, \ldots, x_N) \in H$, then $(D^N_{p,q}: H) \geqslant q^{\frac{1}{2}} p^{(N-1)/2}$.

1. INTRODUCTION

The classical uncertainty inequality and some of its extensions assert (roughly) that a function and its Fourier transform cannot both be concentrated on small sets (see [1] for the classical inequality, and [6] for a recent generalization).

In this note we are concerned with discrete uncertainty type inequalities for finite groups.

Let G be a finite group, and let $Irr(G) = \{\rho_1, \ldots, \rho_t\}$ denote the complex irreducible representations of G, where $\rho_i: G \to GL(V_i)$ and $\deg \rho_i = \dim V_i = n_i$.

For a function $f: G \to \mathbb{C}$ and a representation $\rho: G \to GL(V)$, let $\hat{f}(\rho) = \sum_{x \in G} f(x)\rho(x) \in End(V)$ denote the Fourier transform of f at ρ. This definition may be extended to functions $g: G \to End(U)$, where U is a complex vector space, by $\hat{g}(\rho) = \sum_{x \in G} f(x) \otimes \rho(x) \in End(U \otimes V)$.

Let $Supp\, f = \{x: f(x) \neq 0\}$ and $Supp\, \hat{f} = \{\rho \in Irr(G): \hat{f}(\rho) \neq 0\}$. We shall use $\mu(f) = \sum_{i=1}^t \dim V_i \cdot rank\, \hat{f}(\rho_i)$ and $\bar{\mu}(f) = \sum \{\dim V_i: \hat{f}(\rho_i) \neq 0\}$ as measures of $Supp\, \hat{f}$. Clearly, $\bar{\mu}(f) \leqslant \mu(f) \leqslant \bar{\mu}(f)^2$, and when G is abelian, $\bar{\mu}(f) = \mu(f) = |Supp\, \hat{f}|$.

An alternative definition of $\mu(f)$ in terms of the group algebra $\mathbb{C}[G]$ is as follows. Let $u = \sum_{x \in G} f(x)x \in \mathbb{C}[G]$ and define a linear transformation $T_f: \mathbb{C}[G] \to \mathbb{C}[G]$ by $T_f(v) = uv$.

PROPOSITION 1. $\mu(f) = rank\, T_f$.

PROOF. Define $\varphi: \mathbb{C}[G] \to \prod_{i=1}^t End(V_i)$ by

$$\varphi\Big(\sum_{x \in G} h(x)x\Big) = (\hat{h}(\rho_1), \ldots, \hat{h}(\rho_t))$$

and $S: \prod_{i=1}^t End(V_i) \to \prod_{i=1}^t End(V_i)$ by

$$S(A_1, \ldots, A_t) = (\hat{f}(\rho_1)A_1, \ldots, \hat{f}(\rho_t)A_t).$$

φ is an isomorphism (Proposition 10 in [5]), and it is easy to check that $S\varphi = \varphi T_f$; therefore $rank\, T_f = rank\, S = \sum_{i=1}^t \dim V_i \cdot rank\, \hat{f}(\rho_i)$. □

In Section 2 we prove the following simple uncertainty-type inequality. For abelian groups, part (a) of Theorem 1 was observed in [3], and with a simpler proof in [7].

For a subset $A \subset G$, denote by $1_A(x)$ the indicator function of A.

0195-6698/92/050401 + 07 $02.00/0

THEOREM 1. *Let* $0 \not\equiv f: G \to \mathbb{C}$. *Then*:
(a) $|Supp\, f|\, \mu(f) \geq |G|$.
(b) *Suppose* $f(1) = 1$. *Then* $|Supp\, f|\, \mu(f) = |G|$ *iff* $H = Supp\, f$ *is a subgroup of* G, *and* $f(x) = 1_H(x)\chi(x)$, *where* χ *is a* 1-*dimensional character of* H.

The bound in Theorem 1 may sometimes be improved when more is known on *Supp f*. An example of this with an application to abelian groups is described in [4].

