Combinatorics, Probability and Computing (2008) 17, 741–747. © 2008 Cambridge University Press
doi:10.1017/S0963548308009450 Printed in the United Kingdom

$B_2[g]$ Sets and a Conjecture of Schinzel and Schmidt

JAVIER CILLERUELO and CARLOS VINUESA[†‡]

Departamento de Matemáticas, Universidad Autónoma de Madrid, 28049-Madrid, Spain
(e-mail: franciscojavier.cilleruelo@uam.es, c.vinuesa@uam.es)

Received 27 May 2008; revised 29 July 2008; first published online 3 October 2008

A set of integers $\mathcal{A}$ is called a $B_2[g]$ set if every integer m has at most g representations of the form $m = a + a'$, with $a \leqslant a'$ and $a, a' \in \mathcal{A}$. We obtain a new lower bound for $F(g, n)$, the largest cardinality of a $B_2[g]$ set in $\{1, \ldots, n\}$. More precisely, we prove that $\liminf_{n\to\infty} \frac{F(g,n)}{\sqrt{gn}} \geqslant \frac{2}{\sqrt{\pi}} - \varepsilon_g$ where $\varepsilon_g \to 0$ when $g \to \infty$. We show a connection between this problem and another one discussed by Schinzel and Schmidt, which can be considered its continuous version.

1. Introduction

A set of integers $\mathcal{A}$ is called a $B_2[g]$ set if every integer m has at most g representations of the form $m = a + a'$, with $a \leqslant a'$ and $a, a' \in \mathcal{A}$. We write $r_{\mathcal{A}}(m)$ for the number of such representations.

A major problem in additive number theory is the study of the behaviour of the function $F(g, n)$, the largest cardinality of a $B_2[g]$ set in $\{1, \ldots, n\}$.

It is a well-known result on Sidon sets that $F(1, n) \sim n^{1/2}$, but the asymptotic behaviour of $F(g, n)$ is an open problem for $g \geqslant 2$. The trivial counting argument gives $F(g, n) \leqslant 2\sqrt{gn}$ and it is not too difficult to show (see Section 2) that $F(g, n) \gtrsim \sqrt{gn}$.

We define

$$\beta(g) = \liminf_{n\to\infty} \frac{F(g,n)}{\sqrt{gn}} \leqslant \limsup_{n\to\infty} \frac{F(g,n)}{\sqrt{gn}} = \alpha(g).$$

In the last few years some progress has been made, improving the easier estimates $1 \leqslant \beta(g) \leqslant \alpha(g) \leqslant 2$. In Table 1 we list successive results obtained by several authors, including the improvement obtained in this work.

† This work was developed during the Doccourse in Additive Combinatorics held in the Centre de Recerca Matemàtica from January to March 2007. The authors are extremely grateful for their hospitality.
‡ Both authors are supported by Grants CCG07-UAM/ESP-1814 and DGICYT MTM 2005-04730 (Spain).

Table 1.

$\alpha(g)$	$\leqslant 2$	trivial
	$\leqslant 1.864$	Cilleruelo, Ruzsa and Trujillo [1]
	$\leqslant 1.844$	Green [2]
	$\leqslant 1.839$	Martin and O'Bryant [5]
	$\leqslant 1.789$	Yu [9]
$\beta(g)$	$\geqslant 1$	Kolountzakis [3]
	$\gtrsim 1.060$	Cilleruelo, Ruzsa and Trujillo [1]
	$\gtrsim 1.122$	Martin and O'Bryant [4]
	$\gtrsim 2/\sqrt{\pi} = 1.128\cdots$	Corollary 1.2

The aim of this work is not only to improve the lower bound for $\beta(g)$ but also to show a connection with another problem discussed by Schinzel and Schmidt [7], which can be seen as the continuous version of this problem.

