The number of squares and $B_h[g]$ sets

by

BEN GREEN[1] (Cambridge)

1. Introduction. In this paper we investigate the problem of minimising, over all functions $f : \{1, \dots, N\} \to \mathbb{R}$ with $\sum_x f(x) = N$, the quantity

$$M(f) = \sum_{\substack{a,b,c,d \\ a+b=c+d}} f(a)f(b)f(c)f(d).$$

We obtain a non-trivial lower bound for $M(f)$ using techniques from Fourier analysis. We then demonstrate the relevance of this bound to upper bounds for $B_h[g]$ sets. Recall that $A \subseteq \{1, \dots, N\}$ is a $B_h[g]$-set if the number of representations of any x as $a_1 + \cdots + a_h$ (with $a_i \in A$) is at most g, where we consider two such representations to be the same if they differ only in the ordering of the summands. Letting $A(h, g, N)$ denote the size of the largest $B_h[g]$ set that one may pick from $\{1, \dots, N\}$, we prove that

$$A(3, 1, N) \leq (\tfrac{7}{2})^{1/3} N^{1/3}(1 + o(1))$$

and that

$$A(4, 1, N) \leq 7^{1/4} N^{1/4}(1 + o(1)).$$

Both of these improve on the current best-known bounds. We then obtain new bounds for $A(h, 1, N)$ when h is large. In the final part of the paper we turn our attention to bounds for $A(2, g, N)$. Using an idea from a recent paper of Cilleruelo, Ruzsa and Trujillo [3] in combination with our own approach, we improve on the best-known bounds.

2. Fourier analysis on $\mathbb{Z}_N$. We shall make substantial use of Fourier analysis. Our notation follows [5], but for the convenience of the reader we take this opportunity to give a swift introduction.

Let N be a fixed positive integer, and write $\mathbb{Z}_N$ for the cyclic group with N elements. Let ω denote the complex number $e^{2\pi i/N}$. Although ω clearly depends on N, we shall not indicate this dependence in the rest of the paper, trusting that the value of N is clear from context. Let $f : \mathbb{Z}_N \to \mathbb{C}$ be any

[1]Supported by a grant from the Engineering and Physical Sciences Research Council (EPSRC) of the United Kingdom.

function. Then for $r \in \mathbb{Z}_N$ we define the Fourier transform

$$\hat{f}(r) \;=\; \sum_{x \in \mathbb{Z}_N} f(x)\omega^{rx}.$$

We shall repeatedly use two important properties of the Fourier transform. The first is Parseval's identity, which states that if $f : \mathbb{Z}_N \to \mathbb{C}$ and $g : \mathbb{Z}_N \to \mathbb{C}$ are two functions then

$$N \sum_{x \in \mathbb{Z}_N} f(x)\overline{g(x)} \;=\; \sum_{r \in \mathbb{Z}_N} \hat{f}(r)\overline{\hat{g}(r)}.$$

The second is the interaction of *convolutions* with the Fourier transform. If $f, g : G \to \mathbb{C}$ are two functions on an abelian group G we define the convolution

$$(f * g)(x) \;=\; \sum_{y \in G} f(y)\overline{g(y-x)}.$$

A key fact, which we shall use without further comment, is that

$$(f * g)\hat{}(r) \;=\; \hat{f}(r)\overline{\hat{g}(r)}.$$

The reader will note that this is a rather non-standard definition and, in particular, that the operation we have defined is not associative. There are some situations in which it would be very tedious to indicate the intended bracketing of terms. Therefore we shall adopt the convention that

$$f_1 * f_2 * \cdots * f_k \;=\; (((f_1 * f_2) * f_3) \cdots * f_k)\,.$$

Take, for example, sets A_j $(j = 1, 2, 3)$ and identify them with their characteristic functions. Then $(A_1 * A_2 * A_3)(x)$ is simply the number of triples $(a_1, a_2, a_3) \in A_1 \times A_2 \times A_3$ with $a_1 - a_2 + a_3 = x$. We will often use the $*$ notation in contexts similar to this, and the practice of identifying a set with its characteristic function will also feature repeatedly in what follows.

If $f : G \to \mathbb{C}$ is a function then very occasionally we will write f° for the function defined by $f^\circ(x) = f(-x)$. Observe that $(A_1 * A_2^\circ)(x)$ is the number of pairs $(a_1, a_2) \in A_1 \times A_2$ with $a_1 + a_2 = x$.

One more piece of notation: throughout this paper we use O-notation for quantities varying with N, so that (for example) $X = o(1)$ means that $X \to 0$ as $N \to \infty$.

3. $B_h[g]$ **sets.** This section is a summary of the results known about

$B_h[g]$ sets up to March 2000. Other accounts may be found in [3], [6], [8] and [14].

From now on we denote by $A(h,g,N)$ the size of the largest $B_h[g]$-set contained in $\{1,\dots,N\}$, and write $A(h,1,N)=A(h,N)$ for short.

An early paper in this area was that of Erdős and Turán [4] in 1941, which is nicely exposited in [9]. This paper dealt with the problem of $B_2[1]$-sets, which are also known as B_2- or Sidon Sets. The bound

$$A(2,N) \ \leq \ N^{1/2}+N^{1/4}+1 \tag{1}$$

can be obtained from their argument. Together with a slightly earlier result of Singer, which demonstrates the existence of B_2-sets with $|A| = N^{1/2}(1+o(1))$, this provides an asymptotically correct bound for $A(2,N)$. The question of the best possible error term is an extremely interesting one, not least because no-one has managed so much as to improve the constant attached to the $N^{1/4}$ in (1). It has often been conjectured that the correct error term is $O(N^{\epsilon})$.

The situation for all other values of h and g is rather different, and in fact the correct asymptotics have not been obtained in any case. By way of lower bounds Bose and Chowla showed that $A(h,N) \geq N^{1/h}(1+o(1))$, and in a recent preprint Cilleruelo, Ruzsa and Trujillo [3] obtained good lower bounds for $A(2,g,N)$ with $g>1$.

Turning to upper bounds, a fairly simple counting argument shows that

$$A(h,g,N) \ \leq \ (gh\cdot h!)^{1/h}N^{1/h}. \tag{2}$$

We call this the trivial bound, and for the reader's convenience we sketch now the case $h=2$. Let $A\subseteq\{1,\dots,N\}$ be a $B_2[g]$-set. Observe that if $x=a_1+a_2$ with $a_i\in A$ then $1\leq x\leq 2N$. Hence by double counting ordered pairs $(a_1,a_2)\in A^2$ we find that $|A|^2\leq 2g\cdot 2N$, which translates into the trivial bound in this case, namely

$$A(2,g,N) \ \leq \ (4g)^{1/2}N^{1/2}. \tag{3}$$

These results show that $A(h,g,N)$ has order of magnitude $N^{1/h}$, so it makes sense to define

$$\alpha(h,g) \ = \ \limsup_{N\to\infty} N^{-1/h}A(h,g,N)$$

for all $h\geq 2$ and $g\geq 1$. We write $\alpha(h)=\alpha(h,1)$. The trivial bound and the Bose-Chowla theorem combine to give, in this notation,

$$1 \ \leq \ \alpha(h,g) \ \leq \ (gh\cdot h!)^{1/h}$$

and the results of Erdős – Turán and Singer show that $\alpha(2) = 1$.

Until recently the trivial bound had not been improved for any pair (h, g) with $g > 1$. However Cilleruelo, Ruzsa and Trujillo [3] show that

$$\alpha(2, g) \leq \frac{2\pi + 4}{\sqrt{\pi^2 + 4\pi + 8}} g^{1/2}. \tag{4}$$

The constant appearing here is about 1.864. For $g = 2$ Cilleruelo [2] and Helm have independently given the bound

$$\alpha(2, 2) \leq \sqrt{6}. \tag{5}$$

Cilleruelo's proof is simple and combinatorial, but only generalises to give

$$\alpha(2, g) \leq \sqrt{4g - 2},$$

a slight improvement on (3). In §8 we offer our own improvement to the upper bound (3). This improves previously known results for $g \leq 68$. Finally in §9 we combine some of our ideas with some of the ideas in [3] to improve the bound (4) for all g.