Here we consider another example, as follows. Let G^N be the direct product $G \times \cdots \times G$ (N times), and for $c \in G$ let $A_N(G, c) = \{(x_1, \ldots, x_N): x_1 \cdots x_N = c\}$. Define:

$$\lambda(G, N) = \min\{\mu(f): 0 \not\equiv f: G \to \mathbb{C},\ Supp\, f \subset A_N(G, c) \text{ for some } c \in G\}.$$

$\tilde{\lambda}(G, N)$ is similarly defined using $\tilde{\mu}$; as before, $\tilde{\lambda}(G, N)^2 \geq \lambda(G, N) \geq \tilde{\lambda}(G, N)$.

If G is abelian then $K = A_N(G, c)$ is a coset of the subgroup $H = A_N(G, 1) \subset G^N$. Theorem 1 now implies that $\mu(1_K) = \mu(1_H) = (G^N: H) = |G|$ and $\lambda(G, N) = |G|$.

The situation is rather different when G is non-abelian. In Section 3 we consider the case $G = D_{p,q} = \mathbb{Z}_p \ltimes \mathbb{Z}_q$, where p, q are primes and $p \mid q - 1$.

THEOREM 2. $q^{\frac{1}{2}} p^{(N-1)/2} \leq \tilde{\lambda}(D_{p,q}, N) \leq \lambda(D_{p,q}, N) \leq qp^N$.

As an application we have:

COROLLARY 1. *If* $H \subset A_N(D_{p,q}, 1)$ *is a subgroup of* $D^N_{p,q}$, *then*

$$(D^N_{p,q}: H) = \mu(1_H) \geq \lambda(D_{p,q}, N) \geq q^{\frac{1}{2}} p^{(N-1)/2}.$$

We conclude in Section 4 with some bounds on $\lambda(G, N)$ for general non-abelian groups.

2. PROOF OF THEOREM 1

Let $A = Supp\, f$. To prove (a) it suffices, by Proposition 1, to show that $rank\ T_f \geq |G|/|A|$.

Let t denote the maximal cardinality of a sequence $g_1, \ldots, g_t \in G$ which satisfies $Ag_i \not\subset \bigcup_{j<i} Ag_j$ for all $2 \leq i \leq t$. (Here $Ax = \{ax: a \in A\}$). Clearly if $g_1, \ldots, g_t$ is such a sequence then $T_f(g_1), \ldots, T_f(g_t)$ are linearly independent in $\mathbb{C}[G]$ and so $\mu(f) = rank\ T_f \geq t$. Now the maximality of t implies that $\bigcup_{i=1}^t Ag_i = G$; thus $\mu(f) \geq t \geq |G|/|A|$, which proves (a).

Proof of (b): suppose $f(x) = 1_H(x)\chi(x)$, where χ is a 1-dimensional character of H. Let $g_1, \ldots, g_l$ be a set of $l = (G: H)$ representatives for the right cosets of H in G. It is easy to check that $\{T_f(g_i): 1 \leq i \leq l\}$ forms a basis for the image of T_f in $\mathbb{C}[G]$ and so $\mu(f) = rank\ T_f = (G: H)$.

Conversely, suppose $f(1) = 1$ and $\mu(f) = |G|/|A|$. The proof of part (a) implies that $t = |G|/|A|$ and that, for any $g \in G$, either $Ag = A$ or $Ag \cap A = \emptyset$. (Otherwise $0 < |Ag \cap A| < |A|$ for some $g \in G$. Now choose inductively a maximal sequence $g'_1, \ldots, g'_r \in G$ such that $g'_1 = 1$, $g'_2 = g$ and $Ag'_i \not\subset \bigcup_{j<i} Ag'_j$ for $2 \leq i \leq r$. By maximality $\bigcup_{i=1}^r Ag'_i = G$, and so $t \geq r > |G|/|A|$, a contradiction.)

It follows that A is a subgroup of G: if $a, b \in A$, then $a \in Ab^{-1}a \cap A$, so $Ab^{-1}a = A$, and $b^{-1}a \in A$.

