INTEGER SETS CONTAINING NO ARITHMETIC PROGRESSIONS

D. R. HEATH-BROWN

1. *Introduction*

If h and k are positive integers there exists $N(h,k)$ such that whenever $N \geqslant N(h,k)$, and the integers $1, 2, \ldots, N$ are divided into h subsets, at least one must contain an arithmetic progression of length k. This is the famous theorem of van der Waerden [10], dating from 1927. The proof of this uses multiple nested inductions, which result in extremely weak bounds for $N(h,k)$. We shall define B_k to be the collection of all sets $\mathscr{A} \subseteq \mathbb{N}$ for which $\mathscr{A}$ contains no arithmetic progression of length k. We then set

$$\rho_k(N) = \frac{1}{N}\max\{\#\mathscr{A} : \mathscr{A} \in B_k, \mathscr{A} \subseteq [1,N]\}.$$

It seems reasonable to conjecture that

$$\rho_k(N) \to 0 \quad (N \to \infty) \tag{1.1}$$

for each fixed $k \geqslant 3$, which would clearly include van der Waerden's theorem. This conjecture appears to have been explicitly stated for the first time by Erdös and Turán [2], in 1936. It has been asked whether the sequence of primes contains arbitrarily long arithmetic progressions. This would follow from a strengthened form of the conjecture, namely that

$$\rho_k(N) = o\left(\frac{1}{\log N}\right) \quad (N \to \infty)$$

for each $k \geqslant 3$. (Less obviously, the estimate $\rho_k(N) = o((\log\log N)/\log N)$ would suffice.)

The easiest case of the conjecture is $k = 3$, which was proved by Roth [6] in 1953. Roth's treatment is analytic, and uses the Hardy–Littlewood circle method. Roth shows, indeed, that

$$\rho_3(N) \ll \frac{1}{\log\log N}. \tag{1.2}$$

This is too weak to imply a result about primes. However it immediately yields $N(h,3) \leqslant \exp\exp(O(h))$ for the case $k = 3$ of van der Waerden's theorem; this is far better than the induction method gives. Lower bounds for $\rho_3(N)$ (and hence for $\rho_k(N), k \geqslant 4$) have also been established. In particular Behrend [1] has shown that

$$\rho_3(N) \geqslant \exp(-C(\log N)^{\frac{1}{2}})$$

for a suitable constant $C > 0$. The corresponding set $\mathscr{A} \in B_3$ depends on N. However, it was later shown by Moser [5] that one may construct an infinite set $\mathscr{A} \in B_3$ such that

$$\#(\mathscr{A} \cap [1,N]) \geqslant N\exp(-C(\log N)^{\frac{1}{2}})$$

for all $N \geqslant 1$.

Received 19 May 1986.

1980 *Mathematics Subject Classification* 10L20.

J. London Math. Soc. (2) 35 (1987) 385–394

The case $k = 4$ of the conjecture (1.1) was settled by Szemerédi [8] in 1969. Szemerédi gives a difficult combinatorial argument, which is technically elementary. An explicit bound for $\rho_4(N)$ is not found, and since the treatment is based on van der Waerden's theorem, any such bound would be extremely weak. An alternative proof for the case $k = 4$ was given in 1972 by Roth [7]. The method here is partly analytical, though quite different from Roth's treatment of $\rho_3(N)$. However van der Waerden's theorem is used in this approach too, and again no explicit bound for $\rho_4(N)$ is given.

The full conjecture (1.1), for all $k \geqslant 3$, was finally settled by Szemerédi [9] in 1975, again by an elementary argument using van der Waerden's theorem. A remarkable alternative proof, based on ergodic methods, was later given by Furstenberg [3]. In neither case is an explicit bound for $\rho_k(N)$ obtained.

Our goal in the present paper is to improve on Roth's bound (1.2). Such an improvement was described by Szemerédi in a seminar in Budapest in 1985. In the seminar it was shown that

$$\rho_3(N) \ll \frac{1}{(\log\log N)^A}$$

for any positive constant A. However it was discovered by Balog that if the parameters in the proof are chosen optimally, one in fact obtains

$$\rho_3(N) \ll \exp(-C(\log\log N)^{\frac{1}{2}}),$$

for an appropriate constant $C > 0$. None of this work has been published. The method is largely analytical. The key new ingredient is the use of the k-dimensional form of Dirichlet's approximation theorem, in estimating how often an exponential sum can be large. (See the proof of Lemma 4 in §2.)

