DIFFERENCE SETS AND SHIFTED PRIMES

JASON LUCIER

1. Introduction

For a set of integers $A$ we denote by $A - A$ the set of all differences $a - a'$ with $a$ and $a'$ in $A$, and if $A$ is a finite set we denote its cardinality by $|A|$. Sárközy [12] proved, by the Hardy-Littlewood method, that if $A$ is a subset of $\{1, \ldots, n\}$ such that $A - A$ does not contain a perfect square, then

$$|A| \ll n(\log_2 n)^{2/3}(\log n)^{-1/3}. $$

This estimate was improved by Pintz, Steiger and Szemerédi [10] to

$$|A| \ll n(\log n)^{-1/12} \log \log \log \log n. $$

This improvement was obtained using the Hardy-Littlewood method together with a combinatorial result concerning sums of rationals. Balog, Pelikán, Pintz and Szemerédi [1], elucidating the method in [10], proved for any fixed integer $k \geq 2$, that if $A$ is a subset of $\{1, \ldots, n\}$ such that $A - A$ does not contain a perfect $k$-th power, then

$$|A| \ll_k n(\log n)^{-(1/4)} \log \log \log \log n. $$

In the works cited above the following basic property is used; if $s$ is a perfect $k$-th power then so is $q^k s$ for every positive integer $q$. This multiplicative property is used in the following fashion: Suppose that $B$ is a set of integers and $A = \{c + q^k b : b \in B\}$ for some integers $c$ and $q \geq 1$, if $A - A$ does not contain a perfect $k$-th power, then the same is true for $B - B$. This deduction is the basis of an iteration argument that plays a fundamental rôle in [1], [10], and [12].

Sárközy [13] also considered the set $S = \{p - 1 : p \text{ a prime}\}$ of shifted primes, and showed that if $A$ is a subset of $\{1, \ldots, n\}$ such that $A - A$ does not contain an integer from $S$ then

$$|A| \ll n(\log \log n)^3(\log \log \log \log n)/(\log \log n)^2. $$

The argument Sárközy used in [12] cannot be applied directly to the set $S$ of shifted primes since it does not have a multiplicative property analogous to the one possessed by the set of perfect $k$-th powers.

Date: May 24, 2007.
Sárközy got around this difficulty by not only considering the set $S$ of shifted primes, but also the sets defined for each positive integer $d$ by

$$S_d = \left\{ \frac{p-1}{d} : p \text{ a prime, } p \equiv 1 \pmod{d} \right\}.$$ 

In [13] Sárközy uses an iteration argument based on the following observation. Suppose $B$ is a set of integers and $A = \{c + qb : b \in B\}$ for some integers $c$ and $q \geq 1$, if $A - A$ does not intersect $S_d$ for some positive integer $d$, then $B - B$ does not intersect $S_{dq}$.

In this article we show that the combinatorial argument presented in [1] and [10] can be carried out to improve Sárközy’s result on the set $S$ of shifted primes. We shall prove the following.

**Theorem.** Let $n$ be a positive integer and $A$ a subset of $\{1, \ldots, n\}$. If there does not exist a pair of integers $a, a' \in A$ such that $a - a' = p - 1$ for some prime $p$, then

$$|A| \ll n \left( \frac{(\log \log \log n)^3(\log \log \log \log n)}{\log \log n} \right)^{(\log \log \log \log n)}.$$ 

The set of perfect squares and the set $S$ of shifted primes are examples of *intersective* sets. To define this class of sets we introduce some notation. Given a set of positive integers $H$ we define $D(H, n)$, for any positive integer $n$, to be the maximal size of a subset $A$ of $\{1, \ldots, n\}$ such that $A - A$ does not intersect $H$. A set of positive integers $H$ is called *intersective* if $D(H, n) = o(n)$.

Kamae and Mendès France [6] supplied a general criterion for determining if a set of positive integers is intersective. From their criterion they deduced the following.

(I) For any fixed integer $a$ the set $\{p + a : p \text{ a prime, } p > -a\}$ is intersective if and only if $a = \pm 1$.

(II) Let $h$ be a nonconstant polynomial with integer coefficients and whose leading coefficient is positive. The set $\{h(m) : m \geq 1, h(m) \geq 1\}$ is intersective if and only if for each positive integer $d$ the modular equation $h(x) \equiv 0 \pmod{d}$ has a solution.

Let $h$ be a polynomial as in (II) with degree $k \geq 2$ and such that $h(x) \equiv 0 \pmod{d}$ has a solution for every positive integer $d$. The author [8] has shown that if $A$ is a subset of $\{1, \ldots, n\}$ such that $A - A$ does not intersect $\{h(m) : m \geq 1, h(m) \geq 1\}$, then $|A| \ll n^{(\log_2 n)^{\mu/(k-1)}(\log n)^{-2}}$, where $\mu = 3$ if $k = 2$ and $\mu = 2$ if $k \geq 3$. It is possible to improve this result with the method presented in this paper.
2. Preliminary lemmata

In this paper we use the following notations. For a real number \( x \) we write \( e(x) \) for \( e^{2\pi i x} \), and \( [x] \) is used to denote the greatest integer less than or equal to \( x \). The greatest common divisor of the integers \( u \) and \( v \) is given by \( (u,v) \). Euler’s totient function is given, as usual, by \( \phi \). For any positive integer \( i \) we write \( \log_i \) to denote the \( i \)-th iterated logarithm, that is, \( \log_1 n = \log n \) and \( \log_i n = \log(\log_{i-1} n) \) for every integer \( i \geq 2 \).

A fundamental rôle is played by the following relations; for integers \( n \) and \( r \), with \( n \) positive,

\[
\sum_{t=0}^{n-1} e(rt/n) = \begin{cases} n & \text{if } n \mid r \\ 0 & \text{if } n \nmid r \end{cases}, \quad \int_0^1 e(r\alpha)d\alpha = \begin{cases} 1 & \text{if } r = 0 \\ 0 & \text{if } r \neq 0 \end{cases}.
\]

Given a subset \( A \) of \( \{1, \ldots, n\} \) its generating function is given by

\[
F(\alpha) = \sum_{a \in A} e(\alpha a), \quad \alpha \in \mathbb{R}.
\]

Using the relations above we find that

\[
\sum_{t=1}^n |F(t/n)|^2 = n|A|, \quad \int_0^1 |F(\alpha)|^2d\alpha = |A|.
\]

Of course, these are particular cases of Parseval’s identity.

Sárközy’s method in [12] and [13] is based on Roth’s work [11] on three-term arithmetic progressions in dense sets. Following this method Sárközy uses a functional inequality to derive his results concerning the set of perfect squares and the set \( S \) of shifted primes. Our approach here uses, like Gowers [3] and Green [4], a density increment argument. The next lemma tells us that if the generating function of a finite set \( A \) satisfies a certain size constraint, then it must be concentrated along an arithmetic progression. We use this result in Lemma 10 to obtain a density increment that we iterate in the final section of the paper to prove the theorem.