We define the Schinzel–Schmidt constant

$$S = \sup_{f\in\mathcal{F}} \frac{1}{|f * f|_\infty}, \tag{1.1}$$

where $\mathcal{F} = \{f : f \geqslant 0, \operatorname{supp}(f) \subseteq [0,1], |f|_1 = 1\}$ and $f * f(x) = \int f(t)f(x-t)\,dt$. We use the notation $|g|_1 = \int_0^1 |g(x)|\,dx$, $|g|_\infty = \sup_x g(x)$ and $\operatorname{supp}(g) = \{x : g(x) \neq 0\}$.

Remark. The definition in [7] is $S = \sup_{f\in\widetilde{\mathcal{F}}} |f|_1^2/|f * f|_\infty$ with $\widetilde{\mathcal{F}} = \{f : f \geqslant 0, f \not\equiv 0, \operatorname{supp}(f) \subseteq [0,1], f \in L_1[0,1]\}$, but we can assume that $|f|_1 = 1$ because $|f|_1^2/|f * f|_\infty$ is invariant under dilates of f.

It is easy to see that $1 \leqslant S \leqslant 2$, and Schinzel and Schmidt proved in [7] that $4/\pi \leqslant S \leqslant 1.7373$. The witness for the lower bound is the function $f(x) = \frac{1}{2\sqrt{x}} \in \mathcal{F}$. They also conjecture that $S = 4/\pi$. Our main theorem relates $\alpha(g)$ and $\beta(g)$ to S.

Theorem 1.1. $\sqrt{S} \leqslant \liminf_{g\to\infty} \beta(g) \leqslant \limsup_{g\to\infty} \alpha(g) \leqslant \sqrt{2S}$.

Corollary 1.2. $\beta(g) \geqslant 2/\sqrt{\pi} - \varepsilon_g$, *where* $\varepsilon_g \to 0$ *when* $g \to \infty$.

2. Lower bound constructions

At this point, it is convenient to introduce a few definitions.

Definitions. **(1)** We say that $\mathcal{A}$ is a $B_2^*[g]$ *set* if any integer n has at most g representations of the form $n = a + a'$ with $a, a' \in \mathcal{A}$. We write $r_{\mathcal{A}}^*(n)$ for the number of such representations.

(2) We say that $\mathcal{A}$ is a *Sidon set* (mod m) if $a_1 + a_2 \equiv a_3 + a_4 \pmod m \implies \{a_1, a_2\} = \{a_3, a_4\}$, where $a_i \in \mathcal{A}$.

All the known lower bounds for $\beta(g)$ were obtained from the next lemma (see [1]).

Lemma 2.1. *Let $\mathcal{A} = \{0 = a_1 < \cdots < a_k\}$ be a $B_2^*[g]$ set and let $\mathcal{C} \subseteq [1, m]$ be a Sidon set* (mod m)*. Then $\mathcal{B} = \cup_{i=1}^{k}(\mathcal{C} + ma_i)$ is a $B_2[g]$ set in $[1, m(a_k + 1)]$ with $k|\mathcal{C}|$ elements.*

Remark. The lemma shows how to obtain a $B_2[g]$ set by carefully arranging (with a dilation of a $B_2^*[g]$ set) several copies of a Sidon set (mod m).

Proof. To prove that $\mathcal{B}$ is a $B_2[g]$ set, suppose that we have

$$b_{1,1} + b_{2,1} = \cdots = b_{1,g+1} + b_{2,g+1} \tag{2.1}$$

for some $b_{1,j}, b_{2,j} \in \mathcal{B}$. We can write each $b_{i,j} = c_{i,j} + ma_{i,j}$ in a unique way with $c_{i,j} \in \mathcal{C}$ and $a_{i,j} \in \mathcal{A}$. Let us order the elements $b_{i,j}$ of each sum in such a way that for any i, j we have $c_{1,j} \leqslant c_{2,j}$, and when $c_{1,j} = c_{2,j}$ we order them so $a_{1,j} \leqslant a_{2,j}$.