We shall develop these ideas further, and prove the following.

THEOREM. *There exists an effectively computable constant $c > 0$ such that*

$$\rho_3(N) \ll \frac{1}{(\log N)^c}.$$

The author is most grateful to Professor Balog for informing him of Szemerédi's work on the problem, and for some stimulating discussions on the subject.

In broad outline the proof follows the method of Roth [6]. One takes a set $\mathscr{A} \subseteq [1, N]$ and defines

$$S(\alpha) = \sum_{n\in\mathscr{A}} e(n\alpha).$$

The integral

$$I = \int_0^1 S(\alpha)^2 S(-2\alpha)\,d\alpha$$

then counts arithmetic progressions of length 3 in $\mathscr{A}$, and is estimated by the Hardy–Littlewood circle method. At one key point one has to bound

$$\int_{\mathfrak{m}} |S(\alpha)|^2\,d\alpha$$

for a certain subset $\mathfrak{m}$ of [0, 1]. The standard procedure is to replace $\mathfrak{m}$ by [0, 1] and to use the Parseval identity, giving

$$\int_{\mathfrak{m}} |S(\alpha)|^2\,d\alpha \leqslant \int_0^1 |S(\alpha)|^2\,d\alpha = \#\mathscr{A}.$$

To see that this is sometimes inefficient, it is helpful to consider the corresponding large sieve estimate, namely

$$\sum_{j=1}^{k} |S(\alpha_j)|^2 \ll N(\#\mathscr{A}), \tag{1.3}$$

for 'well-spaced' points α_j. If k is small ($\leqslant N/\#\mathscr{A}$) this is worse than the trivial bound

$$\sum_{j=1}^{k} |S(\alpha_j)|^2 \leqslant k(\#\mathscr{A})^2. \tag{1.4}$$

Thus one might hope to find a form of the large sieve which incorporates both the estimates (1.3) and (1.4), and which would therefore improve our application of the circle method. This we do in Lemma 4. The resulting estimate always includes (1.3) and, subject to mild regularity conditions on $\mathscr{A}$, also includes (1.4). This is the crucial new ingredient that leads to our improvement of (1.2). Unfortunately the new bound can only be sharper than the usual large sieve estimate (1.3) when $k \ll \log N$. This limitation is probably too severe for other applications to the circle method.

The necessary lemmas for our proof are established in §2. These are used for an application of a discrete form of the circle method in §3. This results in a complicated iterative estimate for $\rho_3(N)$. The final section, §4, is devoted to a simple induction argument which extracts the required inequality for $\rho_3(N)$ from this iterative bound. For convenience in what follows we shall merely write B in place of B_3 and $\rho(N)$ in place of $\rho_3(N)$. We shall also employ the notation $e(x) = \exp(2\pi i x)$ and

$$\|x\| = \min\{|x-n| : n \in \mathbb{Z}\}.$$

All constants implied by the symbols $\ll$ and $O(\ )$ will be absolute and effectively computable.

2. *Lemmas*

We begin by proving two rather trivial lemmas.

LEMMA 1. *Let $\mathscr{A} \in B$ and let $\mathscr{P}$ be an arithmetic progression of length n. Then $\#(\mathscr{A} \cap \mathscr{P}) \leqslant n\rho(n)$.*

Let $\mathscr{P} = \{l+k, l+2k, \ldots, l+nk\}$. If $\#(\mathscr{A} \cap \mathscr{P}) > n\rho(n)$, then

$$\left\{\frac{a-l}{k} : a \in \mathscr{A} \cap \mathscr{P}\right\}$$

is a set of more than $n\rho(n)$ integers in the range $[1, n]$. Thus there are distinct elements a, a', $a'' \in \mathscr{A} \cap \mathscr{P}$ for which $(a-l)/k$, $(a'-l)/k$, $(a''-l)/k$ are in arithmetic progression. It follows that a, a', a'' are also in arithmetic progression, contradicting our assumption that $\mathscr{A} \in B$.