**Lemma 1.** Let \( n \) be a positive integer and \( A \) a subset of \( \{1, \ldots, n\} \) with size \( \delta n \). For any real \( \alpha \) let \( F(\alpha) \) denote the generating function of \( A \). Let \( q \) be a positive integer and \( U \) a positive real number such that \( 2\pi qU \leq n \). Let \( E \) denote the subset of \([0,1]\) defined by

\[
E = \left\{ \alpha \in [0,1] : \left| \alpha - \frac{a}{q} \right| \leq \frac{U}{n} \text{ for some } 0 \leq a \leq q \right\}.
\]
If \( \theta \) is a positive number such that

\[
(1) \quad \sum_{t/n \in E} |F(t/n)|^2 \geq \theta |A|^2,
\]

then there exists an arithmetic progression \( P \) in \( \{1, \ldots, n\} \) with difference \( q \) such that

\[
|P| \geq \frac{n}{32\pi qU}\quad \text{and} \quad |A \cap P| \geq |P|\delta\left(1 + 8^{-1}\theta\right).
\]

Proof. This closely resembles Lemma 20 in [8] and can be proved in the same manner. \( \square \)

We now state a combinatorial result presented by Balog, Pelikán, Pintz and Szemerédi in [1], the proof of which uses only elementary techniques. It is this result, that we use in Lemma 9, that allows us to improve Sárközy result on the set \( S \) of shifted primes.

**Lemma 2.** Let \( K \) and \( L \) be positive integers, and let \( \tau \) be the maximal value of the divisor function up to \( KL \). Let \( K \) be a nonempty subset of rationals such that if \( a/k \in K \) is in lowest terms then \( 1 \leq a \leq k \leq K \). Suppose that for each \( a/k \in K \) there corresponds a subset of rationals \( \mathcal{L}_{a/k} \) such that if \( b/l \in \mathcal{L}_{a/k} \) is in lowest terms then \( 1 \leq b \leq l \leq L \). Suppose further that \( B \) and \( H \) are positive integers such that

\[
|\mathcal{L}_{a/k}| \geq H \quad \text{for all} \quad a/k \in K
\]

and

\[
\left| \left\{ b/l \in \bigcup \mathcal{L}_{a/k} \right\} \right| \leq B \quad \text{for all} \quad l \leq L.
\]

Then the size of the set

\[
\mathcal{Q} = \left\{ \frac{a}{k} + \frac{b}{l} : \frac{a}{k} \in K, \frac{b}{l} \in \mathcal{L}_{a/k} \right\}
\]

satisfies

\[
|\mathcal{Q}| \geq |K|H \left( \frac{H}{LB\tau^8(1 + \log K)} \right).
\]

Proof. This is Lemma CR in [1]. \( \square \)
3. Exponential sums over primes

Let $d$ and $n$ denote positive integers. As in [13], our application of the Hardy-Littlewood method employs exponential sums over numbers from the set $S_d$ defined in the introduction. For any real number $\alpha$ we set

$$S_{n,d}(\alpha) = \sum_{\substack{s \in S_d \leq n}} \log(ds + 1)e(\alpha s).$$

In this section we present some estimates related to $S_{n,d}(\alpha)$. Throughout this section we assume $d$ and $n$ satisfy

$$d \leq \log n.$$

**Lemma 3.** For $n$ sufficiently large,

$$S_{d,n}(0) \gg \frac{dn}{\phi(d)}.$$

**Proof.** By the definition of $S_d$ we find that

$$S_{d,n}(0) = \sum_{\substack{p \leq dn + 1 \mod d \equiv 1 \mod d \leq n}} \log p.$$

Since $d \leq \log n$ the Siegel-Walfisz theorem says that this sum is asymptotic to $(dn + 1)/\phi(q)$, from which the result follows. □

The next two lemmas provide estimates of $S(\alpha)$ derived by A. Sárközy.

**Lemma 4.** Let $a$ and $b$ be integers such that $(a, b) = 1$ and $1 \leq b \leq \log n$. There exists a positive real number $c$ such that if $\alpha$ is a real number that satisfies

$$|\alpha - \frac{a}{b}| \leq \frac{\exp(c(\log n)^{1/2})}{n},$$

and $n$ is sufficiently large, then

$$|S_{d,n}(\alpha)| < \frac{dn}{\phi(d)\phi(b)},$$

furthermore, if $\alpha \neq a/b$ then

$$|S_{d,n}(\alpha)| < \frac{d}{\phi(d)\phi(b)} |\alpha - \frac{a}{b}|^{-1}.$$

**Proof.** This is a restatement of Lemma 5 from [13]. □
Let \( R \) denote a real number that satisfies
\[
3 \leq R \leq \log n.
\]
For integers \( a \) and \( b \) such that \((a, b) = 1\) and \( 0 \leq a \leq b \leq R \) we set
\[
\mathcal{M}(b, a) = \left\{ \alpha \in [0, 1] : \left| \alpha - \frac{a}{b} \right| \leq \frac{R}{n \log \log R} \right\}.
\]
Let \( m \) denote the set of real numbers \( \alpha \) for which there do not exist integers \( a \) and \( b \) such that \((a, b) = 1\), \( 1 \leq b < R \), and \( \alpha \in \mathcal{M}(b, a) \).

**Lemma 5.** For \( \alpha \in m \) and large \( n \),
\[
S_{d,n}(\alpha) \ll \frac{dn}{\phi(d)} \cdot \frac{\log \log R}{R}.
\]
**Proof.** This is a restatement of Lemma 9 from [13]. \( \square \)

**Lemma 6.** Let \( a \) and \( b \) be integers such that \( 0 \leq a \leq b \leq R \) and \((a, b) = 1\). Then for \( n \) sufficiently large
\[
\sum_{t/n \in \mathcal{M}(b, a)} |S_{d,n}(t/n)| \ll \frac{dn}{\phi(d) \phi(b)} \log R.
\]
**Proof.** Suppose that \( t/n \in \mathcal{M}(b,a) \). Then
\[
\left| \frac{t}{n} - \frac{a}{b} \right| \leq \frac{R}{n \log \log R} \leq \frac{\log n}{n},
\]
and since \( b \leq R \leq \log n \) we can, for large enough \( n \), apply Lemma 4 with \( \alpha \) replaced by \( t/n \).