To see that $\mathcal{B}$ is a $B_2[g]$ set we need to check that there exist j and j' such that $b_{1,j} = b_{1,j'}$, $b_{2,j} = b_{2,j'}$.

From (2.1), and since $\mathcal{C}$ is a Sidon set (mod m), we get $\{c_{1,1}, c_{2,1}\} = \{c_{1,j}, c_{2,j}\}$ for every $1 \leqslant j \leqslant g + 1$. Moreover, since have we ordered the elements of the equalities in that way, we have $c_{1,1} = c_{1,j}$ and $c_{2,1} = c_{2,j}$ for every j.

Then, the equalities (2.1) imply these equations:

$$a_{1,1} + a_{2,1} = a_{1,2} + a_{2,2} = \cdots = a_{1,g+1} + a_{2,g+1}. \tag{2.2}$$

Since $\mathcal{A}$ satisfies the $B_2^*[g]$ condition, there exist j and j' such that $a_{1,j} = a_{1,j'}$ and $a_{2,j} = a_{2,j'}$. Then, for these j and j' we have that $b_{1,j} = b_{1,j'}$ and $b_{2,j} = b_{2,j'}$. This proves that $\mathcal{B} \in B_2[g]$. Finally, it is clear that $B \subset \{1, \ldots, (a_k + 1)m\}$ and $|\mathcal{B}| = k|\mathcal{C}|$. □

In order to apply Lemma 2.1 in an efficient way, we have to take dense Sidon sets (mod m). For example, for each prime p we consider $\mathcal{C}_p$, the Sidon set (mod m) with $p - 1$ elements and $m = p(p - 1)$ discovered by Ruzsa (see [6]).

Given a positive integer N, we write

$$(a_k + 1)p_n(p_n - 1) < N \leqslant (a_k + 1)p_{n+1}(p_{n+1} - 1)$$

for suitable consecutive primes, p_n and p_{n+1}. Clearly

$$\frac{F(g, N)}{\sqrt{gN}} \geqslant \frac{|\mathcal{C}_{p_n}|k}{\sqrt{g(a_k + 1)p_{n+1}(p_{n+1} - 1)}} \geqslant \frac{k}{\sqrt{g(a_k + 1)}} \cdot \frac{p_n - 1}{p_{n+1}}.$$

Thus

$$\beta(g) = \liminf_{N \to \infty} \frac{F(g, N)}{\sqrt{gN}} \geqslant \frac{k}{\sqrt{g(a_k + 1)}} \liminf_{n \to \infty} \frac{p_n - 1}{p_{n+1}}.$$

Since $\liminf_{n \to \infty} \frac{p_n}{p_{n+1}} = 1$, as a consequence of the Prime Number Theorem, we get

$$\beta(g) \geqslant \frac{k}{\sqrt{g(a_k + 1)}}. \tag{2.3}$$

So, to improve the lower bound for $\beta(g)$, we need to find a set $\mathcal{A} = \{0 = a_1 < \cdots < a_k\}$ which satisfies the $B_2^*[g]$ condition and maximizes the quotient $\frac{k}{\sqrt{g(a_k+1)}}$.

The sets

(a) $\mathcal{A} = \{0, 1, \dots, g-1\}$,
(b) $\mathcal{A} = \{0, 1, \dots, g-1\} \cup \{g+1, g+3, \dots, g-1+2\lfloor g/2 \rfloor\}$,
(c) $\mathcal{A} = \big[0, \lfloor g/3 \rfloor\big) \cup \big(g - \lfloor g/3 \rfloor + 2 \cdot \big[0, \lfloor g/6 \rfloor\big)\big) \cup \big[g, g + \lfloor g/3 \rfloor\big)$
$\cup \big(2g - \lfloor g/3 \rfloor, 3g - \lfloor g/3 \rfloor\big]$