LEMMA 2. *If $m \leqslant n$, then $\rho(n) \leqslant 2\rho(m)$. If $m \mid n$, then $\rho(n) \leqslant \rho(m)$.*

Let $\mathscr{A} \in B$, $\mathscr{A} \subseteq [1, n]$ with $\#\mathscr{A} = n\rho(n)$. If $m \leqslant n$ we break the range $[1, n]$ into $1+[n/m]$ subintervals of length at most m. By Lemma 1 each subinterval contains at most $m\rho(m)$ elements of $\mathscr{A}$, whence

$$n\rho(n) = \#\mathscr{A} \leqslant \left(1+\left[\frac{n}{m}\right]\right) m\rho(m) \leqslant (m+n)\rho(m) \leqslant 2n\rho(m).$$

The first part of the lemma follows. The second part is proved in the same way, save that now n/m subintervals suffice.

Our third lemma is essentially the same exponential sum estimate as was used by Roth [6]. We reproduce the proof here, for completeness.

LEMMA 3. *Let $a_n = 0$ or 1 $(1 \leqslant n \leqslant N)$. For any $M \leqslant N$ define $\xi(M)$ by*

$$M\xi(M) = \max\{\sum_{n\in\mathscr{P}\cap[1,N]} a_n\},$$

where $\mathscr{P}$ runs over all arithmetic progressions of length M. Put

$$S(\alpha) = \sum_1^N a_n\, e(n\alpha), \qquad T(\alpha) = \xi(N)\sum_1^N e(n\alpha).$$

Then

$$S(\alpha) = T(\alpha) + O(N|\xi(N)-\xi(M)|) + O(MN^{\frac{1}{2}})$$

for any $M \leqslant N$.

We begin by supposing that $\alpha = (h/q)+\beta$ for some $h\in\mathbb{Z}$, $q\in\mathbb{N}$. (Note that h/q is not assumed to be in lowest terms, nor to be an approximation to α.) Then

$$\sum_{r=1}^{q}\sum_{m=1}^{N}\sum_{\substack{m\leqslant n<m+qM\\ n\equiv r(\mathrm{mod}\ q)}} a_n\, e(n\alpha) = \sum_{n=1}^{N} a_n\, e(n\alpha)\, w_n,$$

with

$$w_n = \begin{cases} qM, & n \geqslant qM,\\ O(qM), & n < qM.\end{cases}$$

It follows that

$$S(\alpha) = \frac{1}{qM}\sum_{r=1}^{q}\sum_{m=1}^{N}\sum_{\substack{m\leqslant n<m+qM\\ n\equiv r(\mathrm{mod}\ q)}} a_n\, e(n\alpha) + O(qM).$$

In the innermost sum on the right we have

$$e(n\alpha) = e\left(\frac{rh}{q}\right)e(n\beta) = e\left(\frac{rh}{q}\right)e(m\beta) + O(qM|\beta|),$$

whence

$$S(\alpha) = \frac{1}{qM}\sum_{r=1}^{q} e\left(\frac{rh}{q}\right)\sum_{m=1}^{N} e(m\beta)\sum_{\substack{m\leqslant n<m+qM\\ n\equiv r(\mathrm{mod}\ q)}} a_n + O(qM) + O(qMN|\beta|). \qquad (2.1)$$

By the definition of $\xi(M)$ we see that

$$\sum_{\substack{m\leqslant n<m+qM\\ n\equiv r(\mathrm{mod}\ q)}} a_n = M\xi(M) - \Delta(q,r,M,m),$$

say, with $\Delta(q,r,M,m) \geqslant 0$. Thus

$$S(\alpha) = \frac{\xi(M)}{q}\left(\sum_{r=1}^{q} e\left(\frac{rh}{q}\right)\right)\left(\sum_{m=1}^{N} e(m\beta)\right) + O\left(\frac{1}{qM}\sum_{r=1}^{q}\sum_{m=1}^{N}\Delta(q,r,M,m)\right)$$
$$+ O(qM) + O(qMN|\beta|).$$

However, if we take $\alpha = 0$, $\beta = 0$, $h = 0$ in (2.1), we find that

$$N\xi(N) = \frac{1}{qM}\sum_{r=1}^{q}\sum_{m=1}^{N}(M\xi(M)-\Delta(q,r,M,m))+O(qM),$$

whence

$$\frac{1}{qM}\sum_{r=1}^{q}\sum_{m=1}^{N}\Delta(q,r,M,m) \ll qM+N|\xi(N)-\xi(M)|.$$