Let \( u \) and \( v \) be integers such that
\[
\frac{u}{n} < \frac{a}{b} < \frac{v}{n}, \quad v - u = 2.
\]
Applying Lemma 4 we obtain
\[
\sum_{t/n \in \mathcal{M}(b,a), u/n \leq t/n \leq v/n} |S_{d,n}(t/n)| \ll \frac{dn}{\phi(d) \phi(b)}.
\]
For \( t/n \in \mathcal{M}(b,a) \) with \( t/n < u/n \), Lemma 4 implies
\[
|S_{d,n}(t/n)| \ll \frac{d}{\phi(d) \phi(b)} \left| \frac{t}{n} - \frac{a}{b} \right|^{-1} \ll \frac{d}{\phi(d) \phi(b)} \left| \frac{t}{n} - \frac{u}{n} \right|^{-1}.
\]
Therefore
\[
\sum_{t/n \in \mathbb{N}(b,a) \atop t/n < u/n} |S_{d,n}(t/n)| \ll \frac{dn}{\phi(d)\phi(b)} \sum_{t/n \in \mathbb{N}(b,a) \atop t/n < u/n} \frac{1}{|t-u|}
\]
\[
\ll \frac{dn}{\phi(d)\phi(b)} \sum_{1 \leq m \leq R/\log \log R} \frac{1}{m} \ll \frac{dn}{\phi(d)\phi(b)} \log R.
\]

Similarly
\[
\sum_{t/n \in \mathbb{N}(b,a) \atop v/n < t/n} |S_{d,n}(t/n)| \ll \frac{dn}{\phi(d)\phi(b)} \log R.
\]

The result follows. □

A multiplicative arithmetic function \( f \) is called strongly multiplicative if \( f(p^k) = f(p) \) for every prime \( p \) and positive integer \( k \). The next lemma contains a standard deduction on the average order over arithmetic progressions for certain strongly multiplicative arithmetic functions.

**Lemma 7.** Let \( x \) be a real number such that \( x \geq 1 \), and let \( d \) and \( r \) be positive integers. If \( f \) is a strongly multiplicative arithmetic function such that \( f(m) \geq 1 \) for every positive integer \( m \) and \( f(p) = 1 + O(p^{-1}) \). Then
\[
\sum_{m \leq x \atop m \equiv r \mod d} f(m) \ll f((r,d)) \frac{x}{d}.
\]

**Proof.** Let \( g \) be the arithmetic function defined by
\[
g(m) = \sum_{k|m} \mu\left(\frac{m}{k}\right) f(k),
\]
where \( \mu \) is the Möbius function. Using the fact that \( f \) is strongly multiplicative we deduce that
\[
g(m) = \mu(m)^2 \prod_{p|m} (f(p) - 1).
\]

Since \( f(m) \geq 1 \) for every positive integer \( m \) it follows that \( g \) is a non-negative valued arithmetic function. By the Möbius inversion formula \( f(m) = \sum_{k|m} g(k) \), therefore
\[
\sum_{m \leq x \atop m \equiv r \mod d} f(m) = \sum_{m \leq x \atop m \equiv r \mod d} \sum_{k|m} g(k) = \sum_{k \leq x} g(k) \sum_{m \leq x \atop m \equiv r \mod d} 1.
\]
The last sum above is zero if \((k, d) \nmid r\) and at most \(x(d, k)/(dk)\) if \((k, d) \mid r\). This implies, since \(g\) is a non-negative valued function, that

\[
\sum_{m \leq x \atop m \equiv r \mod d} f(m) \leq \frac{x}{d} \sum_{k \leq x \atop (k, d) \mid r} \frac{g(k)(k, d)}{k} = \frac{x}{d} \sum_{s \mid (r, d)} \sum_{k \leq x \atop (k, d) = s} \frac{g(k)}{k} = \frac{x}{d} \sum_{s \mid (r, d)} \sum_{l \leq x/s \atop (l, d/s) = 1} \frac{g(sl)}{l}.
\]

For positive integers \(u\) and \(v\) it can be verified that \(g(uv) \leq g(u)g(v)\), thus

\[
\sum_{m \leq x \atop m \equiv r \mod d} f(m) \leq \frac{x}{d} \sum_{s \mid (r, d)} \sum_{l \leq x} \frac{g(s)g(l)}{l} \\
\leq f((r, d)) \frac{x}{d} \prod_{p \leq x} \left(1 + \frac{1}{p}\right) = f((r, d)) \frac{x}{d} \prod_{p \leq x} \left(1 + \frac{f(p) - 1}{p}\right).
\]

Since \(f(p) \geq 1\) and \(f(p) = 1 + O(p^{-1})\) the previous product is bounded from above by the absolutely convergent infinite product \(\prod_p (1 + p^{-1}(f(p) - 1))\). Therefore

\[
\sum_{m \leq x \atop m \equiv r \mod d} f(m) \ll f((r, d)) \frac{x}{d}.
\]

\[\square\]

The next lemma is analogous to Proposition 11 of Green [4].

**Lemma 8.**

\[
\sum_{t=0}^{n-1} |S_{d, n}(t/n)|^4 \ll \left(\frac{dn}{\phi(d)}\right)^4.
\]

**Proof.** By Gallagher’s inequality [9, Lemma 1.2] we have

\[
\sum_{t=0}^{n-1} |S_{d, n}(t/n)|^4 \leq n \int_0^1 |S_{d, n}(\alpha)|^4 d\alpha + 2 \int_0^1 |S_{d, n}(\alpha)^3 S'_{d, n}(\alpha)| d\alpha,
\]

where \(S'_{d, n}(\alpha)\) is the derivative of \(S_{d, n}(\alpha)\) with respect to \(\alpha\). By H"older’s inequality

\[
\int_0^1 |S_{d, n}(\alpha)^3 S'_{d, n}(\alpha)| d\alpha \leq \left(\int_0^1 |S_{d, n}(\alpha)|^4 d\alpha\right)^{3/4} \left(\int_0^1 |S'_{d, n}(\alpha)|^4 d\alpha\right)^{1/4}.
\]
Let \( r_d(m) \) denote the number of pairs \((p_1, p_2)\) where \( p_1 \) and \( p_2 \) are primes such that \( p_1, p_2 \equiv 1 \pmod d \) and
\[
\frac{p_1 - 1}{d} + \frac{p_2 - 1}{d} = m.
\]

By Parseval’s identity,
\[
\int_0^1 |S_{d,n}(\alpha)|^4 d\alpha \leq (\log n)^4 \sum_{m \leq n} r_d(m)^2
\]
and
\[
\int_0^1 |S'_{d,n}(\alpha)|^4 d\alpha \leq 2\pi (n \log n)^4 \sum_{m \leq n} r_d(m)^2.
\]

From the above we deduce that
\[
(5) \sum_{t=0}^{n-1} |S_{d,n}(t/n)|^4 \ll n(\log n)^4 \sum_{m \leq n} r_d(m)^2.
\]

For each positive integer \( m \) we have
\[
r_d(m) \leq |\{ p : 1 < p \leq dm+2, p \equiv 1 \pmod d, dm+2 - p \text{ is a prime} \}|.
\]

To bound \( r_d(m) \) we apply the combinatorial sieve to estimate the size of the set above. In particular, Corollary 2.4.1 of [5] implies
\[
r_d(m) \ll \prod_{p \mid (dm+2)} \left(1 - \frac{1}{p}\right)^{-1} \frac{dm + 1}{\phi(d) \log^2((dm+1)/d)}.
\]

Note that
\[
\prod_{p \mid (dm+2)} \left(1 - \frac{1}{p}\right)^{-1} \leq \frac{d}{\phi(d)} \left(\frac{dm + 2}{\phi(dm+2)}\right),
\]
therefore
\[
r_d(m) \ll \frac{d^2m}{\phi(d)^2(\log m)^2} \left(\frac{dm + 2}{\phi(dm+2)}\right).
\]