In the case $g = 1$ the situation is slightly better. Here the technique of Erdős and Turán, which gave the value of $\alpha(2)$, has a natural generalisation which gives a non-trivial upper bound for $\alpha(h)$. The first result of this kind was obtained by Lindström [12] in 1969. He showed that

$$\alpha(4) \leq 8^{1/4}. \tag{6}$$

Generalising his technique, Jia [10] obtained the bound

$$\alpha(2k) \leq \left(k(k!)^2\right)^{1/2k}. \tag{7}$$

A modification of this approach gives a corresponding bound for odd values of h. Indeed the bound

$$\alpha(2k - 1) \leq (k!)^{2/(2k-1)} \tag{8}$$

was obtained independently by Chen [1] and Graham [6]. We conclude this introduction by mentioning two further results. The first is the paper of Kolountzakis [11], in which the bound (7) is obtained by an interesting Fourier technique. We believe that this proof and that of Jia are morally the same, but the new perspective is interesting. Secondly it is worth remarking

that Graham [6] obtained a slight improvement on (8) in the case $k = 2$. He proved that

$$\alpha(3) \ \leq \ \left(4 - \tfrac{1}{228}\right)^{1/3}. \tag{9}$$

The argument is long and combinatorial.

4. Bounds for B_4 sets – the first part of the argument. In this section we begin our treatment of B_4 sets. It is hoped that, after reading this section, the reader will have a good idea of the direction in which we are headed.

Like all previous approaches, our attack takes as motivation the original argument of Erdős and Turán from 1941 [4]. We now give this argument in the form that we use to get our generalisation. We leave it as a (slightly non-trivial) exercise for the reader to check that our argument and that of [4] are really the same.

THEOREM 1 (ERDŐS – TURÁN) *For all N we have the bound*

$$A(2,N) \ \leq \ N^{1/2} + N^{1/4} + 1.$$

P r o o f. Let $A \subseteq \{1,\dots,N\}$ be a B_2-set. It is easy to check that we must have $A * A(x) \leq 1$ for all $x \neq 0$. Let u be a positive integer to be chosen later, and regard A as a subset of $\mathbb{Z}_{N+u}$. It is no longer the case that the *modular* version of $A * A$ satisfies $A * A(x) \leq 1$ for all x, but it *is* true that $A * A(x) \leq 1$ for $0 < |x| \leq u$. Let I be the characteristic function of $\{1,\dots,u\}$, and write

$$E \ = \ \sum_{x \in \mathbb{Z}_{N+u}} A * A(x) I * I(x).$$

We count E in two ways. Firstly, by the discussion above, we have

$$\begin{aligned} E \ &\leq \ |A|u + \sum_{0<|x|\leq u} A * A(x) I * I(x) \\ &\leq \ |A|u + u^2. \end{aligned}$$

Secondly, by Parseval's identity, we have

$$\begin{aligned} E \ &= \ \frac{1}{N+u} \sum_r |\hat{A}(r)|^2 |\hat{I}(r)|^2 \\ &\geq \ \frac{|A|^2 u^2}{N+u}, \end{aligned}$$

where the hat symbol denotes Fourier transform in $\mathbb{Z}_{N+u}$. Comparing these upper and lower bounds for E, and putting $u = \lfloor N^{3/4} \rfloor$, gives the result. $\Box$

An interesting feature of the argument is that we only used the fact that $A * A(x) \leq 1$ for $0 < |x| \leq N^{3/4}$, which seems to be a much weaker statement than saying that A is B_2. Somehow this fact is the major barrier to improving the error term in (1).

We now move on to B_4-sets. Let $A \subseteq \{1, \ldots, N\}$ be a B_4-set.

LEMMA 2 *For all $x \in \mathbb{Z}$ we have*

$$A * A * A * A(x) \ \leq \ 4\,(1 + |A|(A * A)(x))\,.$$

P r o o f. Fix x. The quantity $A * A * A * A(x)$ counts the number of quadruples $(a_1, a_2, b_1, b_2) \in A^4$ with

$$a_1 + a_2 - b_1 - b_2 \ = \ x. \tag{10}$$

If there are no solutions to this equation then the lemma is immediate.

We show first that if there is a solution to (10) in which $a_i \neq b_j$ for all i, j then (10) has at most 4 solutions. Indeed fix such a solution (a_1, a_2, b_1, b_2) and suppose that (a_1', a_2', b_1', b_2') is another solution. Then

$$a_1 + a_2 + b_1' + b_2' \ = \ a_1' + a_2' + b_1 + b_2.$$

But A is B_4, so the quadruples (a_1, a_2, b_1', b_2') and (a_1', a_2', b_1, b_2) are the same up to a reordering. It follows that $\{a_1', a_2'\} = \{a_1, a_2\}$ and $\{b_1', b_2'\} = \{b_1, b_2\}$, giving at most 4 possibilities.

If there is no solution of the kind discussed here then all solutions have $a_1 = b_1$, $a_1 = b_2$, $a_2 = b_1$ or $a_2 = b_2$. It is clear that, for each of these possibilities, (10) has $|A|(A * A)(x)$ solutions. Adding together everything above gives the result of the lemma. $\Box$

We remark that the important feature of the above bound is the number 4. On average, $A * A(x)$ will be tiny.

Once again we embed the problem into a cyclic group where we can take finite Fourier transforms. Let $v \leq N$ be a parameter to be chosen later, and regard A as a subset of $\mathbb{Z}_{2N+v}$ in the obvious way. Since $A + A \subseteq [1, \ldots, 2N]$, the *modular* version of $A * A * A * A$ will satisfy the bound of Lemma 2 for $|x| \leq v$. That is to say,

$$A * A * A * A(x) \ \leq \ 4\,(1 + |A|(A * A)(x)) \tag{11}$$

for $|x| \leq v$, where everything in sight lives in $\mathbb{Z}_{2N+v}$. Let $I = [1, \dots, u]$ (as a subset of $\mathbb{Z}_{2N+v}$), where $u \leq v$ is another parameter to be chosen later. It will turn out that u needs to be significantly smaller than v. For the remainder of this section the hat symbol refers to Fourier transforms on $\mathbb{Z}_{2N+v}$. Using (11) we have the following key computation.

$$\begin{aligned}
\frac{1}{2N+v}\sum_r |\hat{A}(r)|^4|\hat{I}(r)|^2 &= \sum_x (A*A*A*A)(x)(I*I)(x) \\
&\leq 4u^2 + 4|A|\sum_x (A*A)(x)(I*I)(x) \\
&= 4u^2 + \frac{4|A|}{2N+v}\sum_r |\hat{A}(r)|^2|\hat{I}(r)|^2 \\
&\leq 4u^2 + \frac{4|A|}{2N+v}|A|^2\sum_r |\hat{I}(r)|^2 \\
&= 4u^2 + \frac{4|A|}{2N+v}|A|^2(2N+v)u \\
&\leq 4u^2 + \frac{2^{24}N^{7/4}u}{2N+v}, \qquad (12)
\end{aligned}$$

where we have used the fact that $v \leq N$ and the trivial bound $|A| \leq 100N^{1/4}$. The inequality (12) gives immediately that

$$8Nu^2 + 4u^2v + 2^{24}N^{7/4}u \geq \sum_r |\hat{A}(r)|^4|\hat{I}(r)|^2. \qquad (13)$$

Using the trivial lower bound $|A|^4u^2$ for the right hand side of (13) together with $u = v = N^{7/8}$ gives the Lindström bound (6). However we are in a position to make a further improvement. The set A is extremely irregularly distributed in $\mathbb{Z}_{2N}$, being contained in $\{1, \dots, N\}$. This information allows us to say something non-trivial about $\hat{A}(r)$ when r is small and *non-zero*. Much of our paper is concerned with exactly how much it is possible to deduce from this observation as regards (13). However the reader who is keen to see an improvement of (6) as quickly as possible may care to find a positive constant c such that either $|\hat{A}(\pm 1)| \geq c|A|$ or $|\hat{A}(\pm 2)| \geq c|A|$. Since I is a rather small interval the coefficients $\hat{I}(\pm 1)$ and $\hat{I}(\pm 2)$ are as near to $|I|$ as makes no difference. Substituting into (13) and putting $u = v = N^{7/8}$ gives a bound of form

$$|A| \leq (8 - 2c^4)^{1/4}N^{1/4}(1 + o(1)).$$

5. A lower bound for the number of squares. Let $f : \{1, \dots, N\} \to \mathbb{R}$ be a function. Write $|f| = \sum_x f(x)$ and suppose that $|f| = N$. Define

the quantity $M(f)$ by

$$M(f) \;=\; \sum_{\substack{a,b,c,d\\ a+b=c+d}} f(a)f(b)f(c)f(d) \;=\; \sum_x (f*f)(x)^2 \;=\; f*f*f*f(0).$$

Since it is quite standard to refer to a quadruple of integers (a,b,c,d) with $a+b=c+d$ as a *square*, we call $M(f)$ the *number of squares* for f. Let us now introduce Fourier analysis to the study of $M(f)$. We can regard f as a subset of $\mathbb{Z}_{2N}$ in a natural way, by identifying $\{1,\dots,N\}$ with the "first half" of $\mathbb{Z}_{2N}$. Furthermore when we do this the *modular* convolution $f*f(x)$ is precisely the same as the $\mathbb{Z}$-version, since the $\mathbb{Z}$-version of $f*f$ is supported in an interval of length $2N$. It follows that

$$M(f) \;=\; \sum_{x\in\mathbb{Z}_{2N}} f*f(x)^2 \;=\; \frac{1}{2N}\sum_{r\in\mathbb{Z}_{2N}} |\hat{f}(r)|^4. \tag{14}$$

We shall be concerned with the following problem.