provide, respectively, the lower bounds

(a) $\beta(g) \geqslant 1$,
(b) $\beta(g) \geqslant \frac{g + \lfloor g/2 \rfloor}{\sqrt{g^2 + 2g\lfloor g/2 \rfloor}} \geqslant \sqrt{\frac{9}{8}} - \varepsilon_g = 1.060\cdots - \varepsilon_g$,
(c) $\beta(g) \geqslant \frac{g + 2\lfloor \frac{g}{3} \rfloor + \lfloor \frac{g}{6} \rfloor}{\sqrt{3g^2 - g\lfloor \frac{g}{3} \rfloor + g}} \geqslant \sqrt{\frac{121}{96}} - \varepsilon_g = 1.122\cdots - \varepsilon_g$,

cited in the Introduction. In the next section we will find a denser set $\mathcal{A}$.

3. The conjecture of Schinzel and Schmidt

The convolution $f * f$ in the conjecture of Schinzel and Schmidt can be thought of as the continuous version of the function $r^*_{\mathcal{A}}(n)$ and $|f * f|_\infty$ as the analogue of the maximum of $r^*_{\mathcal{A}}(n)$.

The idea is to start with a function $f \in \mathcal{F}$ such that $1/|f * f|_\infty$ is close to S (see (1.1)) and use f as a model to construct our set $\mathcal{A}$. We will use the probabilistic method.

An interesting result in [7] relates the constant S with the coefficients of squares of polynomials. We state that result in a more convenient way for our purposes.

Theorem 3.1. *For any $\varepsilon > 0$, for any $n > n(\varepsilon)$, there exists a sequence of non-negative real numbers $c_0, \dots, c_{n-1}$ such that:*

(i) $\sum_{j=0}^{n-1} c_j = \sqrt{n}$,
(ii) $c_j \leqslant n^{-1/6}(1+\varepsilon)$ *for all* $j = 0, \dots, n-1$,
(iii) $\sum_{j<m/2} c_j c_{m-j} \leqslant \frac{1}{2S}(1+\varepsilon)$ *for any* $m = 0, \dots, n-1$.

Proof. We follow the ideas of the proof of assertion (iii) of Theorem 1 in [7]. Let $f \in \mathcal{F}$ with $|f * f|_\infty$ close to $1/S$, say $|f * f|_\infty \leqslant 1/S + 1/n$, and define, for $j = 0, \dots, n-1$,

$$a_j = \frac{n}{2t} \int_{(j+1/2-t)/n}^{(j+1/2+t)/n} f(x)\, dx,$$

where $t = \lceil 2n^{1/3} \rceil$. We have the following estimate:

$$\begin{aligned}
\left(\int_r^s f(x)\, dx \right)^2 &\leqslant \iint\limits_{2r \leqslant x+y \leqslant 2s} f(x) f(y)\, dx\, dy \\
&= \int_{2r}^{2s} \left(\int f(x) f(z-x)\, dx \right) dz \\
&= \int_{2r}^{2s} f * f(z)\, dz \leqslant 2(s-r)(1/S + 1/n) \leqslant 4(s-r),
\end{aligned}$$

where in the last inequality we used the fact that $S \geqslant 1$ and $n \geqslant 1$.

In particular, we can deduce $a_j \leqslant (2n/t)^{1/2}$. The idea for proving Theorem 1(iii) in [7] consists of showing that $\sum_{j=0}^{n-1} a_j \geqslant n + o(n)$ and $\sum_{j=0}^{m} a_j a_{m-j} \leqslant (1/S)(n + o(n))$ for all m. See [7] for details.

We define $c_j = a_j \rho$, where $\rho = \frac{\sqrt{n}}{\sum_{j=0}^{n-1} a_j}$. Clearly $\rho \leqslant (1/\sqrt{n})(1 + o(1))$, so

$$c_j \leqslant n^{-1/6}(1 + o(1)), \quad \sum_{j=0}^{n-1} c_j = \sqrt{n} \quad \text{and} \quad \sum_{j=0}^{m} c_j c_{m-j} \leqslant (1/S)(1 + o(1)). \qquad \square$$

4. The proof

We will use a special case of Chernoff's inequality (see Corollary 1.9 in [8]).