This implies
\[
\sum_{m \leq n} r_d(m)^2 \ll \frac{d^4n^2}{\phi(d)^4(\log n)^4} \sum_{u \equiv 2 \pmod d} \left(\frac{u}{\phi(u)}\right)^2.
\]

Let \( f(u) = (u/\phi(u))^2 \). It can verified that \( f \) is a strongly multiplicative arithmetic function such that \( f(u) \geq 1 \) for every positive integer \( u \) and
Thus, we can apply Lemma 7 to obtain
\[ \sum_{u \leq dn + 2 \mod d} \left( \frac{u}{\phi(u)} \right)^2 \ll n. \]
Therefore
\[ \sum_{m \leq n} r_d(m)^2 \ll \frac{d^2 n^3}{\phi(d)^2 (\log n)^4}, \]
and thus, on account of (3), the result follows. \( \square \)

4. A DENSITY INCREMENT

Throughout this section \( n \) denotes a positive integer and \( A \) a subset of \( \{1, \ldots, n\} \). For any real \( \alpha \) we set
\[
F(\alpha) = \sum_{a \in A} e(\alpha a), \quad F_1(\alpha) = \sum_{a \in A \atop a \leq n/2} e(\alpha a).
\]
We denote by \( C_1 \) a fixed positive constant. This constant will be used throughout the rest of the paper. We will need \( C_1 \) to be sufficiently large, but it should be noted that the size of \( C_1 \) will never be determined by \( n \) or \( A \). Let \( \delta \) denote the density of \( A \), that is, \( |A| = \delta n \). The following parameters are defined in terms of \( C_1 \) and \( \delta \).

(6) \[ R(\delta) = (C_1 \delta^{-1})^{(\log \log C_1 \delta^{-1})^7/8}, \]
(7) \[ \theta(\delta) = (C_1 \delta^{-1})^{-4(\log \log \log C_1 \delta^{-1})^{-1}}, \]
(8) \[ Q_1 = (C_1 \delta^{-1})^{(\log \log \log C_1 \delta^{-1})^{1/8}}, \]
(9) \[ \Lambda = \left[ \frac{3}{4} \log \log \log C_1 \delta^{-1} \right]. \]

With \( R = R(\delta) \) we let \( \mathcal{M}(q, a) \) be defined as in (3), and for any positive integer \( q \leq R \) we set
\[
\mathcal{M}(q) = \bigcup_{a=0 \atop (a, q) = 1}^q \mathcal{M}(q, a).
\]

**Lemma 9.** Let \( d \) be a positive integer such that \( d \leq \log n \). Suppose that \( A - A \) does not intersect \( S_d \) and that
\[
C_1 \delta^{-1} \leq e^{(\log \log n)^{1/2}}.
\]
Provided \( C_1 \) and \( n \) are sufficiently large there exists a positive integer \( q \leq R(\delta) \) such that

\[
\sum_{t=1}^{n-1} \frac{|F(t/n)|^2}{t/n \in \mathcal{M}(\varphi)} \geq \theta(\delta)|A|^2.
\]

**Proof.** Here we adopt the method used in [1]. Given any positive integer \( \lambda \) we make the following definitions. For integers \( a \) and \( k \), with \( k \geq 1 \), we define

\[
\mathcal{M}_\lambda(k, a) = \left\{ \alpha \in [0, 1] : \left| \alpha - \frac{a}{k} \right| \leq \frac{\lambda R}{n \log \log R} \right\},
\]

and for real numbers \( K, U \geq 1 \) we define

\[
\mathcal{P}_\lambda(K, U) = \left\{ \frac{a}{k} : 1 \leq a \leq k \leq K, (a, k) = 1, \max_{t/n \in \mathcal{M}_\lambda(k, a)} |F_1(t/n)| \geq |A|/U \right\}.
\]

Furthermore, we set

\[
Q_\lambda = Q_{1, \lambda}^{-1} \quad \text{and} \quad \mu_\lambda = \max_{1 \leq K \leq Q_\lambda} \frac{1 \leq U \leq U_\lambda^{-1}}{|\mathcal{P}_\lambda(K, U)| U^2}.
\]

Let \( K_\lambda \) and \( U_\lambda \) denote a pair for which \( \mu_\lambda \) takes its maximum. As \( K = U = 1 \) is considered in the definition of \( \mu_\lambda \) we have

\[
1 \leq \mu_\lambda \leq \frac{K_\lambda^2}{U_\lambda^2}.
\]

It follows that

\[
1 \leq U_\lambda \leq K_\lambda \leq Q_\lambda.
\]

For each \( \lambda \leq \Lambda \) we want that the intervals \( \mathcal{M}_\lambda(k, a) \) with \( k \leq Q_\lambda \) to be pairwise disjoint. It can be verified that this will happen if

\[
\frac{2\lambda R}{n \log \log R} < \frac{1}{Q_\lambda^2} \quad \text{(for } \lambda \leq \Lambda).\]

To show this is true we estimate \( \lambda, R, \) and \( Q_\lambda \) for \( \lambda \leq \Lambda \). By (9) and (10) we deduce that

\[
\lambda \leq \frac{3}{4} \log \log \log n \quad \text{(for } \lambda \leq \Lambda).\]

By (5) we find that \( 2^\lambda \leq (\log \log C_1 \delta^{-1})^{3/4} \), and thence by (8) and (12) we find that

\[
\log Q_\lambda \leq 2^\lambda \log Q_1 \leq (\log \log C_1 \delta^{-1})^{7/8} \log C_1 \delta^{-1}.
\]
By (6) this implies $\log Q_\lambda \leq \log R$, and so

$$Q_\lambda \leq R.$$  

(16)

By (6) and (10) we find, for $n$ large enough, that

$$3 \leq R \leq \log n.$$  

(17)

From the above estimates for $\lambda$, $R$, and $Q_\lambda$ we deduce that (15) holds for sufficiently large $n$. Therefore, when $\lambda \leq \Lambda$ we have

$$\mu_\lambda |A|^2 = |P_\lambda(K_\lambda, U_\lambda)| \frac{|A|^2}{U_\lambda^2} \leq \sum_{t=0}^{N-1} |F_1(t/n)|^2 \leq n|A|.$$  

So

$$\delta \leq \mu_\lambda^{-1}.$$  

(18)

Let us assume, to obtain a contradiction, that

$$\sum_{t/n \in \mathbb{M}(q)} |F(t/n)|^2 < \theta(\delta)|A|^2 \quad (for \ all \ 1 \leq q \leq R).$$  

(19)

By using Lemma 2 and (19) we will show, provided $C_1$ and $n$ are sufficiently large, that

$$\mu_{\lambda+1} \geq \theta(\delta)^{-1/2} \mu_\lambda \quad (for \ 1 \leq \lambda \leq \Lambda).$$  

(20)

Assuming for now that (20) holds we show how a contradiction is obtained, thus proving that the assumption (19) is false. Since $\mu_1 \geq 1$, it follows from (20) that $\mu_{\lambda+1} \geq \theta(\delta)^{-(1/2)^\lambda}$, and thus by (18) we have

$$\delta \leq \theta(\delta)^{(1/2)^\lambda}.$$  

We can take $C_1$ to be large enough so that (19) implies $\Lambda \geq (1/4) \log_3 C_1 \delta^{-1}$, then by (7) we find that

$$\delta \leq C_1^{-1} \delta < \delta,$$

a contradiction. Therefore (19) cannot hold for all $1 \leq q \leq R$.