Now let $1 = g_1, \ldots, g_l$ be representatives for the right cosets of A. The subspaces $U_i = \mathbb{C}[A] \cdot g_i$ are all invariant under T_f, and $\bigoplus_{i=1}^l U_i = \mathbb{C}[G]$. Hence $rank\ T_f =$

$(G: A) = l$ implies that $rank\ T_{f\,|\,U_i} = 1$ for all $1 \leq i \leq l$. Taking $i = 1$ it follows that for any $y \in A$, $T_f(y) = h(y)T_f(1)$ for some $h(y) \in \mathbb{C}$. Thus $\sum_{x\in A} f(x)xy = \sum_{x\in A} h(y)f(x)x$, which easily implies $f(xy) = f(x)f(y)$ for all $x, y \in A$. □

3. An Uncertainty Inequality on $D_{p,q}^N$

Let p, q be primes with $p \mid q-1$, and let λ be a (multiplicative) generator of $\mathbb{Z}_q^* = \mathbb{Z}_q - \{0\}$. Write $r = (q-1)/p$ and $\alpha = \lambda^r$.

$C_p = \langle a \rangle$, the cyclic group of order p, acts on $C_q = \langle b \rangle$, the cyclic group of order q, by $b^a = b^\alpha$. The semi-direct product $C_p \ltimes C_q$ with respect to this action is denoted by $D_{p,q}$, and has the following presentation:

$$D_{p,q} = \langle a, b \colon a^p = b^q = 1 \quad a^{-1}ba = b^\alpha \rangle.$$

For $x = a^k b^l \in D_{p,q}$, let $\pi(x) = a^k$.

The complex irreducible representations of $D_{p,q}$ are as follows: (see p. 94 in [2] for the more general case of Frobenius groups):

(1) $D_{p,q}$ has p 1-dimensional representations $\{\varphi_j\}_{j=0}^{p-1}$ defined by $\varphi_j(a^k b^l) = e_p(jk)$, where $e_p(x) = e^{2\pi i x/p}$.

(2) Let $\{\psi_j\}_{j=0}^{q-1}$ be the (1-dimensional) representations of C_q, $\psi_j(b^l) = e_q(jl)$. The induced representations $\rho_j = ind\ \psi_j$ may be described as follows. Let W be the p-dimensional complex vector space spanned by $\{w_t \colon t \in \mathbb{Z}_p\}$. Define $\rho_j \colon D_{p,q} \to GL(W)$ by

$$\rho_j(a^k b^l)(w_t) = e_q(jl\alpha^t) w_{t+k}. \tag{1}$$

All ρ_j, $j \in \mathbb{Z}_q^*$ are irreducible and $\rho_j \simeq \rho_{j'}$ iff $j' = \alpha^u j$ for some u. Thus $\Lambda = \{\rho_j \colon j = \lambda^m \ 0 \leq m < (q-1)/p\}$ constitutes all irreducible p-dimensional representations of $D_{p,q}$.

We now prove Theorem 2. For the upper bound note that

$$H = \left\{(b^{l_1}, \ldots, b^{l_N}) \colon \sum_{i=1}^N l_i \equiv 0 \ (\mathrm{mod}\ q)\right\} \subset A_N(D_{p,q}, 1)$$

is a subgroup of $D_{p,q}^N$. Thus

$$\lambda(D_{p,q}, N) \leq \mu(1_H) = (D_{p,q}^N \colon H) = pq^N.$$

For the lower bound we first estimate $\tilde{\mu}(f)$ on two restricted classes of functions.

Proposition 2. *Suppose* $0 \not\equiv f \colon D_{p,q}^N \to \mathbb{C}$ *satisfies* $Supp\, f \subset A_N(D_{p,q}, 1)$, *and* $f(a^{k_1}b^{l_1}, \ldots, a^{k_N}b^{l_N}) = f(a^{k_1}, \ldots, a^{k_N})$ *whenever* $\prod_{i=1}^N a^{k_i}b^{l_i} = 1$. *Then* $\mu(f) \geq (q-1)p^N$ *and* $\tilde{\mu}(f) \geq (q-1)p^{N-1}$.