It follows that

$$S(\alpha) = \frac{\xi(M)}{q}\left(\sum_{r=1}^{q} e\left(\frac{rh}{q}\right)\right)\left(\sum_{m=1}^{N} e(m\beta)\right) + O(qM)+O(qMN|\beta|)+O(N|\xi(N)-\xi(M)|). \qquad (2.2)$$

Now let $q \leqslant N^{\frac{1}{2}}$, $(h,q) = 1$ and $|\beta| \leqslant q^{-1}N^{-\frac{1}{2}}$, as is possible by Dirichlet's theorem. When $\|\alpha\| > N^{-\frac{1}{2}}$, we have $q > 1$, and the estimate (2.2) reduces to

$$S(\alpha) \ll N|\xi(N)-\xi(M)|+MN^{\frac{1}{2}}.$$

Moreover,

$$T(\alpha) \ll \xi(N)\|\alpha\|^{-1} \ll N^{\frac{1}{2}},$$

so that the lemma follows in this case. If $\|\alpha\| \leqslant N^{-\frac{1}{2}}$, we may take $q = 1$, so that (2.2) yields

$$\begin{aligned} S(\alpha) &= \xi(M)\sum_{1}^{N} e(m\alpha)+O(N|\xi(N)-\xi(M)|)+O(MN^{\frac{1}{2}}) \\ &= \xi(N)\sum_{1}^{N} e(m\alpha)+O(N|\xi(N)-\xi(M)|)+O(MN^{\frac{1}{2}}), \end{aligned}$$

thereby establishing the lemma in this case too.

Our next result is the key one referred to in the introduction.

LEMMA 4. *Let $a_n \in \mathbb{C}$ $(1 \leqslant n \leqslant N)$, and put $S(\alpha) = \sum_{1}^{N} a_n e(n\alpha)$. For any $M \leqslant N$ define $\xi(M)$ by*

$$M\xi(M) = \max\{\sum_{n\in\mathscr{P}} |a_n|\},$$

where $\mathscr{P}$ runs over arithmetic progressions of length M. Let $\alpha_1, \ldots, \alpha_k \in \mathbb{R}$ satisfy

$$\|\alpha_i-\alpha_j\| \geqslant \frac{1}{N} \qquad (i \neq j). \qquad (2.3)$$

Then

$$\sum_{j=1}^{k} |S(\alpha_j)|^2 \ll N^2\xi(N)\,\xi(M),$$

where $M = [\frac{1}{2}N^{1/(k+1)}]$.

Our starting point is the Sobolev–Gallagher inequality

$$|f(x_0)| \leqslant \delta^{-1}\int_{x_0}^{\delta+x_0} |f(x)|\,dx+\int_{x_0}^{\delta+x_0} |f'(x)|\,dx,$$

valid for any continuously differentiable function $f(x)$. (See Montgomery [4, Lemma 1.1].) We take $\delta = N^{-1}, f(x) = S(x)^2$, and we sum for $x_0 = \alpha_j$ $(1 \leqslant j \leqslant k)$. Thus

$$\begin{aligned} \sum_{j=1}^{k} |S(\alpha_j)|^2 &\leqslant N\sum_{j=1}^{k}\int_{\alpha_j}^{N^{-1}+\alpha_j} |S(\alpha)|^2\,d\alpha+2\sum_{j=1}^{k}\int_{\alpha_j}^{N^{-1}+\alpha_j} |S(\alpha)\,S'(\alpha)|\,d\alpha \\ &\leqslant N\Sigma^{(1)}+2\{\Sigma^{(1)}\Sigma^{(2)}\}^{\frac{1}{2}}, \end{aligned} \qquad (2.4)$$

where

$$\Sigma^{(1)} = \sum_{j=1}^{k} \int_{\alpha_j}^{N^{-1}+\alpha_j} |S(\alpha)|^2\, d\alpha,$$

$$\Sigma^{(2)} = \sum_{j=1}^{k} \int_{\alpha_j}^{N^{-1}+\alpha_j} |S'(\alpha)|^2\, d\alpha,$$