We now proceed to show that (20) holds. To that end, let us fix $\lambda$ with $1 \leq \lambda \leq \Lambda$. For now we also fix a rational $a/k$ in $P_\lambda(U_\lambda, K_\lambda)$. We associate with $a/k$ a fraction $u/n \in \mathbb{M}(k, a)$ such that $|F(u/n)| \geq |A|/U_\lambda$. Such a $u/n$ exists by the way $a/k$ was chosen.

Since $A - A$ contains no integers from $S_d$ we find that

$$\sum_{t=0}^{n-1} F_1(u/n + t/n)F(-t/n)S_{d,n}(t/n) = 0.$$
By the triangle inequality, Lemma 3 and the way \( u/n \) was chosen we find that
\[
|A|^2 \frac{dn}{\phi(d)} \ll \sum_{t=1}^{n-1} |F_1(u/n + t/n)| |F(t/n)| |S_{d,n}(t/n)|.
\]

Set
\[
Y = (C_1 \delta^{-1})^{3/2} Q_A^2
\]
and let \( \mathcal{N} \) denote the set of \( t/n \) such that \(|F(t/n)| \leq |A|/Y\). By two applications of the Cauchy-Schwartz inequality, Parseval’s identity, and Lemma 8 we find that
\[
\sum_{t/n \in \mathcal{N}} |F_1(u/n + t/n)| |F(t/n)| |S_{d,n}(t/n)| \ll \frac{dn^{3/2} |A|^{1/2}}{\phi(d)} \left( \sum_{t/n \in \mathcal{N}} |F(t/n)|^4 \right)^{1/4}.
\]

Now
\[
\left( \sum_{t/n \in \mathcal{N}} |F(t/n)|^4 \right)^{1/4} \leq \max_{t/n \in \mathcal{N}} |F(t/n)|^{1/2} \left( \sum_{t=0}^{n-1} |F(t/n)|^2 \right)^{1/4} \leq \frac{|A|^{1/2}}{Y^{1/2}} \cdot \left( n |A| \right)^{1/4} = \frac{n^{1/4} |A|^{3/4}}{Y^{1/2}}.
\]
Therefore
\[
\sum_{t/n \in \mathcal{N}} |F_1(u/n + t/n)| |F(t/n)| |S_{d,n}(t/n)| \ll \frac{dn^{7/4} |A|^{5/4}}{\phi(d) Y^{1/2}}.
\]

By (14) and (22) we find that
\[
Y^{-1/2} = C_1^{-3/4} \delta^{3/4} Q_A^{-1} \leq C_1^{-3/4} |A|^{3/4} n^{-3/4} U^{-1},
\]
thus
\[
\sum_{t/n \in \mathcal{N}} |F_1(u/n + t/n)| |F(t/n)| |S_{d,n}(t/n)| \ll C_1^{-3/4} |A|^2 \left( \frac{dn}{\phi(d)} \right).
\]
Let \( \mathcal{N}_1 \) denote the set of \( t/n \) such that \( |F_1(u/n + t/n)| \leq |A|/Y \). By the same reasoning used in the deduction of (23) we find that

\[
(24) \quad \sum_{t/n \in \mathcal{N}_1} |F_1(u/n + t/n)||F(t/n)||S_{d,n}(t/n)| \ll C_1^{-3/4}|A|^2 \left( \frac{dn}{\phi(d)} \right).
\]

For \( \lambda \leq \Lambda \) we have \( Q_{\lambda+1}/Q_\lambda < R \). Indeed, (9) and (12) imply

\[
Q_{\lambda+1} / Q_\lambda \leq (C_1 \delta^{-1})^{(\log \log C_1 \delta^{-1})^{3/4}} < R.
\]

Let \( m^* \) denote the union of the \( \mathfrak{M}(q) \) with \( Q_{\lambda+1}/Q_\lambda \leq q \leq R \). By the Cauchy-Schwartz inequality we find that

\[
(25) \quad \sum_{t/n \in m^*} |F_1(u/n + t/n)||F(t/n)||S_{d,n}(t/n)| \leq (n|A|) \sup_{t/n \in m^*_\lambda} |S_{d,n}(t/n)|.
\]

We are now going to show that

\[
(26) \quad \sup_{t/n \in m^*_\lambda} |S_{d,n}(t/n)| \ll C_1^{-1}U_\lambda^{-1} \delta \left( \frac{dn}{\phi(d)} \right).
\]

Suppose that \( t/n \in m^* \), then \( t/n \in \mathfrak{M}(q, a) \) for some integers \( a \) and \( q \) such that \( 0 \leq a \leq q \), \( (a, q) = 1 \), and \( Q_{\lambda+1}/Q_\lambda \leq q \leq R \). Since \( q \leq R \leq \log n \), we deduce from Lemma 4 that

\[
S_{d,n}(t/n) \ll \frac{dn}{\phi(d)\phi(q)}.
\]

Using the well-known estimate

\[
(27) \quad \phi(q) \gg \frac{q}{\log \log q},
\]

(see for example [7, Theorem 328]), we obtain

\[
(28) \quad S_{d,n}(t/n) \ll \left( \frac{dn}{\phi(d)} \right) \frac{\log \log q}{q}.
\]

The lower bound on \( q \) implies

\[
(29) \quad \frac{\log \log q}{q} \ll \frac{\log \log Q_{\lambda+1}/Q_\lambda}{Q_{\lambda+1}/Q_\lambda}.
\]

By (12) we have \( Q_{\lambda+1}/Q_\lambda = Q_\lambda Q_1 = Q_1^{2\lambda} \), thus

\[
\frac{\log \log Q_{\lambda+1}/Q_\lambda}{Q_{\lambda+1}/Q_\lambda} = \frac{\log \log Q_1^{2\lambda}}{Q_\lambda Q_1} = \frac{\lambda(\log 2) + \log \log Q_1}{Q_\lambda Q_1}.
\]
Using (8) and (9) we find that \( \lambda \ll \frac{\log \log Q}{Q} \). By this and (14) we obtain

\[
\frac{\log \log Q_{1+\lambda}/Q_\lambda}{Q_{1+\lambda}/Q_\lambda} \ll \frac{\log \log Q_1}{U_\lambda Q_1}.
\]

Using (8) we find, by taking \( C_1 \) large enough, that

\[
\log \left( \frac{\log \log Q_1}{Q_1} \right) \leq -\log C_1 \delta^{-1},
\]

and thus

\[
\frac{\log \log Q_1}{Q_1} \leq C_1^{-1}\delta.
\]

From (29) and the subsequent estimates we obtain

\[
(30) \log \log q \ll C_1^{-1}\delta.
\]