Problem 3 *How small can $M(f)$ be, if $|f|=N$?*

The reader who has looked at Section 4 will realise, in view of (14), the pertinence of this problem to the issue of upper bounds for B_4-sets.

To get a feel for Problem 3 we prove a few easy results.

Lemma 4 *We have $M(f)\geq N^3/2$ for all f.*

P r o o f. Observe that $\sum_x f*f(x) = N^2$ and that $f*f(x)=0$ for $x\notin\{-N+1,\dots,N-1\}$. The result is now immediate from the Cauchy-Schwarz inequality. Alternatively, the result is trivial from (14). □

Lemma 5 *We can have $M(f)\leq 2N^3/3+O(N)$.*

P r o o f. Take f to be the characteristic function of $\{1,\dots,N\}$. □

Exactly as in Section 4 we realise, on closer examination of the second argument in Lemma 4, that a lot of information has been thrown away. We have not considered any of the non-zero Fourier coefficents $\hat{f}(r)$ $(r\neq 0)$. Furthermore, since f is extremely irregularly distributed (being contained in $\{1,\dots,N\}$, which only fills half of $\mathbb{Z}_{2N}$) we have every right to expect that the contribution from these coefficients will be significant. In fact, because of the way that f is distributed, we expect the non-zero Fourier coefficients $\hat{f}(r)$ with $|r|$ very small to make a significant contribution. Our objective

now is to obtain a strong quantitative result from this observation.

Let $f : \{1, \dots, N\} \to \mathbb{R}$ be a function. Let v be a positive integer (which will be assigned various values later on) and regard f as a function on $\mathbb{Z}_{2N+v}$ in the natural way. In the following we will use the hat symbol ($\hat{}$) to denote Fourier transforms on $\mathbb{Z}_{2N+v}$. Exactly as in (14) we have

$$M(f) \;=\; \frac{1}{2N+v} \sum_r |\hat{f}(r)|^4. \tag{15}$$

The reason for introducing v will be clear to the reader who has studied §4.

Define

$$E(X) \;=\; \sum_{0<|r|\le X} |\hat{f}(r)|^4.$$

We can now state the main theorem of this section. In this theorem (and for the remainder of the section) the tilde symbol ($\tilde{}$) denotes the Fourier transform on $\mathbb{R}$. In other words if $F \in \mathcal{L}^1[0,1]$ then we write, for $\lambda \in \mathbb{R}$,

$$\tilde{F}(\lambda) \;=\; \int_{-\infty}^{\infty} F(x) e^{ix\lambda}\, dx.$$

THEOREM 6 *Let $f : \{1, \dots, N\} \to \mathbb{R}$ be a function with $|f| = N$, and let v, X be positive integers. Let f be regarded as a function on $\mathbb{Z}_{2N+v}$ in the natural way, and let the hat symbol denote Fourier transforms on that group. Let $p \in \mathcal{C}^1[0,1]$ be such that*

$$\int_0^1 p(x)\, dx \;=\; 2.$$

Then there is a constant C, depending only on p, such that

$$E(X) \;\ge\; \gamma(p) N^4 \left(1 - C\left(\frac{v}{N} + \frac{N^2}{v^2 X} + \frac{X^2}{N}\right)\right),$$

where

$$\gamma(p) \;=\; 2\left(\sum_{r\ge 1} |\tilde{p}(\pi r)|^{4/3}\right)^{-3}.$$

P r o o f. We remark that, for suitable choices of v and X, the dominant term in the above bound will be $\gamma(p)N^4$. Throughout this proof C will denote a constant which depends only on the fixed function p. We follow the traditional convention in analytic number theory of allowing the same

letter C to denote different constants!

For $x \in [0,2]$ define

$$U(x) \;=\; \begin{cases} 1 & (0 \le x < 1) \\ 1 - p(x-1) & (1 \le x < 2), \end{cases} \tag{16}$$

and set, for $x \in \mathbb{Z}_{2N+v}$,

$$G(x) \;=\; U\left(\frac{x}{N+\frac{v}{2}}\right). \tag{17}$$

Let I be the characteristic function of the interval $\{1, \dots, \frac{v}{4}\}$ and write

$$H(x) \;=\; \left(\frac{4}{v}\right)^2 G * (I * I)(x). \tag{18}$$

The idea here is that G is a discretised version of U, and H is a smoothed version of G. Observe that G is equal to 1 for $x = 1, \dots, N + \frac{v}{2}$, and that $I * I$ is supported in $\{-v/4, v/4\}$. Therefore H is equal to 1 for $x = \frac{v}{4}, \dots, N + \frac{v}{4}$. It follows that

$$\sum_x f(x) H\left(x + \frac{v}{4}\right) \;=\; N.$$

Applying Parseval's identity and the triangle inequality gives

$$\sum_r |\hat{f}(r)||\hat{H}(r)| \;\ge\; 2N^2. \tag{19}$$

In order to use this we require a variety of estimates for $\hat{H}(r)$. These will be of two forms. The first estimate says that, when $|r|$ is small, $\hat{H}(r)$ can be estimated by approximating the sum

$$\hat{H}(r) \;=\; \sum_x H(x)\omega^{rx}$$

by an integral. Observe that here we are using ω to denote the quantity $e^{\frac{2\pi i}{2N+v}}$, because we are working with the group $\mathbb{Z}_{2N+v}$. The second estimate tells us that $\hat{H}(r)$ is small when $|r|$ is at all large. It is for the purpose of proving such a result that we are using the smoothed function H rather than G.

LEMMA 7 *Let $r : [0,1] \to \mathbb{R}$ be piecewise continuously differentiable, and let M be an integer. Then*

$$\left| \int_0^1 r(x)\,dx \;-\; \frac{1}{M} \sum_{0 \le n < M} r\left(\frac{n}{M}\right) \right| \;\le\; \frac{\|r'\|_\infty}{M}.$$

P r o o f. This is just an easy application of the Fundamental Theorem of Calculus. □

Observe that

$$|\hat{H}(r)| \;=\; \left(\frac{4}{v}\right)^2 |\hat{G}(r)||\hat{I}(r)|^2. \tag{20}$$

It follows that $|\hat{H}(r)| \leq |\hat{G}(r)|$ for all r. Furthermore when $r \neq 0$ we have

$$|\hat{G}(r)| \;=\; \left| \sum_{0 \leq x < N + \frac{v}{2}} p\left(\frac{x}{N+\frac{v}{2}}\right) \omega^{rx} \right|.$$

Hence, using this and Lemma 7 with $r(x) = p(x)e^{\pi i r x}$ and $M = N + \frac{v}{2}$ gives us what we called our first estimate.

LEMMA 8 *Let $0 < |r| < N + \frac{v}{2}$. Then we have the inequality*

$$|\hat{H}(r)| \;\leq\; |\hat{G}(r)| \;\leq\; (N+v)|\tilde{p}(\pi r)| + C|r|.$$

P r o o f. Indeed we can take $C = 4\left(\|p'\|_\infty + \|p\|_\infty\right)$. □

It is possible to prove by very similar means that

$$|\hat{H}(0)| \;\leq\; C. \tag{21}$$

We now turn our attentions to estimating $|\hat{H}(r)|$ for large $|r|$. To this end recall (20). It follows immediately from Lemma 8 that there is a constant C such that

$$|\hat{G}(r)| \;\leq\; CN \tag{22}$$

for all $|r| \leq N + \frac{v}{2}$. We shall also require an upper bound for $|\hat{I}(r)|$.