by Cauchy's inequality. The intervals here are disjoint modulo 1, by the spacing condition (2.3). We now use the key idea introduced by Szemerédi. Let Q be a positive integer. By the k-dimensional version of Dirichlet's theorem we may find $q \leqslant Q^k$ such that $\|q\alpha_j\| \leqslant Q^{-1}$ for each α_j. If $Q = 2M \leqslant N^{1/(k+1)}$ we deduce that

$$\|q\alpha\| \leqslant Q^{-1}+qN^{-1} \leqslant 2Q^{-1}$$

whenever $\alpha_j \leqslant \alpha \leqslant N^{-1}+\alpha_j$. It follows that

$$\begin{aligned}\Sigma^{(1)} &\leqslant \sum_{r=1}^{q} \int_{-2(qQ)^{-1}}^{2(qQ)^{-1}} \left|S\left(\frac{r}{q}+\alpha\right)\right|^2 d\alpha \\ &\leqslant \sum_{r=1}^{q} \int_{-\infty}^{\infty} \left|S\left(\frac{r}{q}+\alpha\right)\right|^2 \left(\frac{\sin(\pi\alpha qQ/4)}{\alpha qQ/2}\right)^2 d\alpha \\ &= \frac{\pi^2}{Q} \sum_{\substack{|m-n|<qQ/4 \\ m\equiv n (\mathrm{mod}\ q)}} a_m \overline{a_n}\left(1-\frac{|m-n|}{qQ/4}\right).\end{aligned}$$

Here n runs over an interval of length $qQ/2 = qM$ for each available value of m. Thus

$$\Sigma^{(1)} \leqslant \frac{\pi^2}{Q} \sum_{m=1}^{N} |a_m| M\xi(M) = \frac{\pi^2}{2} N\xi(N)\,\xi(M).$$

In an exactly similar way we find that

$$\Sigma^{(2)} \leqslant \frac{\pi^2}{2} N^3\xi(N)\,\xi(M).$$

The lemma follows, by (2.4).

Our final lemma is just a form of the large sieve.

LEMMA 5. *Under the hypotheses of Lemma* 4 *we have*

$$\sum_{j=1}^{k} |S(\alpha_j)|^2 \ll N \sum_{n=1}^{N} |a_n|^2.$$

For a proof, see for example Montgomery [4, Corollary 2.2].

3. *The circle method*

In this section we take a set $\mathscr{A} \in B$, $\mathscr{A} \subseteq [1,N]$ with $\#\mathscr{A} = N\rho(N)$, and use the circle method to estimate the number of 3-term arithmetic progressions in $\mathscr{A}$. Since this number should be zero, we shall conclude that the error terms in our estimate are at least as big as the supposed main term. We write $N_s = 2^{4^s}$ $(s = 0, 1, 2, \ldots)$ and $\nu(s) = \rho(N_s)$, and we take $N = N_t$ so that $\rho(N) = \nu(t)$. For $1 \leqslant n \leqslant N$ let

$$a_n = \begin{cases} 1, & n \in \mathscr{A}, \\ 0, & n \notin \mathscr{A}, \end{cases}$$

and $S_1(\alpha) = \Sigma a_n e(n\alpha)$, $S_2(\alpha) = \Sigma a_n e(-2n\alpha)$. Instead of using the circle method in its classical form we shall set $L = 3N$ and investigate

$$\sum_{l=1}^{L} S_1\left(\frac{l}{L}\right)^2 S_2\left(\frac{l}{L}\right) = \Sigma_1,$$

say. The advantage in using a sum rather than an integral is merely that it is easier to pick out well-spaced points. Since $L > 2N$ and $\mathscr{A} \in B$, we have

$$\begin{aligned}\Sigma_1 &= L\,\#\{(n_1,n_2,n_3)\colon n_i \in \mathscr{A}, n_1+n_2 \equiv 2n_3 (\operatorname{mod} L)\}\\ &= L\,\#\{(n_1,n_2,n_3)\colon n_i \in \mathscr{A}, n_1+n_2 = 2n_3\}\\ &= LN\nu(t).\end{aligned} \tag{3.1}$$