Since \( t/n \in \mathfrak{m}^* \) is arbitrary (28) and (30) imply that (26) is true. By (25) and (26) we have

\[
(31) \sum_{t/n \in \mathfrak{m}^*} |F_1(u/n + t/n)||F(t/n)||S_{d,n}(t/n)| \ll C_1^{-1}|A|^2 \frac{dn}{\phi(d)} \left( \frac{d}{\phi(d)} \right).
\]

The contribution to the sum in (21) coming from the terms with \( t/n \in \mathfrak{m} \) can similarly be bounded. By the Cauchy-Schwartz inequality and Lemma 5 we find that

\[
\sum_{t/n \in \mathfrak{m}} |F_1(u/n + t/n)||F(t/n)||S_{d,n}(t/n)| \leq (n|A|) \sup_{t/n \in \mathfrak{m}} |S(t/n)|
\]

\[
\ll (n|A|) \left( \frac{dn}{\phi(d)} \right) \log \log R \frac{R}{R}.
\]

Since \( R \geq Q_{\lambda+1}/Q_\lambda \) the argument used the previous paragraph implies

\[
(32) \sum_{t/n \in \mathfrak{m}} |F_1(u/n + t/n)||F(t/n)||S_{d,n}(t/n)| \ll C_1^{-1}|A|^2 \frac{dn}{\phi(d)} \left( \frac{d}{\phi(d)} \right).
\]

Let \( \mathfrak{N}(b, a) \) be the set of \( t/n \in \mathfrak{M}(b, a) \) with \( t/n \neq 0 \) such that

\[
|F(t/n)| \geq \frac{|A|}{Y}, \quad |F_1(u/n + t/n)| \geq \frac{|A|}{Y}.
\]

By (23), (24), (31), and (32) it follows for \( C_1 \) large enough that

\[
\frac{d|A|^2n}{\phi(d)U_\lambda} \ll
\sum_{b \leq Q_{\lambda+1}/Q_\lambda} \sum_{(a, b) = 1} \max_{t/n \in \mathfrak{N}(b, a)} |F(t/n)| \max_{t/n \in \mathfrak{N}(b, a)} |F_1(u/n + t/n)| \sum_{t/n \in \mathfrak{N}(b, a)} |S_{d,n}(t/n)|.
\]
Since $d \leq \log n$ we can apply Lemma 6 to the inner sum above to obtain
\[
\frac{|A|^2}{U_\lambda \log R} \ll \sum_{b \leq Q_{\lambda+1}/Q_\lambda} \frac{1}{\phi(b)} \sum_{(a,b)=1} \max_{t/n \in \mathfrak{M}(b,a)} |F(t/n)| \max_{t/n \in \mathfrak{M}(b,a)} |F_1(u/n + t/n)|.
\]

Let $L(L, V, W)$ denote the set of reduced fractions $b/l \in [0, 1]$ such that
\[
\frac{L}{2} \leq l \leq L,
\]
\[
\frac{|A|}{V} \leq \max_{t/n \in \mathfrak{M}(l,b)} |F(t/n)| \leq 2 \frac{|A|}{V},
\]
\[
\frac{|A|}{W} \leq \max_{t/n \in \mathfrak{M}(l,b)} |F_1(u/n + t/n)| \leq 2 \frac{|A|}{W}.
\]

For $b/l \in L(L, V, W)$, we have
\[
\frac{1}{\phi(l)} \max_{t/n \in \mathfrak{M}(l,b)} |F(t/n)| \max_{t/n \in \mathfrak{M}(l,b)} |F_1(u/n + t/n)| \ll \frac{(\log \log 3L)|A|^2}{LVW}
\]
by (27). Therefore
\[
\frac{|A|^2}{U_\lambda \log R} \ll \sum_L \sum_V \sum_W |L(L, V, W)| \frac{(\log \log 3L)|A|^2}{LVW}.
\]

where $L$ runs through all the powers of 2 in the interval $[1, 2Q_{\lambda+1}/Q_{\lambda}]$, and $V$ and $W$ run through all the powers of 2 in the interval $[1, 2Y]$. There must exist a triple $(L, V, W)$ of such indices such that
\[
|L(L, V, W)| \gg \frac{LVW}{U_\lambda (\log \log 3L)(\log R)}.
\]
We associate this triple with $a/k$.

The number of possible triples $(L, V, W)$ is $\ll (Q_{\lambda+1}/Q_{\lambda})(\log Y)^2$, which by (16) and (22) is $\ll (\log R)^3$. Therefore there exists a subset $K \subset P_{\lambda}$, satisfying
\[
|K| \gg \frac{|P_\lambda(K, U_\lambda)|}{(\log R)^3},
\]
such that for each $a/k \in K$ we associate the same triple, say $(L, V, W)$.

Let $a/k \in K$, then together with the associated fraction $u/n \in \mathfrak{M}(k,a)$, we associate a set $L_{a/k}$ of rationals $b/l$, $0 \leq b \leq l$, $(b, l) = 1$, $L/2 \leq l \leq L$, such that
\[
|L_{a/k}| \gg \frac{LVW}{U_\lambda (\log \log 3L)(\log R)},
\]
\( \frac{|A|}{V} \leq \max_{v/n \in \mathcal{M}(l,b)} |F(v/n)| \leq \frac{2|A|}{V}. \)

(36)  \[ \frac{|A|}{W} \leq \max_{w/n \in \mathcal{M}(l,b)} |F_1(u/n + w/n)| \leq \frac{2|A|}{W}. \]

Set

\[ Q = \left\{ \frac{a}{k} + \frac{b}{l} : \frac{a}{k} \in \mathcal{K}, \frac{b}{l} \in \mathcal{L}_{a/k} \right\}. \]

Let us estimate the cardinality of \( Q \). Since \( L \leq Q_{\lambda+1}/Q_{\lambda} \leq R \), assumption (19) and (35) imply

\[ \left| \left\{ b : \frac{b}{l} \in \bigcup \mathcal{L}_{a/k} \right\} \right| \leq \theta(\delta)|A|^2. \]

So that \( \left| \left\{ b : \frac{b}{l} \in \bigcup \mathcal{L}_{a/k} \right\} \right| \ll \theta(\delta)V^2. \)

Lemma 2 then implies

\[ |Q| \gg |\mathcal{K}| \cdot \frac{L^2 V^2 W^2}{U_\lambda^2 (\log \log 3L)^2 (\log R)^2} \cdot \frac{\theta(\delta)^{-1}}{LV^2 \tau^8 (1 + \log K_{\lambda})}. \]

From (14) and (16) we obtain \( \log K_{\lambda} \leq \log R \), by this and (33) it follows that

\[ |Q| \gg W^2 \left( \frac{\theta(\delta)^{-1}}{\tau^8 (\log R)^6} \right) \frac{|P_\lambda(K_{\lambda}, U_{\lambda})|}{U_\lambda^2}. \]

Note that \( Q \) is a subset of \((0, 2]\). Let \( Q_1 = Q \cap (0, 1] \) and \( Q_2 = Q \cap (1, 2]\). Let us assume without loss of generality that \( |Q_1| \geq (1/2)|Q| \). If this is not the case, then \( |Q_2| \geq (1/2)|Q| \), and we can replace \( Q_1 \) in the argument below by the rational numbers in \( Q_2 \) shifted to the left by 1. Since \( |Q_1| \geq (1/2)|Q| \) we see that (37) is still valid with \( Q \) replaced by \( Q_1 \).