LEMMA 9 *Let $0 < |r| \leq N + \frac{v}{2}$. Then*

$$|\hat{I}(r)| \;\leq\; \frac{3N}{|r|}.$$

P r o o f. By summing a geometric progression it is easy to see that

$$\begin{aligned} |\hat{I}(r)| \;&\leq\; \frac{2}{|\omega^r - 1|} \\ &=\; \left(\sin\left(\frac{\pi r}{2N+v}\right)\right)^{-1}. \end{aligned}$$

It is also a simple matter to verify, for $\theta \in [-\pi/2, \pi/2]$, the inequality

$$|\sin\theta|^{-1} \ \leq \ |\theta|^{-1} + 1.$$

The lemma follows immediately. □

LEMMA 10 *There is a constant C such that*

$$|\hat{H}(r)| \ \leq \ \frac{CN^3}{v^2|r|^2}.$$

P r o o f. This follows quickly from (20), (22) and the previous lemma. □

Using Lemma 10 and the fact that $|f| = N$, we get that

$$\sum_{|r|>X} |\hat{f}(r)||\hat{H}(r)| \ \leq \ \frac{CN^4}{v^2X}.$$

Using this and (21) it follows from (19) that

$$\sum_{0<|r|\leq X} |\hat{f}(r)||\hat{H}(r)| \ \geq \ 2N^2\left(1 - C\left(\frac{1}{N} + \frac{N^2}{v^2X}\right)\right).$$

Bringing Lemma 8 to bear on this gives, after a little calculation,

$$\sum_{0<|r|\leq X} |\hat{f}(r)||\tilde{p}(\pi r)| \ \geq \ 2N\left(1 - C\left(\frac{v}{N} + \frac{N^2}{v^2X} + \frac{X^2}{N}\right)\right). \tag{23}$$

Since both f and p are real-valued we have that $|\hat{f}(r)| = |\hat{f}(-r)|$ and $|\tilde{p}(\pi r)| = |\tilde{p}(-\pi r)|$ for all r. Therefore (23) implies that

$$\sum_{1\leq r\leq X} |\hat{f}(r)||\tilde{p}(\pi r)| \ \geq \ N\left(1 - C\left(\frac{v}{N} + \frac{N^2}{v^2X} + \frac{X^2}{N}\right)\right). \tag{24}$$

The proof of Theorem 6 can now be concluded by a single application of Hölder's Inequality with exponents $(4, 4/3)$. □

Apart from the problem of choosing a suitable function p, we can use Theorem 6 to get a lower bound for $M(f)$.

THEOREM 11 *Let $f : \{1, \ldots, N\} \to \mathbb{R}$ be a function with $|f| = N$. Let $p \in \mathcal{C}^1[0,1]$ be such that*

$$\int_0^1 p(x)\,dx \ = \ 2.$$

Then

$$M(f) \;\geq\; \left(\frac{1+\gamma(p)}{2}\right) N^3(1+O(N^{-1/7})),$$

where

$$\gamma(p) \;=\; 2\left(\sum_{r\geq 1} |\tilde{p}(\pi r)|^{4/3}\right)^{-3}.$$

P r o o f. Recall (15). Using this and Theorem 6 with $v = N^{6/7}$, $X = N^{3/7}$ gives the result. □

It only remains to choose a good function p, where "good" means that $\int_0^1 p(x)\,dx$ equals 2 and $\gamma(p)$ is as large as possible. Unfortunately we have not been able to give a best possible choice in closed form. A simple function that gives a good bound is

$$p(x) \;=\; \tfrac{5}{2} - 40\left(x-\tfrac{1}{2}\right)^4. \tag{25}$$

One can compute that

$$|\tilde{p}(\pi r)| \;=\; \begin{cases} \dfrac{40}{\pi^2|r|^2} - \dfrac{960}{\pi^4|r|^4} & r \text{ even}, r\neq 0 \\ \dfrac{240}{\pi^3|r|^3} - \dfrac{1920}{\pi^5|r|^5} & r \text{ odd}, \end{cases} \tag{26}$$

and then that

$$\gamma(p) \;=\; \frac{2\left(\frac{\pi^2}{40}\right)^4}{\left(S_1 + \left(\frac{6}{\pi}\right)^{4/3} S_2\right)^3}, \tag{27}$$

where

$$S_1 \;=\; \sum_{\substack{r\,\text{even}\\ r\geq 0}} \left|\frac{1}{r^2} - \frac{24}{\pi^2 r^4}\right|^{4/3} \tag{28}$$

and

$$S_2 \;=\; \sum_{\substack{r\,\text{odd}\\ r\geq 0}} \left|\frac{1}{r^3} - \frac{8}{\pi^2 r^5}\right|^{4/3}. \tag{29}$$

There seems to be little hope of an analytic expression for these series, but one can compute that $S_1 \approx 0.0839757$, $S_2 \approx 0.1219299$. It then follows from

(27) that $\gamma(p) > 1/7$ (in fact it turns out that $\gamma(p) \approx 1/6.9994$).

To conclude this section we restate Theorems 6 and 11 with this particular choice of p.

THEOREM 12 *Let $f : \{1, \dots, N\} \to \mathbb{R}$ be a function with $|f| = N$, and let v, X be positive integers. Let f be regarded as a function on $\mathbb{Z}_{2N+v}$ in the natural way, and let the hat symbol denote Fourier transforms on that group. Write*

$$E(X) \ = \sum_{0<|r|<X} |\hat{f}(r)|^4.$$

Then there is an absolute constant C such that

$$E(X) \ \geq \ \tfrac{1}{7}N^4 \left(1 - C\left(\frac{v}{N} + \frac{N^2}{v^2 X} + \frac{X^2}{N}\right)\right).$$

THEOREM 13 *Let $f : \{1, \dots, N\} \to \mathbb{R}$ be a function with $|f| = N$. Then we have*

$$M(f) \ \geq \ \tfrac{4}{7}N^3$$

for all sufficiently large N.

6. A return to B_4 sets. Recall that our knowledge of B_4 sets is currently encapsulated in (13), which we urge the reader to reconsider now. In the remarks following that equation we stated that our goal would be to say something about the Fourier coefficients $\hat{A}(r)$ with r non-zero and small. We now have this knowledge, in the form of Theorem 12.

In (13) we must contend with the presence of $|\hat{I}(r)|^2$. Notice, however, that $|\hat{I}(r)|$ will differ insignificantly from u if $|r| \ll N/u$. Indeed

LEMMA 14

$$|\hat{I}(r)| \ \geq \ u - \frac{\pi|r|u^2}{N}.$$

P r o o f. Let $\omega = e^{2\pi i/(2N+v)}$. Then we have

$$\left|u - \hat{I}(r)\right| \ \leq \ \sum_{x=1}^{u} |1 - \omega^{rx}| \ \leq \ \frac{2\pi|r|u^2}{2N+v} \ \leq \ \frac{\pi|r|u^2}{N},$$

which is all we need. □

Applying Theorem 12 with $f(x) = NA(x)/|A|$ gives

$$\begin{aligned}\sum_r |\hat{A}(r)|^4|\hat{I}(r)|^2 &\geq \sum_{|r|\leq X} |\hat{A}(r)|^4|\hat{I}(r)|^2 \\ &\geq \tfrac{8}{7}u^2|A|^4\left(1 - C\left(\frac{v}{N} + \frac{N^2}{v^2X} + \frac{X^2}{N}\right)\right)\left(1 - \frac{\pi Xu}{N}\right)^2,\end{aligned}$$

where C is an absolute constant. From (13) we now have

$$8N + 2^{24}\left(v + \frac{N^{7/4}}{u}\right) \geq \tfrac{8}{7}|A|^4\left(1 - C\left(\frac{v}{N} + \frac{N^2}{v^2X} + \frac{X^2}{N} + \frac{Xu}{N}\right)\right). \quad (30)$$

We must now choose suitable values for u, v and X, recalling that we require $u \leq v$. There are many such choices and one is $u = N^{13/17}$, $v = N^{16/17}$, $X = N^{3/17}$. With these values in (30) we get

THEOREM 15

$$A(4, N) \leq 7^{1/4}N^{1/4}(1 + o(1)).$$

We now turn our attention to B_3-sets. We shall be very brief here as there very little difference between this and the case of B_4-sets.

LEMMA 16 *Let $A \subseteq \{1, \ldots, N\}$ be a B_3-set. Then*

$$A * A * A * A(x) \leq 2|A|(1 + (A * A)(x)).$$

P r o o f. A counting argument very similar to that in Lemma 2 gives

$$A * A * A(x) \leq 2(1 + |A|A(x)).$$

Using the fact that

$$A * A * A * A(x) = \sum_y (A * A * A)(y)A(y - x),$$

the lemma follows immediately. □

The remainder of the derivation is almost exactly as before. One winds up with

THEOREM 17

$$A(3, N) \leq \left(\tfrac{7}{2}\right)^{1/3} N^{1/3}(1 + o(1)).$$

7. Large values of h. In this section we again consider upper bounds for B_h-sets. Our aim is to convince the reader that the methods we have just been using for B_3 and B_4 sets generalise rather easily to the case $h \geq 5$. For any given value of $h \geq 5$, the difficulties we have experienced optimising our approach (i.e. choosing a good function p) are even more apparent. Therefore we shall not, in the sequel, discuss any such specific value of h. Rather we shall turn our attention to the behaviour of our methods as h becomes large. It turns out that rather simple ideas constitute essentially the best possible application of the methods of this paper.