We now write

$$T_1(\alpha) = \nu(t)\sum_{1}^{N} e(n\alpha), \qquad T_2(\alpha) = T_1(-2\alpha),$$

and

$$D_i(\alpha) = S_i(\alpha) - T_i(\alpha) \quad (i = 1,2).$$

Then

$$S_1^2 S_2 = T_1^2 T_2 + (2T_1 D_1 T_2 + D_1^2 T_2 + T_1^2 D_2 + 2T_1 D_1 D_2 + D_1^2 D_2). \tag{3.2}$$

Since L is even we have

$$\sum_{l=1}^{L} \left|T_2\left(\frac{l}{L}\right)\right|^3 = \sum_{l=1}^{L} \left|T_1\left(-\frac{2l}{L}\right)\right|^3 \leqslant 2\sum_{l=1}^{L} \left|T_1\left(\frac{l}{L}\right)\right|^3,$$

with similar results for D_2 and D_1. Moreover,

$$T_1(\alpha) \ll \nu(t)\min(N, \|\alpha\|^{-1}),$$

whence

$$\sum_{l=1}^{L} \left|T_1\left(\frac{l}{L}\right)\right|^3 \ll (N\nu(t))^3.$$

By Hölder's inequality it therefore follows from (3.2) that

$$\sum_{l=1}^{L} \left(S_1\left(\frac{l}{L}\right)^2 S_2\left(\frac{l}{L}\right) - T_1\left(\frac{l}{L}\right)^2 T_2\left(\frac{l}{L}\right)\right) \ll (N\nu(t))^2 \Sigma_2^{\frac{1}{3}} + \Sigma_2,$$

where

$$\Sigma_2 = \sum_{l=1}^{L} \left|D_1\left(\frac{l}{L}\right)\right|^3.$$

Since

$$\begin{aligned}\sum_{l=1}^{L} T_1\left(\frac{l}{L}\right)^2 T_2\left(\frac{l}{L}\right) &= \nu(t)^3 L\,\#\{(n_1,n_2,n_3)\colon 1 \leqslant n_i \leqslant N, n_1+n_2 \equiv 2n_3 \,(\operatorname{mod} L)\}\\ &\gg (N\nu(t))^3,\end{aligned}$$

we therefore conclude from (3.1) that either

$$\nu(t) \ll N^{-\frac{1}{2}} \tag{3.3}$$

or

$$\Sigma_2 \gg (N\nu(t))^3. \tag{3.4}$$

We shall estimate $D_1(\alpha)$ by means of Lemma 3, in which we take $M = N^{\frac{1}{4}} = N_{t-1}$. From our definitions we have $\xi(N) = \rho(N)$, and by Lemma 1 we have $\xi(M) \leqslant \rho(M)$. Moreover, since $M \mid N$, Lemma 2 yields

$$\rho(M) = \nu(t-1) \geqslant \rho(N) = \nu(t).$$

Thus Lemma 3 produces

$$D_1(\alpha) \ll N(\nu(t-1)-\nu(t))+N^{\frac{3}{4}}.$$

We now set

$$\Sigma_3 = \sum_{l=1}^{L} \left|D_1\left(\frac{l}{L}\right)\right|^{\frac{5}{2}},$$

whence

$$\Sigma_2 \ll \{N(\nu(t-1)-\nu(t))+N^{\frac{3}{4}}\}^{\frac{1}{2}}\Sigma_3. \tag{3.5}$$

We proceed to bound Σ_3, using Lemmas 4 and 5. We split Σ_3 into three sums depending on the residue class of l (mod 3), and call the largest of the sums Σ_4, so that

$$\Sigma_3 \ll \Sigma_4. \tag{3.6}$$

We then label the corresponding points l/L as $\alpha_1, \alpha_2, \ldots$, in such an order that

$$|D_1(\alpha_1)| \geqslant |D_1(\alpha_2)| \geqslant \ldots.$$

The points α_j will satisfy the spacing condition (2.3). Moreover, if $b_n = a_n - \rho(N)$, then Lemmas 1 and 2 yield

$$\sum_{n\in\mathscr{P}} |b_n| \leqslant \sum_{n\in\mathscr{P}} a_n + M\rho(N) \leqslant M\rho(M)+M\rho(N) \ll M\rho(M),$$

where $\mathscr{P}$ is any arithmetic progression of length $M \leqslant N$. We may therefore apply Lemma 4 to $D_1(\alpha)$, with $\xi(M) \ll \rho(M)$. This yields

$$k|D_1(\alpha_k)|^2 \leqslant \sum_{j=1}^{k} |D_1(\alpha_j)|^2 \ll N^2\rho(N)\,\rho(M),$$