Let \( r/s = a/k + b/l \) be in \( Q_1 \). For \( u/n \in \mathcal{M}_\lambda(k,a) \) and \( w/n \in \mathcal{M}(l,b) \) we have

\[ \left| \frac{r}{s} - \left( \frac{u}{n} + \frac{w}{n} \right) \right| \leq \left| \frac{u}{n} - \frac{a}{k} \right| + \left| \frac{w}{n} - \frac{b}{l} \right| \leq \frac{(\lambda + 1)R}{n \log \log R}, \]

and therefore \( u/n + w/n \in \mathcal{M}_{\lambda+1}(s,r) \). Thus, by (36) we deduce that

\[ \max_{t/n \in \mathcal{M}_{\lambda+1}(s,r)} |F_1(t/n)| \geq \frac{|A|}{W} \quad \text{(for } r/s \in Q_1). \]

We now estimate the size of the denominator of \( r/s \). Certainly \( s \leq kl \leq K_{\lambda}L \). By (14) we have \( K_{\lambda} \leq Q_{\lambda} \) and \( L \) was chosen to satisfy
\[ L \leq Q_{\lambda+1}/Q_\lambda. \] Therefore \( s \leq Q_{\lambda+1} \) whenever \( r/s \in Q_1. \) By this and (38) we obtain
\[
Q_1 \subset \mathcal{P}_{\lambda+1}(Q_{\lambda+1}, W).
\]
By (37), with \( Q \) replaced by \( Q_1, \) and (39) we find that
\[
\frac{\left| \mathcal{P}_{\lambda+1}(Q_{\lambda+1}, W) \right|}{W^2} \gg \left( \frac{\theta(\delta)^{-1}}{\tau^{8}(\log R)^{6}} \right) \frac{\left| \mathcal{P}_{\lambda}(K_\lambda, U_\lambda) \right|}{U_\lambda^2}.
\]
This implies
\[
\mu_{\lambda+1} \gg \frac{\theta(\delta)^{-1}}{\tau^{8}(\log R)^{6}} \mu_\lambda.
\]
We now estimate \( \tau \) the maximum of the divisor function up to \( K_\lambda L \leq Q_{\lambda+1}. \) If \( d(m) \) is the number of divisors of \( m \) then
\[
\log d(m) \ll \frac{\log m}{\log \log m}.
\]
(see [7, Theorem 317]). Thus, by (12), we have
\[
\log \tau \ll \frac{\log Q_{\lambda+1}}{\log \log Q_{\lambda+1}} \ll \frac{2^\lambda \log Q_1}{\log \log Q_1},
\]
and since \( \lambda \leq \Lambda \) we deduce from (8) and (9) that
\[
\log \tau \ll \frac{\log C_1 \delta^{-1}}{(\log \log C_1 \delta^{-1})^{1/4}}.
\]
It follows from (7) that
\[
\log \tau = o(\log \theta(\delta)^{-1}) \quad \text{(for } C_1 \delta^{-1} \to \infty)\).
\]
We also find from (6) and (7) that
\[
\log \log R = o(\log \theta(\delta)^{-1}) \quad \text{(for } C_1 \delta^{-1} \to \infty)\).
\]
Since \( \theta(\delta)^{-1} \) tends to infinity as \( C_1 \delta^{-1} \) tends to infinity, we deduce from (40), (41), and (42) that for \( C_1 \) sufficiently large
\[
\mu_{\lambda+1} \geq \theta(\delta)^{-1/2} \mu_\lambda.
\]
Since \( \lambda \leq \Lambda \) was arbitrary (20) is true, and as shown earlier the lemma can be deduced from this.

We now derive a density increment argument that will be iterated in the next section to prove our theorem.
Lemma 10. Let $d$ be a positive integer such that $d \leq \log n$. Suppose that $A - A$ does not intersect $S_d$ and that $\delta$, the density of $A$, satisfies (14). Provided $C_1$ and $n$ are sufficiently large there exist positive integers $d'$ and $n'$, and a subset $A'$ of $\{1, \ldots, n'\}$ of size $\delta n'$, such that $A' - A'$ does not intersect $S_{d'}$, and moreover;
$$
d \leq d' \leq R(\delta) d, \quad R(\delta)^{-2} n' \leq n, \quad \delta' \geq \delta (1 + 8^{-1} \theta(\delta)).$$

Proof. By the hypotheses Lemma 9 implies there exists a positive integer $q \leq R(\delta)$ such that (11) is true. With this $q$ and $U = R(\delta)/\log \log R(\delta)$ let $E$ be defined as in Lemma 1. Note that $M(q) \subset E$. The inequality (17) is still valid, thus $2\pi q U \leq 2\pi R(\delta)^2 \leq n$ for sufficiently large $n$. Therefore, we can apply Lemma 1 with $\theta = \theta(\delta)$ to deduce that there exists an arithmetic progression $P$ with difference $q$ such that

$$\text{(43)} \quad |P| \geq \frac{n \log \log R(\delta)}{32\pi q R(\delta)}$$

and

$$\text{(44)} \quad |A \cap P| \geq |P| \delta (1 + 8^{-1} \theta(\delta)).$$

Let $n' = |P|$. Then there exists an integer $c$ and subset $A'$ of $\{1, \ldots, n'\}$ such that $A \cap P = \{ c + qa' : a' \in A' \}$. Put $d' = dq$. Since $A - A$ does not intersect $S_d$, we deduce that $A'$ does not intersect $S_{d'}$. Let the size of $A'$ be $\delta' n'$. Then (14) implies

$$\delta' \geq \delta (1 + 8^{-1} \theta(\delta)).$$

To finish we need to estimate $n'$ and $d'$. Since $q \leq R(\delta)$ we find by (13) and for $C_1$ large enough that $n' \geq R(\delta)^{-2} n$, and clearly, $n' \leq n$. Now, again by the fact that $q \leq R(\delta)$, we obtain $q \leq d' = dq \leq R(\delta) q$. This completes the proof. \hfill \Box

5. Proof of the Theorem

Let us assume, for a contradiction, that the theorem is false. Then for $C_1$ and $n$ sufficiently large, there exists a subset $A$ of $\{1, \ldots, n\}$ of size $\delta n$, such that $A - A$ does not intersect $S$ and

$$\text{(45)} \quad \delta \geq C_1 \left( \frac{\log n}{(\log_3 n)^2 (\log_4 n)} \right)^{-\log_5 n}.$$