Proposition 4.1 (Chernoff's inequality). *Let $X = t_1 + \cdots + t_n$, where the t_i are independent Boolean random variables. Then, for any $\delta > 0$,*

$$\mathbb{P}(|X - \mathbb{E}(X)| \geqslant \delta \mathbb{E}(X)) \leqslant 2e^{-\min(\delta^2/4, \delta/2)\mathbb{E}(X)}. \tag{4.1}$$

Given $\varepsilon > 0$ and the constants c_j defined in Theorem 3.1, we consider the probability space of all the subsets $\mathcal{A} \subseteq \{0, 1, 2, \ldots, n-1\}$ defined by $\mathbb{P}(j \in \mathcal{A}) = \lambda_n c_j$, where $\lambda_n = \lfloor n^{1/6}/(1 + \varepsilon) \rfloor$ (observe that $c_j \lambda_n \leqslant 1$ for n large enough).

Lemma 4.2. *With the conditions above, given $\varepsilon > 0$, there exists n_0 such that, for all $n \geqslant n_0$,*

$$\mathbb{P}\big(|\mathcal{A}| \geqslant \lambda_n \sqrt{n}(1 - \varepsilon)\big) > 0.9.$$

Proof. Since $|\mathcal{A}|$ is a sum of independent Boolean variables and $\mathbb{E}(|\mathcal{A}|) = \sum_{j=0}^{n-1} \mathbb{P}(j \in \mathcal{A}) = \lambda_n \sqrt{n}$, we can apply Chernoff's lemma to deduce that

$$\mathbb{P}\big(|\mathcal{A}| < \lambda_n \sqrt{n}(1 - \varepsilon)\big) \leqslant 2e^{-\min(\varepsilon^2/4, \varepsilon/2)\lambda_n \sqrt{n}} < 0.1$$

for n large enough. $\square$

Lemma 4.3. *Again with the same conditions, given $0 < \varepsilon < 1$, there exists n_1 such that, for all $n \geqslant n_1$,*

$$r^*_{\mathcal{A}}(m) \leqslant \frac{\lambda_n^2}{S}(1 + \varepsilon)^3 \quad \textit{for all } m,$$

with probability > 0.9.

Proof. Since $r^*_{\mathcal{A}}(m) = \sum_{j=0}^{m} \mathbb{I}(j \in \mathcal{A})\mathbb{I}(m - j \in \mathcal{A})$ is a sum of Boolean variables which are not independent, it is convenient to define a new variable,

$$r^{*\prime}_{\mathcal{A}}(m) = \frac{1}{2} r^*_{\mathcal{A}}(m) - \frac{1}{2}\mathbb{I}(m/2 \in \mathcal{A}) = \sum_{j < m/2} \mathbb{I}(j \in \mathcal{A})\mathbb{I}(m - j \in \mathcal{A}).$$

Now we can apply Chernoff's inequality to this variable.

Let μ_m denote the expected value of ${r^*_{\mathcal{A}}}'(m)$. We observe that, from the independence of the indicator functions, $\mathbb{E}\big(\mathbb{I}(j \in \mathcal{A})\mathbb{I}(m-j \in \mathcal{A})\big) = \mathbb{P}(j \in \mathcal{A})\mathbb{P}(m-j \in \mathcal{A}) = \lambda_n^2 c_j c_{m-j}$ for every $j < m/2$, and so

$$\mu_m = \sum_{j<m/2} \mathbb{E}\big(\mathbb{I}(j \in \mathcal{A})\mathbb{I}(m-j \in \mathcal{A})\big) = \sum_{j<m/2} \lambda_n^2 c_j c_{m-j} \leqslant \frac{\lambda_n^2}{2S}(1+\varepsilon),$$

by Theorem 3.1(iii).