where $M = [\frac{1}{2}N^{1/(k+1)}]$. Now if $2^{h-1} \leqslant k < 2^h$, one has

$$\tfrac{1}{2}N^{1/(k+1)} \geqslant \tfrac{1}{2}N^{2^{-h}} \geqslant N^{4^{-h}} = N_{t-h},$$

providing that $h \leqslant t$. Thus $M \geqslant N_{t-h}$, whence Lemma 2 produces $\rho(M) \leqslant 2\nu(t-h)$. It follows that

$$|D_1(\alpha_k)|^2 \ll \frac{N^2\nu(t)\,\nu(t-h)}{2^h} \qquad (2^{h-1} \leqslant k < 2^h, 1 \leqslant h \leqslant t),$$

so that

$$\sum_{k<2^t} |D_1(\alpha_k)|^{\frac{5}{2}} \ll N^{\frac{5}{2}}\nu(t)^{\frac{5}{4}} \sum_{1\leqslant h\leqslant t} \nu(t-h)^{\frac{5}{4}}2^{-h/4}. \tag{3.7}$$

For the remaining range $2^t \leqslant k \ll L$ we use an analogous argument based on Lemma 5. Here we observe that, if $b_n = a_n - \rho(N)$ as before, then

$$\sum_1^N |b_n|^2 \ll \sum_1^N a_n^2 + \sum_1^N \rho(N)^2 \ll N\rho(N).$$

One therefore obtains

$$\begin{aligned}\sum_{k\geqslant 2^t} |D_1(\alpha_k)|^{\frac{5}{2}} &\ll N^{\frac{5}{2}}\nu(t)^{\frac{5}{4}} \sum_{h>t} 2^{-h/4}\\ &\ll N^{\frac{5}{2}}\nu(t)^{\frac{5}{4}}2^{-t/4}.\end{aligned}$$

In conjunction with (3.7) this yields

$$\Sigma_4 \ll N^{\frac{5}{2}}\nu(t)^{\frac{5}{4}}\,\{2^{-t/4} + \sum_{1\leqslant h\leqslant t} \nu(t-h)^{\frac{5}{4}}2^{-h/4}\}. \tag{3.8}$$

We now note that $\nu(j) = \rho(N_j) \leqslant 1$ for $j \geqslant 0$, whence

$$\nu(t-1)-\nu(t) \ll 1$$

and

$$\sum_{1 \leqslant h \leqslant t} \nu(t-h)^{\frac{5}{4}} 2^{-h/4} \ll 1.$$

A comparison of (3.3), (3.4), (3.5), (3.6) and (3.8) then shows that either

$$\nu(t) \ll 2^{-t/7}, \tag{3.9}$$

or

$$\nu(t)^{\frac{7}{4}} \ll \{\nu(t-1)-\nu(t)\}^{\frac{1}{2}} \sum_{1 \leqslant h \leqslant t} \nu(t-h)^{\frac{5}{4}} 2^{-h/4}. \tag{3.10}$$

4. *Completion of the proof*

In this section we shall use induction, based on the estimates (3.9) and (3.10), to bound $\nu(t)$. We write the implied constants in these estimates as 2^A, so that either

$$\nu(t) \leqslant 2^{A-t/7} \tag{4.1}$$

or

$$\nu(t)^{\frac{7}{4}} \leqslant 2^A \{\nu(t-1)-\nu(t)\}^{\frac{1}{2}} \sum_{1 \leqslant h \leqslant t} \nu(t-h)^{\frac{5}{4}} 2^{-h/4}. \tag{4.2}$$

Here A is an effectively computable numerical constant. We choose further constants B and C such that

$$0 < B \leqslant \tfrac{1}{10}, \tag{4.3}$$

$$2^B \leqslant 1+2^{-2A-8}, \tag{4.4}$$

$$C = \max(A, 0). \tag{4.5}$$

We shall now prove, by induction on j, that

$$\nu(j) \leqslant 2^{C-Bj} \quad (j \geqslant 0). \tag{4.6}$$

If $j = 0$, then $\nu(0) = \rho(2^{4^0}) \leqslant 1$, and (4.6) follows, since $C \geqslant 0$, by (4.5). We now assume the truth of (4.6) for each non-negative integer $j < t$, and proceed to prove (4.6) for $j = t$.