Set

$$\text{(46)} \quad Z = \left[ 64 \theta(\delta)^{-1} \log C_1 \delta^{-1} \right];$$

and put $d_0 = 1$, $n_0 = n$, $A_0 = A$, and $\delta_0 = \delta$. By using Lemma 10 repeatedly we can show that for each integer $k$, with $1 \leq k \leq Z$, there
are integers \( d_k \) and \( n_k \) and a subset \( A_k \) of \( \{1, \ldots, n_k\} \) of size \( \delta_k n_k \) such that \( A_k - A_k \) does not intersect \( S_{d_k} \). Moreover, \( d_k, n_k, \) and \( \delta_k \) satisfy
\[
d_{k-1} \leq d_k \leq R(\delta_{k-1})d_{k-1}, \quad R(\delta_{k-1})^{-2}n_{k-1} \leq n_k \leq n_{k-1},
\]
\[
\delta_k \geq \delta_{k-1}(1 + 8^{-1}\theta(\delta_{k-1})).
\]

Since \( d_0 = 1 \) and \( n_0 = n \), these estimates imply
\[
(47) \quad d_k \leq R(\delta)^k, \quad n_k \geq R(\delta)^{-2k}n, \quad \delta_k \geq \delta(1 + 8^{-1}\theta(\delta))^k.
\]

Let us show that we can actually perform this iteration \( Z \) many times. Let \( 0 \leq l \leq Z - 1 \), and suppose that we have performed this iteration \( l \) many times. To show that Lemma 10 can be applied a \((l+1)\)-th time we need to show that \( n_l \) is sufficiently large, \( d_l \leq \log n_l \), and that (10) is satisfied with \( \delta \) replaced by \( \delta_l \).

We begin by estimating \( n_l \). By (47) we obtain
\[
(48) \quad \log n_l \geq \log n - 2l \log R(\delta).
\]

Since \( l < Z \), (6) and (46) imply
\[
l \log R(\delta) \leq 64 \theta(\delta)^{-1}(\log C_1 \delta^{-1})^2(\log_2 C_1 \delta^{-1})^{7/8}.
\]

By (45) we obtain
\[
(\log C_1 \delta^{-1})^2(\log_2 C_1 \delta^{-1})^{3/4} \leq 2(\log_3 n)^2(\log_4 n)^{7/8}(\log_5 n)^2
\]
for large enough \( n \). By (7) and (45) we find, for \( n \) and \( C_1 \) sufficiently large, that
\[
\log \theta(\delta)^{-1} = \frac{4 \log C_1 \delta^{-1}}{\log_3 C_1 \delta^{-1}} \leq \log \left( \frac{\log_3 n}{(\log_3 n)^2(\log_4 n)} \right).
\]

(Here we used that \( (\log x)(\log_3 x)^{-1} \) is eventually increasing.) Therefore
\[
\theta(\delta)^{-1} \leq \frac{\log_2 n}{(\log_3 n)^2(\log_4 n)}.
\]

From the above we deduce, for \( n \) and \( C_1 \) large enough, that
\[
(49) \quad l \log R(\delta) \leq \log_2 n.
\]

Therefore, by (48),
\[
\log n_l \geq \log n - 2\log_2 n = \log \left( \frac{n}{(\log n)^2} \right),
\]
and so
\[
(50) \quad n_l \geq \frac{n}{(\log n)^2}
\]
for \( l < Z \). This shows that by taking \( n \) to be arbitrarily large, the same is true for \( n_l \).
We now show that \( d_l \leq \log n_l \). By (47) we have \( \log d_l \leq l \log R(\delta) \), and thus by (49) we obtain \( \log d_l \leq (1/2) \log n \). For large \( n \) this implies
\[
d_l \leq (\log n)^{1/2} \leq \log \frac{n}{(\log n)^2} \leq \log n_l
\]
by (50).

We leave it to the reader to verify that (45) and (50) imply, for \( n \) and \( C_1 \) sufficiently large, that (10) is satisfied with \( \delta \) and \( n \) replaced by \( \delta_l \) and \( n_l \) respectively. Finally, since \( A_l - A_l \) does not intersect \( S_{d_l} \), we can apply Lemma 10 to obtain the desired outcome.

Since (47) is true with \( k = Z \) we find that
\[
\log \delta_Z \geq Z \log \left(1 + 8^{-1} \theta(\delta)\right) - \log C_1 \delta^{-1}.
\]
Since \( 8^{-1} \theta(\delta) < 1 \), this implies
\[
\log \delta_Z \geq 16^{-1} Z \theta(\delta) - \log C_1 \delta^{-1}.
\]
(Here we used \( \log(1 + x) \geq x/2 \) for \( 0 \leq x \leq 1 \).) For \( C_1 \) large enough \( Z \geq 32 \theta(\delta)^{-1} \log C_1 \delta^{-1} \), thus
\[
\log \delta_Z \geq 2 \log C_1 \delta^{-1} - \log C_1 \delta^{-1} > 0.
\]
This implies \( \delta_Z > 1 \), a contradiction, since by definition \( \delta_Z \leq 1 \). This contradiction establishes the theorem.

**Acknowledgements**

The author was supported by a postdoctoral fellowship from the Centre de recherches mathématiques at Montréal.

**References**

[1] A. Balog, J. Pelikán, J. Pintz and E. Szemerédi, Difference sets without \( \kappa \)-powers, *Acta Math. Hungar.*, 65 (1994), 165-187.
[2] H. Furstenberg, Ergodic behaviour of diagonal measures and a theorem of Szemerédi on arithmetic progressions, *J. Analyse Math.*, 31 (1977), 204-256.
[3] W.T. Gowers, A new proof of Szemerédi’s theorem, *Geom. Funct. Anal.*, 11 (2001), 465-588.
[4] B. Green, On arithmetic structures in dense sets of integers, *Duke Math. J.*, 114 (2002), 215-238.
[5] H. Halberstam and H.-E. Richert, *Sieve Methods* (Academic Press, London, 1974).
[6] T. Kamae and M. Mendès France, Van der Corput’s difference theorem, *Israel J. Math.*, 31 (1978), 335-342.
[7] G.H. Hardy and E.M. Wright, *An introduction to the theory of numbers*, (Oxford University Press, Oxford, 1960)
[8] J. Lucier, Intersective sets given by a polynomial, *Acta Arith.*, 123 (2006), 57-95.
[9] H.L. Montgomery, *Topics in Multiplicative Number Theory*, Lecture Notes in Math., 127 (Springer-Verlag, Berlin, 1971).

[10] J. Pintz, W.L. Steiger and E. Szemerédi, On sets of natural numbers whose difference set contains no squares, *J. London Math. Soc.*, 37 (1988), 219-231.

[11] K. F. Roth, On certain sets of integers, *J. London Math. Soc.*, 28 (1953), 104-109.

[12] A. Sárközy, On difference sets of sequences on integers I, *Acta Math. Acad. Sci. Hungar.*, 31 (1978), 125-149.

[13] A. Sárközy, On difference sets of sequences on integers III, *Acta Math. Acad. Sci. Hungar.*, 31 (1978), 355-386.

Centre de recherches mathématiques
Université de Montréal
Case postale 6128, Succursale Centre-ville
Montréal, H3C 3J7
Canada