Proof. For $\mathbf{k} = (k_1, \ldots, k_N) \in \mathbb{Z}_p^N$, $\mathbf{l} = (l_1, \ldots, l_N) \in \mathbb{Z}_q^N$, we abbreviate $a^{\mathbf{k}}b^{\mathbf{l}} = \prod_{i=1}^N a^{k_i}b^{l_i}$.

By repeated applications of the defining relations of $D_{p,q}$ we obtain:

$$a^{\mathbf{k}}b^{\mathbf{l}} = a^A b^B \qquad \text{where} \qquad A = \sum_{i=1}^N k_i, \quad B = \sum_{i=1}^N l_i \alpha^{\sum_{s=i+1}^N k_s}. \tag{2}$$

For a fixed $\mathbf{k} \in K = \{(k_1, \ldots, k_N) \in \mathbb{Z}_p^N \colon \sum_{i=1}^N k_i \equiv 0 \ (\mathrm{mod}\, p)\}$, let $L(\mathbf{k}) = \{\mathbf{l} \in \mathbb{Z}_q^N \colon a^{\mathbf{k}}b^{\mathbf{l}} = 1\}$. By (2),

$$\mathbf{l} \in L(\mathbf{k}) \quad \text{iff} \quad l_N \equiv -\sum_{i=1}^{N-1} l_i \alpha^{-\sum_{s=1}^i k_s} \quad (\mathrm{mod}\, q). \tag{3}$$

Keeping with previous notation, let ρ_j be an irreducible p-dimensional representation of $D_{p,q}$ and denote

$$F_j(\mathbf{k}) = \sum_{\mathbf{l}\in L(\mathbf{k})} \bigotimes_{i=1}^{N} \rho_j(b^{l_i}) \in End(W^{\otimes N}).$$

Let $\otimes_{i=1}^{N} w_{t_i} \in W^{\otimes N}$. Using (1) and (3) we obtain

$$F_j(\mathbf{k})\left(\bigotimes_{i=1}^{N} w_{t_i}\right) = \sum_{\mathbf{l}\in L(\mathbf{k})} \bigotimes_{i=1}^{N} e_q(jl_i\alpha^{t_i})w_{t_i}$$

$$= \left(\sum_{\mathbf{l}\in L(\mathbf{k})} e_q\left(j\sum_{i=1}^{N} l_i\alpha^{t_i}\right)\right) w_{t_1}\otimes\cdots\otimes w_{t_N}$$

$$= \left(\prod_{i=1}^{N-1}\sum_{l_i=0}^{q-1} e_q(jl_i(\alpha^{t_i} - \alpha^{t_N-\sum_{s=1}^{i} k_s}))\right) w_{t_1}\otimes\cdots\otimes w_{t_N}.$$

Thus $F_j(\mathbf{k})(\otimes_{i=1}^{N} w_{t_i}) = q^{N-1} \otimes_{i=1}^{N} w_{t_i}$ if

$$t_i \equiv t_N - \sum_{s=1}^{i} k_s \pmod p \qquad \text{for all } 1 \leqslant i \leqslant N \tag{4}$$

and is 0 otherwise.

We rewrite (4) as

$$k_1 \equiv t_N - t_1 \pmod p \quad \text{and} \quad k_i \equiv t_{i-1} - t_i \pmod p \qquad \text{for } 2 \leqslant i \leqslant N. \tag{5}$$

Now, by the assumptions on f:

$$\hat{f}(\rho_j\otimes\cdots\otimes\rho_j) = \sum_{\mathbf{k}\in K} f(a^{k_1},\ldots,a^{k_N}) \sum_{\mathbf{l}\in L(\mathbf{k})} \bigotimes_{i=1}^{N} \rho_j(a^{k_i}b^{l_i})$$

$$= \sum_{\mathbf{k}\in K} f(a^{k_1},\ldots,a^{k_N}) \bigotimes_{i=1}^{N} \rho_j(a^{k_i}) \cdot F_j(\mathbf{k}). \tag{6}$$