Let $f : G \to \mathbb{R}$ be a function on an abelian group G. Then throughout this section we will write f^{*k} for the k-fold convolution of f with itself.

The following proposition, a sort of generalisation of Theorem 12, will be our main tool. This comes as little surprise.

PROPOSITION 18 *Let k be a positive integer. Let $f : \{1, \dots, N\} \to \mathbb{R}^+$ be a function, and regard f as a function on $\mathbb{Z}_{kN+v}$ in the natural way. Here k is to be regarded as fixed (but large), and N, v are positive integers with $v \ll N$. Then we have*

$$\sum_{|r| \leq k/2} |\hat{f}(r)|^{2k} \;\geq\; \frac{1}{\sqrt{\pi}} k^{1/2} (1 - \varepsilon(k)) |f|^{2k}, \tag{31}$$

where $\varepsilon(k) \to 0$ as $k \to \infty$.

P r o o f. The idea is rather simple, but (as the form of (31) might suggest) some fairly careful analysis is required. Throughout the following k will be taken sufficiently large. We have

$$\begin{aligned} |\hat{f}(r)| &= \left| \sum_x f(x) \omega^{r\left(x - \frac{N}{2}\right)} \right| \\ &\geq \sum_x f(x) \cos\left(\frac{2\pi r \left(x - \frac{N}{2}\right)}{kN + v} \right). \end{aligned}$$

Therefore if $|r| \leq k/2$ we have

$$|\hat{f}(r)| \;\geq\; |f| \cos\left(\frac{\pi r}{k}\right).$$

Now we simply compute

$$\begin{aligned} |f|^{-2k} \sum_{|r|\le k/2} |\hat{f}(r)|^{2k} &\ge \sum_{|r|\le k/2} \left|\cos \frac{\pi r}{k}\right|^{2k} \\ &\ge \sum_{|r|\le k^{5/8}} \left|1 - \frac{\pi^2 r^2}{2k^2}\right|^{2k} \\ &\ge \left|1 - \frac{25}{k^{3/2}}\right|^{2k} \sum_{|r|\le k^{5/8}} e^{-\pi^2 r^2/k}. \end{aligned}$$

In this last step we have used the inequality

$$1 - x \ \ge \ e^{-x}(1 - x^2),$$

which holds for $x \le 1$. Now one observes that

$$\left|1 - \frac{25}{k^{3/2}}\right|^{2k} \longrightarrow 1$$

as $k \to \infty$, and that

$$\frac{1}{\sqrt{k}} \sum_{|r|\le k^{5/8}} e^{-\pi^2 r^2/k} \longrightarrow \int_{-\infty}^{\infty} e^{-\pi^2 x^2}\, dx \ = \ \frac{1}{\sqrt{\pi}}.$$

The proposition now follows. The conscientious reader may care to check that we can even take $\varepsilon(k) = 100k^{-1/8}$. □

Interestingly the above is essentially best possible. We take the opportunity to sketch a proof of this fact now.

Proposition 19 *The bound of Proposition 18 is best possible in that the constant $1/\sqrt{\pi}$ cannot be increased.*

S k e t c h P r o o f. Let $\delta > 0$ and let χ be the characteristic function of the set A_δ, which consists of the integers $n \in \{-N/2, \dots, N/2\}$ with $|n| \ge (1-\delta)N/2$. Let $f(n) = \delta^{-1}\chi(n)$, so that $|f| = N(1 + o(1))$. For $x \in [-1/2, 1/2]$ define

$$g(x) \ = \ \begin{cases} \delta^{-1} & (|x| \ge (1-\delta)/2) \\ 0 & (\text{otherwise}) \end{cases}$$

Now g is the probability density function of a random variable X with mean 0 and variance

$$\sigma^2 \ = \ \frac{1 - (1-\delta)^3}{12\delta} \ > \ \tfrac{1}{4}(1-\delta). \tag{32}$$

Let $\{X_i\}_{i=1}^{\infty}$ be a sequence of independent identically distributed random variables with density g. Then, by a suitable version of the Central Limit Theorem (see [7]), the density function of

$$\frac{X_1 + \cdots + X_m}{\sigma\sqrt{m}}$$

tends to the standard normal $\frac{1}{\sqrt{2\pi}}e^{-x^2/2}$ uniformly in x. In other words,

$$\sqrt{m} \cdot g^{*m}(x\sigma\sqrt{m}) \longrightarrow \frac{1}{\sigma\sqrt{2\pi}}e^{-x^2/2}$$

uniformly in x. In particular for $m \geq m(\delta)$ we have, using (32), that

$$g^{*m}(0) \ \leq \ \sqrt{\frac{2}{m\pi(1-\delta)}}. \tag{33}$$

Now let k be a fixed positive integer, and regard f as a function on $\mathbb{Z}_{kN}$ in the natural way (in Proposition 18 we worked with $\mathbb{Z}_{kN+v}$, but we choose to ignore this technicality here). Using the hat symbol to denote Fourier transforms on this group, we have

$$\begin{aligned} \sum_r |\hat{f}(r)|^{2k} &= kN \sum_x |f^{*k}(x)|^2 \\ &= kN|f^{*2k}(0)|. \end{aligned} \tag{34}$$

Note that the modular version of $|f^{*2k}(0)|$ is the same as the $\mathbb{Z}$-version because f is supported in $\{-N/2, N/2\}$. It is thus not hard to see that, as $N \to \infty$, we have

$$\frac{f^{*2k}(0)}{N^{2k-1}} \longrightarrow g^{*2k}(0).$$

It follows from (34) that

$$|f|^{-2k} \sum_r |\hat{f}(r)|^{2k} \longrightarrow k g^{*2k}(0),$$

again as $N \to \infty$. If $2k \geq m(\delta)$ (as defined earlier) then this implies, by (33), that

$$|f|^{-2k} \sum_r |\hat{f}(r)|^{2k} \ \leq \ \sqrt{\frac{k}{\pi(1-2\delta)}}$$

for N sufficiently large. Since δ can be chosen arbitrarily small, the proposition follows. $\square$

We turn now to the business of actually using Proposition 18 to get information about B_h sets. We shall be extremely brief, as almost all of the relevant ideas have been covered in §4 (which it may help to recall at this point). First of all we require generalisations of Lemmas 2 and 16.

LEMMA 20 *Let $h = 2k$ be a positive even integer, and let $A \subseteq \{1, \dots, N\}$ be a B_h-set. Then, for any $x \in \mathbb{Z}$, we have that*

$$A^{*2k}(x) \ \leq \ (k!)^2 + k^2|A|A^{*(2k-2)}(x).$$

LEMMA 21 *Let $h = 2k-1$ be a positive odd integer, and let $A \subseteq \{1, \dots, N\}$ be a B_h-set. Then, for any $x \in \mathbb{Z}$, we have that*

$$A^{*2k}(x) \ \leq \ |A| \left(k!(k-1)! + k(k-1)A^{*(2k-2)}(x)\right).$$

Regard A as a subset of $\mathbb{Z}_{kN+v}$, and let I be the characteristic function of $\{1, \dots, u\}$ where $u \ll v \ll N$. In the case $h = 2k$, an appropriate generalisation of (13) (which may be proved in exactly the same way) is

$$k(k!)^2Nu^2 + (2k+4)!\left(N^{2-1/2k}u + u^2v\right) \ \geq \ \sum_r |\hat{A}(r)|^{2k}|\hat{I}(r)|^2.$$

Applying Proposition 18 and Lemma 14 quickly gives

$$k(k!)^2N + (2k+4)!\left(\frac{N^{2-1/2k}}{u} + v\right) \\ \geq \ \frac{1}{\sqrt{\pi}}k^{1/2}(1-\varepsilon(k))|A|^{2k}\left(1 - \frac{\pi ku}{N}\right)^2,$$

where here (and in the following) $\varepsilon(k) \to 0$ as $k \to \infty$. Taking $u = N^{1-1/3k}$ and $v = N^{1-1/4k}$ gives the following improvement of (7).