If (4.1) holds, then the case $j = t$ of (4.6) is immediate, since $C \geqslant A$, by (4.5), and $B \leqslant \frac{1}{7}$, by (4.3). If (4.2) holds our induction assumption yields

$$\nu(t)^{\frac{7}{4}} \leqslant 2^A \{\nu(t-1)-\nu(t)\}^{\frac{1}{2}} \sum_{1 \leqslant h \leqslant t} 2^{5C/4-5Bt/4} 2^{-(\frac{1}{4}-5B/4)h}. \tag{4.7}$$

We now observe that $\frac{1}{4}-\frac{5}{4}B \geqslant \frac{1}{8}$, by (4.3), and that

$$\sum_{h=1}^{\infty} 2^{-h/8} \leqslant 2^4.$$

We may therefore deduce from (4.7) that

$$\nu(t)^{\frac{7}{4}} \leqslant 2^{A+4+5C/4-5Bt/4} \{\nu(t-1)-\nu(t)\}^{\frac{1}{2}}.$$

If

$$\nu(t-1)-\nu(t) < 2^{-2A-8}\nu(t)$$

we shall have

$$\nu(t)^{\frac{7}{4}} < 2^{5C/4-5Bt/4}\nu(t)^{\frac{1}{2}},$$

and the case $j = t$ of (4.6) will follow. Otherwise, we have

$$\nu(t-1)-\nu(t) \geqslant 2^{-2A-8}\nu(t),$$

whence

$$\nu(t) \leqslant \frac{1}{1+2^{-2A-8}}\nu(t-1) \leqslant 2^{-B}\nu(t-1)$$

by (4.4). However, our induction assumption yields

$$\nu(t-1) \leqslant 2^{C-B(t-1)},$$

so that the case $j = t$ of (4.6) follows in this instance also. This completes the proof of the estimate (4.6).

We now have

$$\rho(N_t) = \nu(t) \ll 2^{-Bt} \ll (\log N_t)^{-D}, \tag{4.8}$$

where $D = \frac{1}{2}B$. It remains to consider more general values of N. For $N \geqslant 2$, we choose $t \geqslant 0$ so that $N_t \leqslant N < N_{t+1}$. Then

$$\log N \leqslant \log N_{t+1} = 4 \log N_t,$$

whence Lemma 2 in conjunction with (4.8) yields

$$\rho(N) \leqslant 2\rho(N_t) \ll (\log N_t)^{-D} \ll (\log N)^{-D}.$$

This completes the proof of the theorem, with $c = D$.

Note added 16.9.86. Since this paper was submitted for publication the author has learned from Professor Szemerédi that he has refined his method to give the same result as our theorem, even with an explicit exponent $c = \frac{1}{20}$.

References

1. F. A. Behrend, 'On sets of integers which contain no three terms in arithmetic progression', *Proc. Nat. Acad. Sci. USA* 32 (1946) 331–332.
2. P. Erdös and P. Turán, 'On some sequences of integers', *J. London Math. Soc.* 11 (1936) 261–264.
3. H. Furstenberg, 'Ergodic behaviour of diagonal measures and a theorem of Szemerédi on arithmetic progressions', *J. Analyse Math.* 31 (1977) 204–256.
4. H. L. Montgomery, *Topics in multiplicative number theory* (Springer, Berlin, 1971).
5. L. Moser, 'On non-averaging sets of integers', *Canad. J. Math.* 5 (1953) 245–252.
6. K. F. Roth, 'On certain sets of integers', *J. London Math. Soc.* 28 (1953) 104–109.
7. K. F. Roth, 'Irregularities of sequences relative to arithmetic progressions. IV', *Period. Math. Hungar.* 2 (1972) 301–326.
8. E. Szemerédi, 'On sets of integers containing no four elements in arithmetic progression', *Acta Math. Acad. Sci. Hungar.* 20 (1969) 89–104.
9. E. Szemerédi, 'On sets of integers containing no k elements in arithmetic progression', *Acta Arith.* 27 (1975) 299–345.
10. B. L. van der Waerden, 'Beweis einer Baudetschen Vermutung', *Nieuw Arch. Wisk.* (2) 15 (1927) 212–216.

Magdalen College
Oxford OX1 4AU