Combining (5) and (6), we obtain

$$\hat{f}(\rho_j\otimes\cdots\otimes\rho_j)\left(\bigotimes_{i=1}^{N} w_{t_i}\right)$$

$$= q^{N-1} f(a^{t_N-t_1},\ldots,a^{t_{N-1}-t_N})\rho_j(a^{t_N-t_1})\otimes\cdots\otimes\rho_j(a^{t_{N-1}-t_N})\left(\bigotimes_{i=1}^{N} w_{t_i}\right)$$

$$= q^{N-1} f(a^{t_N-t_1}, a^{t_1-t_2},\ldots,a^{t_{N-1}-t_N}) w_{t_N}\otimes w_{t_1}\otimes\cdots\otimes w_{t_{N-1}}. \tag{7}$$

Now, by assumption, $f(a^{k_1},\ldots,a^{k_N}) \neq 0$ for some $\mathbf{k}\in K$, so (7) implies that $\hat{f}(\rho_j\otimes\cdots\otimes\rho_j)$ is 1–1 on

$$Span\left\{\bigotimes_{i=1}^{N} w_{k-k_1-\cdots-k_i} : k\in\mathbb{Z}_p\right\} \subset W^{\otimes N}.$$

Therefore rank $\hat{f}(\rho_j\otimes\cdots\otimes\rho_j) \geqslant p$, and so

$$\mu(f) \geqslant \sum_{\rho_j\in\Lambda} (\deg\rho_j)^N \, rank\, \hat{f}(\rho_j\otimes\cdots\otimes\rho_j) \geqslant (q-1)p^N.$$

Similarly, $\tilde{\mu}(f) \geqslant (q-1)p^{N-1}$. □

For a function $f: D_{p,q}^N \to \mathbb{C}$ and $x, y \in D_{p,q}$, let $f_{x,y}: D_{p,q}^{N-2} \to \mathbb{C}$ be defined by $f_{x,y}(x_1,\ldots,x_{N-2}) = f(x_1,\ldots,x_{N-2},x,y)$.

PROPOSITION 3. *Let* $f: D_{p,q}^N \to \mathbb{C}$ *satisfy* $Supp\, f \subset A_N(D_{p,q}, c)$, *and suppose there exist* $u_1, u_2, v_1, v_2 \in D_{p,q}$ *such that*:
(1) $u_1 u_2 = v_1 v_2 = c'$ *and* $\pi(u_i) = \pi(v_i)$ *for* $i = 1, 2$.
(2) $f_{u_1,u_2}(x_1, \ldots, x_{N-2}) \not\equiv f_{v_1,v_2}(x_1, \ldots, x_{N-2})$ *on* $D_{p,q}^{N-2}$.
Then $\bar{\mu}(f) \geq p\bar{\lambda}(D_{p,q}, N-2)$.

PROOF. Define $g: D_{p,q}^{N-2} \to \mathbb{C}$ by

$$g(x_1, \ldots, x_{N-2}) = f_{u_1,u_2}(x_1, \ldots, x_{N-2}) - f_{v_1,v_2}(x_1, \ldots, x_{N-2}),$$

and let $E = Supp\, \hat{g} = \{\bar{\eta} \in Irr(D_{p,q}^{N-2}): \hat{g}(\bar{\eta}) \neq 0\}$.

Clearly $Supp\, g \subset A_{N-2}(D_{p,q}, c(c')^{-1})$ and $g \not\equiv 0$, so:

$$\sum_{\bar{\eta} \in E} \deg \bar{\eta} = \bar{\mu}(g) \geq \bar{\lambda}(D_{p,q}, N-2). \tag{8}$$

Now fix a representation $\bar{\eta}: D_{p,q}^{N-2} \to GL(U)$, $\bar{\eta} = \eta_1 \otimes \cdots \otimes \eta_{N-2} \in E$, and define $h: D_{p,q}^2 \to End(U)$ by $h(x, y) = \widehat{f_{x,y}}(\bar{\eta})$.