THEOREM 22

$$\alpha(2k) \ \leq \ \left(\pi^{1/2}k^{1/2}(k!)^2(1+\varepsilon(k))\right)^{1/2k}.$$

The case $h = 2k-1$ may be treated similarly and one winds up with

THEOREM 23

$$\alpha(2k-1) \ \leq \ \left(\pi^{1/2}k^{-1/2}(k!)^2(1+\varepsilon(k))\right)^{1/(2k-1)}.$$

8. New bounds for $B_2[g]$-sets part I. In this section we apply the results of §5 to the problem of bounding $\alpha(2,g)$ above. We show that our ideas lead to a non-trivial bound which is stronger than that of [3] for $g \leq 68$. Let $A \subseteq \{1,\dots,N\}$ be a $B_2[g]$-set. Let $0 < v \leq N$ be an integer to be chosen later, and regard A as a subset of $\mathbb{Z}_{2N+v}$ in the obvious way. Then we have

$$M(A) \;=\; \sum_x (A*A^\circ)(x)^2 \;\leq\; 2g\sum_x (A*A^\circ)(x) \;=\; 2g|A|^2. \tag{35}$$

On the other hand, using the hat symbol to denote Fourier transforms in $\mathbb{Z}_{2N+v}$, we have

$$(2N+v)M(A) \;=\; \sum_r |\hat{A}(r)|^4. \tag{36}$$

Now let X be another positive integer to be chosen later, and split the sum in (36) into the two parts

$$\Sigma_1 \;=\; \sum_{|r|\leq X} |\hat{A}(r)|^4$$

and

$$\Sigma_2 \;=\; \sum_{X<|r|\leq N+\frac{v}{2}} |\hat{A}(r)|^4.$$

Applying Proposition 12 with $f(x) = NA(x)/|A|$ gives

$$\Sigma_1 \;\geq\; \tfrac{8}{7}|A|^4\left(1 - \frac{C}{N}\left(v + \frac{N^3}{v^2X} + X^2\right)\right). \tag{37}$$

Furthermore by the Cauchy-Schwarz inequality, Parseval's identity and the trivial bound $|A| \leq (4g)^{1/2}N^{1/2}$ we have

$$\begin{aligned}
\Sigma_2 \;&\geq\; \frac{1}{2N+v}\left(\sum_{X<|r|\leq N+\frac{v}{2}} |\hat{A}(r)|^2\right)^2 \\
&\geq\; \frac{1}{2N+v}\left((2N+v)|A| - 2X|A|^2\right)^2 \\
&\geq\; (2N+v)\left(|A| - 12gX\right)^2. \qquad (38)
\end{aligned}$$

Taking $X = N^{3/7}$, $v = N^{6/7}$ in the above and doing a little calculation with (35), (36), (37) and (38) gives the following result.

THEOREM 24 *We have*

$$\alpha(2,g) \ \leq \ \sqrt{\tfrac{7}{2}g - \tfrac{7}{4}}.$$

This improves on the bound of [3] *for* $g \leq 68$*, and in particular*

$$\alpha(2,2) \ \leq \ \tfrac{1}{2}\sqrt{21}.$$

9. New Bounds for $B_2[g]$-sets part II. In this section we discuss the paper [3]. We begin by translating the techniques of that paper into the language we have been using here, a relatively easy task. We then show that our methods complement those of [3], in the sense that we can get an improved bound on $A(2,g,N)$. We shall in fact prove the following result.

THEOREM 25

$$A(2,g,N) \ \leq \ \left(\tfrac{17}{5}\right)^{1/2} g^{1/2}N^{1/2}(1+o(1)).$$

Observe that $(17/5)^{1/2} = 1.84391..$ (in fact our method gives the slightly better constant 1.84385). This is weaker than the bound of Theorem 24 for $g \leq 18$, but stronger than the bound of [3] for all g. We give this bound more as an illustration of the sort of techniques that might be useful in this problem rather than for the constant 17/5 itself.

We now translate the technique used in [3] to obtain the bound (4) into the language of our paper. Let $A \subseteq \{1,\dots,N\}$ be a $B_2[g]$ set, and regard A as a subset of $\mathbb{Z}_{2N}$. Define $f(x) = 2g - (A*A^\circ)(x)$, so that $0 \leq f(x) \leq 2g$ for all $x \in \mathbb{Z}_{2N}$. For any $r \neq 0$ the Fourier transform $\hat{f}(r)$ is simply $-\hat{A}(r)^2$. Hence we have, if $\omega = e^{2\pi i/2N}$,

$$\begin{aligned} |\hat{A}(r)|^2 &= \left|\sum_x (2g - (A*A^\circ)(x))\,\omega^{rx}\right| \\ &\leq \sum_x |2g - (A*A^\circ)(x)| \\ &= 4Ng - |A|^2. \end{aligned} \tag{39}$$

Noting that $A \subseteq \{1,\dots,N\}$, Cilleruelo, Ruzsa and Trujillo show that A must have a large non-zero Fourier coefficient $\hat{A}(r)$. The technique used to do this bears some resemblance to the techniques we used earlier to show that, under the same hypotheses, $\sum_{r\neq 0}|\hat{A}(r)|^4$ cannot be too small. One finds a non-negative function f, supported on $\{1,\dots,N\}$, for which $\sum_{r\neq 0}|\hat{f}(r)|$ is large compared to $|f|$. Observing that

$$\sum_x A(x)f(x+N) \ = \ 0,$$

one uses Parseval's identity to conclude that

$$\sum_{r\neq 0} |\hat{A}(r)||\hat{f}(r)| \;\geq\; |A||f|,$$

from which it follows that

$$\sup_{r\neq 0} |\hat{A}(r)| \cdot \sum_{r\neq 0} |\hat{f}(r)| \;\geq\; |A||f|.$$

We suppress a more detailed discussion, referring the interested reader to [3].

For the rest of the paper define

$$N_\infty(A) \;=\; \frac{1}{|A|} \sup_{r\neq 0} |\hat{A}(r)|$$

and

$$N_4(A) \;=\; \frac{1}{|A|^4} \sum_{r\neq 0} |\hat{A}(r)|^4.$$

The situation may be summarised by saying that [3] obtains information from $N_\infty(A)$, whereas we profited from consideration of $N_4(A)$. Since these are rather different objects, it is not altogether surprising that a stronger bound can be achieved by playing the two approaches off against one another. The remainder of the paper, which aims to show that this is indeed so, consists of three parts. In Step 1 we show that a lower bound on $N_\infty(A)$ can be used slightly more effectively than was done in (39). In Step 2 we show how a lower bound on $N_4(A)$ gives information in a rather simpler (but slightly weaker) way than in §8. This keeps the whole argument manageable. Finally, in Step 3, we show that considering $N_\infty(A)$ and $N_4(A)$ together gives stronger information, for large g, than separate consideration of either $N_\infty(A)$ (cf. [3]) or $N_4(A)$ (cf. §8).

Step 1. Let us reconsider the derivation (39). There was only one inequality, but it was rather crude. Our task here is to improve it.

LEMMA 26 *Let L, M, R be integers with $L+1 \leq M/R$. Let $\mathcal{C}(M,R)$ be the set of all functions $f : \mathbb{Z}_L \to \{0,1,2,\dots\}$ with $|f| = M$ and $f(x) \leq R$ for all x. Then, for all $f \in \mathcal{C}(M,R)$,*

$$|\hat{f}(1)| \;\leq\; R \left| \frac{\sin \frac{\pi}{L}\left(\frac{M}{R}+1\right)}{\sin \frac{\pi}{L}} \right|.$$

P r o o f. The result clearly generalises to $|\hat{f}(r)|$ with $r \neq 0$. It is saying nothing more than that $|\hat{f}(1)|$ is maximised, among all functions in $\mathcal{C}(M,R)$, when f is as concentrated as possible. We prove this using a sort of compression argument. Let f be a member of $\mathcal{C}(M,R)$ with $|\hat{f}(1)|$ maximal. Let $u, v \in \mathbb{Z}_L$ be such that $f(u) > 0$ and $f(v) < M$, and define a new function $g_{u,v} \in \mathcal{C}(M,R)$ by

$$\begin{array}{rcll} g(x) & = & f(x) & (x \neq u, v) \\ g(u) & = & f(u) - 1 & \\ g(v) & = & f(v) + 1. & \end{array}$$

Let $\omega = e^{2\pi i/L}$ and suppose that $a \in [0, L)$ is such that $\hat{f}(1) = |\hat{f}(1)|\omega^{ra}$ (a need not be an integer). Then one can check that

$$\begin{aligned} |\hat{g}(1)| &= \left| |\hat{f}(1)| + \omega^{v-a} - \omega^{u-a} \right| \\ &\geq |\hat{f}(1)| + \cos\left(\frac{2\pi(v-a)}{L}\right) - \cos\left(\frac{2\pi(u-a)}{L}\right). \end{aligned}$$