- If $\mu_m \geqslant \frac{\lambda_n^2}{6S}(1+\varepsilon)$, we apply Proposition 4.1 (observe that $\varepsilon < 2$ implies that $\varepsilon^2/4 \leqslant \varepsilon/2$), to obtain

$$\begin{aligned}\mathbb{P}\left({r^*_{\mathcal{A}}}'(m) \geqslant \frac{\lambda_n^2}{2S}(1+\varepsilon)^2\right) &\leqslant \mathbb{P}\big({r^*_{\mathcal{A}}}'(m) \geqslant \mu_m(1+\varepsilon)\big) \\ &\leqslant 2\exp\left(-\frac{\mu_m \varepsilon^2}{4}\right) \\ &\leqslant 2\exp\left(-\frac{\lambda_n^2}{24S}(1+\varepsilon)\varepsilon^2\right).\end{aligned}$$

- If $\mu_m = 0$ then ${r^*_{\mathcal{A}}}'(m) = 0$.
- If $0 < \mu_m < \frac{\lambda_n^2}{6S}(1+\varepsilon)$, for $\delta = \frac{\lambda_n^2}{\mu_m 2S}(1+\varepsilon)^2 - 1 \geqslant 2$ (now $\delta/2 \leqslant \delta^2/4$), we obtain

$$\begin{aligned}\mathbb{P}\left({r^*_{\mathcal{A}}}'(m) \geqslant \frac{\lambda_n^2}{2S}(1+\varepsilon)^2\right) &= \mathbb{P}\big({r^*_{\mathcal{A}}}'(m) \geqslant \mu_m(1+\delta)\big) \\ &\leqslant 2\exp(-\delta\mu_m/2) \\ &\leqslant 2\exp\left(-\frac{\lambda_n^2}{4S}(1+\varepsilon)^2 + \frac{\mu_m}{2}\right) \\ &\leqslant 2\exp\left(-\frac{\lambda_n^2}{4S}(1+\varepsilon)^2 + \frac{\lambda_n^2}{12S}(1+\varepsilon)\right) \\ &\leqslant 2\exp\left(-\frac{\lambda_n^2}{6S}(1+\varepsilon)^2\right).\end{aligned}$$

Then

$$\begin{aligned}&\mathbb{P}\left({r^*_{\mathcal{A}}}'(m) \geqslant \frac{\lambda_n^2}{2S}(1+\varepsilon)^2 \text{ for some } m\right) \\ &\quad\leqslant 2n\left(\exp\left(-\frac{\lambda_n^2}{24S}(1+\varepsilon)\varepsilon^2\right) + \exp\left(-\frac{\lambda_n^2}{6S}(1+\varepsilon)^2\right)\right) < 0.1\end{aligned}$$

for n large enough.

Because of the way we defined ${r^*_{\mathcal{A}}}'(m)$, this means

$$\mathbb{P}\left(r^*_{\mathcal{A}}(m) \geqslant \frac{\lambda_n^2}{S}(1+\varepsilon)^2 + \mathbb{I}(m/2 \in \mathcal{A}) \text{ for some } m\right) < 0.1,$$

so

$$\mathbb{P}\left(r^*_{\mathcal{A}}(m) \geqslant \frac{\lambda_n^2}{S}(1+\varepsilon)^3 \text{ for some } m\right) < 0.1$$

for n large enough. $\square$

Lemmas 4.2 and 4.3 imply that, for any $0 < \varepsilon < 1$, for $n \geqslant n(\varepsilon) = \max(n_0, n_1)$, the probability that $|\mathcal{A}| \geqslant \lambda_n \sqrt{n}(1-\varepsilon)$ and $r^*_{\mathcal{A}}(m) \leqslant \frac{\lambda_n^2}{S}(1+\varepsilon)^3$ for all m is greater than 0.8. We now choose one of these sets $\mathcal{A} \subset \{0, \dots, n-1\}$ for a suitable n.