For any $\eta_{N-1} \otimes \eta_N \in Irr(D_{p,q}^2)$, we have

$$\begin{aligned}\hat{f}(\eta_1 \otimes \cdots \otimes \eta_N) &= \sum_{x,y} \sum_{x_1,\ldots,x_{N-2}} f_{x,y}(x_1, \ldots, x_{N-2})\eta_1(x_1) \otimes \cdots \otimes \eta_{N-2}(x_{N-2}) \otimes \eta_{N-1}(x) \otimes \eta_N(y) \\ &= \sum_{x,y} \widehat{f_{x,y}}(\bar{\eta}) \otimes \eta_{N-1}(x) \otimes \eta_N(y) = \hat{h}(\eta_{N-1} \otimes \eta_N). \end{aligned} \tag{9}$$

CLAIM. There exists $\eta_{N-1} \otimes \eta_N \in Irr(D_{p,q}^2)$ such that $\deg(\eta_{N-1} \otimes \eta_N) \geq p$, and $\hat{h}(\eta_{N-1} \otimes \eta_N) \neq 0$.

PROOF. Otherwise $Supp\, \hat{h} \subset \{\varphi_i \otimes \varphi_j \in Irr(D_{p,q}^2): 0 \leq i,\ j \leq p-1\}$ (where $\{\varphi_i\}_{i=0}^{p-1}$ are the 1-dimensional representations of $D_{p,q}$), and so $h(x, y) = \sum_{i,j=0}^{p-1} \varphi_i(x)\varphi_j(y)A_{ij}$ for some A_{ij}'s in $End(U)$.

Now $\pi(u_i) = \pi(v_i)$ implies that $\varphi(u_i) = \varphi(v_i)$ for any 1-dimensional representation φ, and so

$$\widehat{f_{u_1,u_2}}(\bar{\eta}) = h(u_1, u_2) = h(v_1, v_2) = \widehat{f_{v_1,v_2}}(\bar{\eta}),$$

contradicting the choice of $\bar{\eta}$. □

The claim, together with (8) and (9), imply

$$\begin{aligned}\bar{\mu}(f) &= \sum \{\deg(\eta_1 \otimes \cdots \otimes \eta_N): \eta_i \in Irr(D_{p,q}) \hat{f}(\eta_1 \otimes \cdots \otimes \eta_N) \neq 0\} \\ &\geq \sum_{\bar{\eta} \in E} (\deg \bar{\eta})p \geq p\bar{\lambda}(D_{p,q}, N-2). \quad \square\end{aligned}$$

We now prove Theorem 2 by induction on N. First note that by theorem 1 $\lambda(D_{p,q}, N) \geq |D_{p,q}^N|/|A_N(D_{p,q}, c)| = pq$. In particular, $\bar{\lambda}(D_{p,q}, 1) \geq \sqrt{pq}$ and $\bar{\lambda}(D_{p,q}, 2) \geq \sqrt{pq}$.

Now suppose that $N \geq 3$ and $f: D_{p,q}^N \to \mathbb{C}$ satisfies $Supp\, f \subset A_N(D_{p,q}, c)$. Clearly $g(x_1, \ldots, x_N) = f(x_1, \ldots, x_{N-1}, x_N c)$ satisfies $Supp\, g \subset A_N(D_{p,q}, 1)$, and $\bar{\mu}(f) = \bar{\mu}(g)$. We may thus assume that f itself satisfies $Supp\, f \subset A_N(D_{p,q}, 1)$.

We consider two possibilities.

Case *1.* For any $1 \leq j \leq N-1$ and $u_1, u_2, v_1, v_2 \in D_{p,q}$, if $u_1u_2 = v_1v_2$ and $\pi(u_i) = \pi(v_i)$, $i = 1, 2$, then

$$f(x_1, \ldots, x_{j-1}, u_1, u_2, x_{j+2}, \ldots, x_N) = f(x_1, \ldots, x_{j-1}, v_1, v_2, x_{j+2}, \ldots, x_N)$$

for all $x_1, \ldots, x_{j-1}, x_{j+2}, \ldots, x_N \in D_{p,q}$.

In case 1 we repeatedly apply $(a^{k_i}b^{l'})(a^{k_{i+1}}b^{l_{i+1}}) = a^{k_i}(a^{k_{i+1}}b^{l'\alpha^{k_{i+1}}+l_{i+1}})$ to obtain:

$$f(a^{k_1}b^{l_1}, \ldots, a^{k_N}b^{l_N}) = f(a^{k_1}, \ldots, a^{k_N}b^{e}), \tag{10}$$

where $e = \sum_{i=1}^{N} l_i \alpha^{\sum_{s=i+1}^{N} k_s}$.