In words, $|\hat{g}(1)|$ is greater than $|\hat{f}(1)|$ if $|v-a| < |u-a|$, where distance is measured on the torus $[0, L)$ which contains $\mathbb{Z}_L$ as a subgroup. By the extremal property of f, this means that we cannot select u and v with $|v-a| < |u-a|$, $f(u) > 0$ and $f(v) < M$. In other words f is as concentrated about a as possible. □

We can now use this lemma in place of the inequality (39), with $f(x) = 2g - (A * A^\circ)(x)$, $L = 2N$ and $M = 2g$. One gets for any $r \neq 0$ that

$$|\hat{A}(r)|^2 \leq 2g \left| \frac{\sin \frac{\pi}{2N}\left(\frac{4Ng - |A|^2}{2g} + 1\right)}{\sin \pi/2N} \right|.$$

Writing (here and for the rest of the paper)

$$Q = \frac{|A|^2}{4Ng},$$

this simplifies to

$$|\hat{A}(r)|^2 \leq 2g \left| \frac{\sin\left(\pi Q - \frac{\pi}{2N}\right)}{\sin(\pi/2N)} \right|.$$

Recalling that $Q < 1$ uniformly in N (a consequence of Theorem 24) this reduces yet further to give

$$|\hat{A}(r)|^2 \leq \frac{4gN \sin \pi Q}{\pi}(1 + o(1)).$$

Finally this implies our strengthened version of (39), namely

$$\frac{\sin \pi Q}{\pi Q} \ \geq \ N_\infty(A)^2(1+o(1)). \tag{40}$$

Step 2. In this brief section we show that upper bounds for $B_2[g]$ sets are related to lower bounds for $N_4(A) = \sum_{r\neq 0} |\hat{A}(r)|^4/|A|^4$ in a very simple way (which is a little weaker than the approach taken in §8). Let $A \subseteq \{1,\dots,N\}$ be a $B_2[g]$ set and regard A as a subset of $\mathbb{Z}_{2N}$. Then

$$\begin{aligned} |A|^4(1+N_4(A)) &= \sum_r |\hat{A}(r)|^4 \\ &= 2N\sum_x (A*A^\circ)(x)^2 \\ &\leq 4Ng\sum_x (A*A^\circ)(x) \\ &= \frac{|A|^4}{Q}. \end{aligned}$$

Hence

$$Q \ \leq \ \frac{1}{1+N_4(A)}\,. \tag{41}$$

Step 3. Unfortunately this section is a touch computational. We trust the reader will accept our apologies for this. At this point we take the opportunity to recall equation (24), from which we deduced Theorem 6 by a simple application of Hölder's Inequality. Let $f : \{1,\dots,N\} \to \mathbb{R}$ be a function with $|f| = N$, and regard f as a function on $\mathbb{Z}_{2N+v}$. Let $p : [0,1] \to \mathbb{R}$ be a continuously differentiable function with $\int_0^1 p(x)\,dx = 2$. Then, using the hat and tilde symbols to denote Fourier transforms on $\mathbb{Z}_{2N+v}$ and $\mathbb{R}$ respectively, we had

$$\sum_{1\leq r\leq X} |\hat{f}(r)||\tilde{p}(\pi r)| \ \geq \ N\left(1 - C\left(\frac{v}{N} + \frac{N^2}{v^2X} + \frac{X^2}{N}\right)\right). \tag{42}$$

Take $f(x) = NA(x)/|A|$ and $p(x) = \frac{5}{2} - 40\left(x - \frac{1}{2}\right)^4$ (as we did in proving Theorem 6). With $X = N^{3/7}$ and $v = N^{6/7}$, (42) gives

$$\sum_{1\leq r<N} |\hat{A}(r)||\tilde{p}(\pi r)| \ \geq \ |A|(1+o(1)). \tag{43}$$

Suppose that $|\hat{A}(1)| = \alpha|A|$. Then, recalling (26), we get that

$$\sum_{2\le r<N} |\hat{A}(r)||\tilde{p}(\pi r)| \ \ge \ |A|\left(1-\alpha\left(\frac{240}{\pi^3}-\frac{1920}{\pi^5}\right)\right)(1+o(1)). \tag{44}$$

Suppose that $\alpha < \frac{7}{10}$, so that

$$1-\alpha\left(\frac{240}{\pi^3}-\frac{1920}{\pi^5}\right) \ \ge \ 0.$$

Then we may apply Hölder's Inequality to (44) to obtain, after a few calculations, that

$$N_4(A) \ \ge \ \left(2\alpha^4+\frac{2\left(\frac{\pi^3}{240}\right)^4\left(1-\alpha\left(\frac{240}{\pi^3}-\frac{1920}{\pi^5}\right)\right)^4}{\left(\left(\frac{\pi}{6}\right)^{4/3}S_1+S_2-\left(1-\frac{8}{\pi^2}\right)^{4/3}\right)^3}\right)(1+o(1)) \tag{45}$$

$$\approx \ \left(2\alpha^4+4.8607836\,(1-1.4662621\alpha)^4\right)(1+o(1)), \tag{46}$$

where S_1 and S_2 are the sums appearing in (28) and (29). Call the polynomial appearing in (46) $p(\alpha)$. Then one can check that $p'(\alpha) < 0$ for $\alpha \in [0, 0.47]$. Hence, putting $\alpha = 0.4124078$ in (46), we get that either

$$N_\infty(A) \ \ge \ \frac{|\hat{A}(1)|}{|A|} \ \ge \ 0.4124078 \tag{47}$$

or else

$$N_4(A) \ \ge \ 0.1765468\,(1+o(1)). \tag{48}$$

If (48) holds then, by (41), we have

$$Q \ \le \ 0.8499448\,(1+o(1)).$$

If (47) holds then, by (40) and a little easy computation we have again that

$$Q \ \le \ 0.8499448\,(1+o(1)).$$

Either way, it is easy to see (recalling that $Q = |A|^2/4Ng$) that Theorem 25 is true. □

10. Concluding remarks on $B_h[g]$ sets. In this paper we have been concerned only with the problem of finding upper bounds for $B_h[g]$-subsets of $\{1,\dots,N\}$. However the notion of $B_h[g]$-set makes sense on any subset

of an abelian group and perhaps the most natural questions concern $B_h[g]$-subsets of $\mathbb{Z}_N$. Indeed one feels that in passing from $\mathbb{Z}_N$ to $\{1,\dots,N\}$ one has somehow only introduced "boundary effects" that should have little bearing on the apparently deeper underlying arithmetic questions. Our work in this paper has been concerned with improving the estimates for these boundary effects, and unfortunately our methods are unable to give any new information about $B_h[g]$-subsets of $\mathbb{Z}_N$. Let $M(h,g,N)$ denote the size of the largest $B_h[g]$-subset of $\mathbb{Z}_N$. Clearly then $M(h,g,N) \le A(h,g,N)$. So far as I am aware, the best known upper bounds on $M(h,N) = M(h,1,N)$ come from simple applications of Lemmas 20 and 21 (which, as one can easily check, hold equally well in the modular case). That is to say, one has

$$M(2k,N) \ \le \ (k!)^{1/k} N^{1/2k}(1+o(1))$$

and

$$M(2k-1,N) \ \le \ (k!(k-1)!)^{1/(2k-1)}\, N^{1/(2k-1)}(1+o(1)).$$

In my opinion any significant lowering of these bounds would require a substantial advance in our understanding of these additive representation questions.

For higher values of g it seems that essentially no non-trivial upper bounds are known in the modular case. For $B_2[g]$ sets one could adapt the argument of §8 to get the bound

$$M(2,g,N) \ \le \ (2g-1)^{1/2} N^{1/2}(1+o(1)),$$

a slight improvement on the trivial bound. Non-trivial lower bounds can be obtained, but it should be noted that the results in [3] do not apply to the modular case. All these questions are very interesting.

11. Further remarks on functions with minimal $M(f)$. In this section, which is really an appendix, we offer a miscellany of further results concerning Problem 3. Although these results are not necessary for an understanding of the rest of the paper they do throw a little light on some of the methods we have been using.

We start by showing that the upper bound of Lemma 5 is not tight, even if we restrict attention to functions taking only two values.