Equation (10) implies that $f(a^{k_1}b^{l_1}, \ldots, a^{k_N}b^{l_N}) = f(a^{k_1}, \ldots, a^{k_N})$ whenever $\prod_{i=1}^{N} a^{k_i}b^{l_i} = 1$. Therefore, by Proposition 2, $\tilde{\mu}(f) \geq (q-1)p^{N-1} > q^{\frac{1}{2}}p^{(N-1)/2}$.

Case 2. There exist $1 \leq j \leq N-1$ and $u_1, u_2, v_1, v_2 \in D_{p,q}$, which satisfy $u_1u_2 = v_1v_2$ and $\pi(u_i) = \pi(v_i)$, $i = 1, 2$, and such that

$$f(x_1, \ldots, x_{j-1}, u_1, u_2, x_{j+2}, \ldots, x_N) \not\equiv f(x_1, \ldots, x_{j-1}, v_1, v_2, x_{j+2}, \ldots, x_N).$$

In this case define $g(z_1, \ldots, z_N) = f(z_{N-j}, \ldots, z_N, z_1, \ldots, z_{N-j-1})$. Clearly, *Supp* $g \subset A_N(D_{p,q}, 1)$ and $g(z_1, \ldots, z_{N-2}, u_1, u_2) \not\equiv g(z_1, \ldots, z_{N-2}, v_1, v_2)$, so by Proposition 3 and the induction hypothesis

$$\tilde{\mu}(f) = \tilde{\mu}(g) \geq p\tilde{\lambda}(D_{p,q}, N-2) \geq q^{\frac{1}{2}}p^{(N-1)/2}. \qquad \square$$

4. On $\lambda(G, N)$ for General Non-abelian Groups

We first note the following upper bounds on $\lambda(G, N)$:

(1) If A is an abelian subgroup of G, then $H = \{(x_1, \ldots, x_N) \in A^N : x_1, \ldots, x_N = 1\}$ is a subgroup of G^N, and so

$$\lambda(G, N) \leq \mu(1_H) = (G: H) = |A|\,(G: A)^N.$$

(2) Let $f(x)$ denote the indicator function of $A_N(G, 1)$. A simple computation using the orthogonality relations yields:

Proposition 4. *$\lambda(G, N) \leq \mu(f) = \sum_{i=1}^{t} n_i^{2N}$, where $n_1, \ldots, n_t$ are the degrees of the irreducible representations of G.*

Note that both bounds exceed $b(G)^N$, where $b(G) = \max\{n_i : 1 \leq i \leq t\}$. For a lower bound we have the following:

Theorem 3. *For any non-abelian group G, there exists $c(G) > 1$ such that $\lambda(G, N) \geq c(G)^N$.*

The proof uses the approach of Theorem 2, but the $c(G)$ obtained is usually very small. For some classes of groups we have a uniform bound; i.e. if G is non-solvable then $\lambda(G, N) \geq \sqrt{2}^N$. We defer the details to a subsequent paper.

Acknowledgement

This research was supported by Technion V. P. R. Grant No. 100–854.

References

1. H. Dym and H. P. McKean, *Fourier Series and Integrals*, Academic Press, New York, 1972.
2. I. M. Isaacs, *Character Theory of Finite Groups*, Academic Press, New York, 1976.

3. J. Kahn and R. Meshulam, On mod-p transversals, *Combinatorica,* **11** (1991), 17–22.
4. R. Meshulam, An uncertainty inequality and zero subsums, *Discr. Math.* **84** (1990), 197–200.
5. J.-P. Serre, *Linear Representations of Finite Groups,* Springer Verlag, New York, 1977.
6. K. T. Smith, The uncertainty principle on groups, IMA preprint series, 402, 1988.
7. M. Szegedy, Private communication, 1989.

Received 20 August 1991 and accepted in revised form 5 March 1992

Roy Meshulam
Department of Mathematics,
Technion,
Haifa 32000, *Israel*