LEMMA 27 *There is an $f : \{1,\dots,N\} \to \{0,1\}$ with $|f| = N$ and $M(f) \le 0.64074\, N^3 + O(N^2)$.*

P r o o f. Let A_α be the set obtained by removing an interval of length αN from the middle of $\{1,\dots,N\}$. Let f_α be the characteristic function of A_α, weighted by a factor $(1-\alpha)^{-1}$ so that $|f_\alpha| = N$. A slightly tedious computation enables one to show that for $\alpha < 1/3$ we have

$$M(f_\alpha) \;=\; \frac{\frac{2}{3} - 3\alpha + 6\alpha^2 - 5\alpha^3}{(1-\alpha)^4} N^3 + O(N^2).$$

It is straightforward to check that the minimum in $[0, 1/3]$ occurs at $\alpha \approx 0.13257$. □

We now turn to a study of the extremal functions in Problem 3. Letting $\mathcal{S}$ denote the set of all $f : \{1,\dots,N\} \to \mathbb{R}$ with $|f| = N$, an easy compactness argument shows that there is a function $F \in \mathcal{S}$ such that $M(f) \geq M(F)$ for all $f \in \mathcal{S}$. We write $M(F) = M_0$.

Lemma 28 *$F * F * F$ is equal to M_0/N on $\{1,\dots,N\}$.*

P r o o f. Let $g : \{1,\dots,N\} \to \mathbb{R}$ be any function with $\sum_x g(x) = 0$. Then for any ϵ we must have $M(F+\epsilon g) \geq M_0$. A small computation gives that

$$\begin{aligned} \frac{d}{d\epsilon} \sum_x \left((F+\epsilon g) * (F+\epsilon g)(x)\right)^2 \Big|_{\epsilon=0} &= 4 \sum_x (F*F)(x)(F*g)(x) \\ &= 4 \sum_x (F*F*F)(x) g(x). \end{aligned}$$

This expression must equal 0, and simple linear algebra tells us that this is the case precisely when $F*F*F$ equal to some constant $c(F)$ on $\{1,\dots,N\}$. It is easy to compute the value of $c(F)$ in terms of M_0. Indeed

$$M_0 \;=\; \sum_x (F*F)(x)^2 \;=\; \sum_x (F*F*F)(x)F(x) \;=\; c(F)N. \tag{49}$$

Lemma 29 *There is a unique extremal function in Problem 3.*

P r o o f. For the proof of this lemma we let the hat symbol ($\hat{}$) denote the Fourier transform on $\mathbb{Z}$. Thus for $\theta \in \mathbb{T} = [0,1]$ we set

$$\hat{f}(\theta) \;=\; \sum_x f(x) e(x\theta),$$

where $e(t) = e^{2\pi i t}$. With this notation it follows, using standard facts about Fourier transforms, that

$$M(f) \;=\; \int_0^1 |\hat{f}(\theta)|^4 \, d\theta.$$

Let $f, g : \{1, \dots, N\} \to \mathbb{R}$ be two functions with $|f| = |g| = N$. We use the inequality

$$\left|\frac{a+b}{2}\right|^4 + \left|\frac{a-b}{2}\right|^4 \ \leq \ \frac{|a|^4 + |b|^4}{2},$$

which is valid for all $a, b \in \mathbb{C}$ and follows immediately from the identity

$$|a+b|^4 + |a-b|^4 + 6\left(|a|^2 - |b|^2\right)^2 + 2\left(|ab|^2 - \Re a^2\overline{b}^2\right) \ = \ 8(|a|^4 + |b|^4).$$

Setting $a = \hat{f}(\theta)$, $b = \hat{g}(\theta)$ and integrating over $\theta \in [0, 1]$ we get that

$$M\left(\frac{f+g}{2}\right) \ \leq \ \frac{M(f) + M(g)}{2}, \tag{50}$$

with strict inequality unless $\|\hat{f} - \hat{g}\|_4 = 0$. Since $\hat{f}$ and $\hat{g}$ are both continuous this implies that $\hat{f} = \hat{g}$, which in turn forces $f = g$ identically. Suppose now that $M(f) = M(g) = M_0$. Then, as $|(f+g)/2| = N$, we must have equality in (50). This proves the lemma. □

For the remainder of this section we will work in $\mathbb{Z}_{2N}$. As usual we shall regard functions

$$f : \{1, \dots, N\} \to \mathbb{R}$$

as functions on $\mathbb{Z}_{2N}$, and the hat symbol will once again refer to the Fourier transform on $\mathbb{Z}_{2N}$.

Lemma 30 *Let $G : \{1, \dots, N\} \to \mathbb{R}$ be a function with $|G| = N$. Let $\mathcal{H}_{2N}$ denote the set of all functions $H : \mathbb{Z}_{2N} \to \mathbb{R}$ with $|H| = 0$ and $H(x) = 1$ for $x = 1, \dots, N$ (compare §5). Then we have*

$$\left(\sum_{r \neq 0} |\hat{G}(r)|^4\right)\left(\sum_{r \neq 0} |\hat{H}(r)|^{4/3}\right)^3 \ \geq \ 16N^8 \tag{51}$$

for all $H \in \mathcal{H}_{2N}$. Suppose that in addition $G * G * G$ is constant on $\{1, \dots, N\}$. Then equality can occur in (51).

S k e t c h P r o o f. The first part of the lemma (that is to say the inequality (51)) can be derived in much the same way that we proved Theorem 6 in §5. In fact, the argument is a great deal simpler because we have not introduced any smoothing device here. For the second statement, we simply observe that one can take

$$H(x) \ = \ \frac{2NG * G * G(x) - N^3}{2M(G) - N^3}.$$

The convolutions are taken in $\mathbb{Z}_{2N}$, but one can check that the modular convolution $G * G * G$ is also constant on $\{1, \dots, N\}$. This concludes the proof of the lemma. □

This lemma has a number of consequences. First of all it provides justification for the approach we used in §5 to obtain a lower bound for $M(f)$. Secondly it allows us to prove

COROLLARY 31 *Suppose $G : \{1, \dots, N\} \to \mathbb{R}$ is a function with $|G| = N$ for which $G * G * G$ is constant on $\{1, \dots, N\}$. Then $G = F$.*

P r o o f. It follows easily from Lemma 30 that G is extremal for Problem 3, the problem of minimising $M(G)$. Hence, by Lemma 29, $G = F$. □

To conclude we should like to remark that Problem 3 is closely related to the problem of finding the best possible constants in what are known as Inequalities of Nikol'skĭi Type.

Acknowledgements. The author would like to thank Alex Barnard, for plotting our extremal function F numerically and for advice concerning computations; Tim Gowers, for helpful advice; and Imre Ruzsa for making the preprint [3] available. Finally I would like to thank the referee for a couple of helpful suggestions.

References

[1] S. C h e n, *On the Size of Finite Sidon Sequences*, Proc. Amer. Math. Soc. **121** (1994) 353–356.

[2] J. C i l l e r u e l o, *An Upper Bound for $B_2[2]$ Sequences*, Journal of Combinatorial Theory, Series A **89** (2000) 141–144.

[3] J. C i l l e r u e l o, I. Z. R u z s a and C. T r u j i l l o, *Upper and Lower Bounds for Finite $B_h[g]$ Sequences, $g > 1$*, to appear in Journal of Number Theory.

[4] P. E r d ő s and P. T u r á n, *On a Problem of Sidon in Additive Number Theory and On Some Related Problems*, Journal of the London Mathematical Society **16** (1941) 212–215.

[5] W. T. G o w e r s, *A New Proof of Szemerédi's Theorem for Progressions of Length Four*, Geom. Funct. Anal. **8** (1998) 529 – 551.

[6] S. W. G r a h a m, B_h *Sequences*, in Analyic Number Theory Vol 1 (Allerton Park, IL, 1995) 431–449, Progress in Mathematics **138**, Birkhäuser, Boston MA 1996.

[7] G. R. G r i m m e t t and D. R. S t i r z a k e r, *Probability and Random Processes*, Clarendon Press, Oxford 1992.

[8] R. K. G u y, *Unsolved Problems in Number Theory* Second Edition, Springer 1994.

[9] H. H a l b e r s t a m and K. F. R o t h, *Sequences* Second Edition, Springer 1983.

[10] X. J i a, *On B_{2k} Sequences*, Journal of Number Theory **48** (1994) 183–196.

[11] M. N. K o l o u n t z a k i s, *The Density of $B_h[g]$ Sequences and the Minimum of Dense Cosine Sums*, Journal of Number Theory **56** (1996) 4–11.

[12] B. L i n d s t r ö m, *A Remark on B_4-Sequences*, Journal of Combinatorial Theory **7** (1969) 276–277.

[13] H. L. M o n t g o m e r y, *Topics in Multiplicative Number Theory*, Springer 1971.

[14] A. S á r k ő z y and V. T. S ó s, *On Additive Representation Functions*, in The Mathematics of Paul Erdős, Vol. 1, Springer 1997.

DEPARTMENT OF PURE MATHEMATICS AND MATHEMATICAL STATISTICS
UNIVERSITY OF CAMBRIDGE
WILBERFORCE ROAD
CAMBRIDGE CB3 0WB, ENGLAND