Write $g_\varepsilon = \lfloor \frac{\lambda_{n(\varepsilon)}^2}{S}(1+\varepsilon)^3 \rfloor$. For any $g \geqslant g_\varepsilon$ we take n such that $g = \lfloor \frac{\lambda_n^2}{S}(1+\varepsilon)^3 \rfloor$ (this is possible because $\frac{\lambda_n^2}{S}(1+\varepsilon)^3$ grows more slowly than n). Thus, for $g \geqslant g_\varepsilon$,

$$\beta(g) \geqslant \frac{|\mathcal{A}|}{g^{1/2} n^{1/2}} \geqslant \frac{\lambda_n \sqrt{n}(1-\varepsilon)}{(\lambda_n/\sqrt{S})(1+\varepsilon)^{3/2} n^{1/2}} = \sqrt{S}\frac{1-\varepsilon}{(1+\varepsilon)^{3/2}},$$

which completes the proof for the lower bound in Theorem 1.1, since we can take ε arbitrarily small.

To obtain the upper bound in Theorem 1.1, we will use the following result (assertion (ii) of Theorem 1 in [7]).

Theorem 4.4. *Let S be the Schinzel–Schmidt constant and $\mathcal{Q} = \{Q : Q \in \mathbb{R}_{\geqslant 0}[x],\ Q \not\equiv 0, \deg(Q) < N\}$. Then*

$$\frac{1}{N} \sup_{Q \in \mathcal{Q}} \frac{|Q^2(x)|_1}{|Q^2(x)|_\infty} \leqslant S,$$

where $|P|_1$ is the sum and $|P|_\infty$ the maximum of the coefficients of a polynomial P.

Given a $B_2[g]$ set, $\mathcal{A} \subseteq \{0, \dots, N-1\}$, we define the polynomial $Q_{\mathcal{A}}(x) = \sum_{a \in \mathcal{A}} x^a$, so $Q^2_{\mathcal{A}}(x) = \sum_n r^*_{\mathcal{A}}(n) x^n$. Theorem 4.4 says that, in particular,

$$S \geqslant \frac{1}{N} \sup_{\mathcal{A} \subseteq \{0,\dots,N-1\}} \frac{|\mathcal{A}|^2}{2g} = \frac{F^2(g,N)}{2gN},$$

and so $\frac{F(g,N)}{\sqrt{gN}} \leqslant \sqrt{2S}$.

References

[1] Cilleruelo, J., Ruzsa, I. and Trujillo, C. (2002) Upper and lower bounds for finite $B_2[g]$ sequences. *J. Number Theory* **97** 26–34.

[2] Green, B. (2001) The number of squares and $B_h[g]$ sequences. *Acta Arithmetica* **100** 365–390.

[3] Kolountzakis, M. (1996) The density of $B_h[g]$ sequences and the minimum of dense cosine sums. *J. Number Theory* **56** 4–11.

[4] Martin, G. and O'Bryant, K. (2006) Constructions of generalized Sidon sets. *J. Combin. Theory Ser. A* **113** 591–607.

[5] Martin, G. and O'Bryant, K. (2007) The symmetric subset problem in continuous Ramsey theory. *Experiment. Math.* **16** 145–166.

[6] Ruzsa, I. (1993) Solving a linear equation in a set of integers I. *Acta Arithmetica* **65** 259–282.

[7] Schinzel, A. and Schmidt, W. M. (2002) Comparison of L^1- and L^∞-norms of squares of polynomials. *Acta Arithmetica* **104** 283–296.

[8] Tao, T. and Vu, V. (2006) *Additive Combinatorics*, Vol. 105 of *Cambridge Studies in Advanced Mathematics*, Cambridge University Press.

[9] Yu, G. (2007) An upper bound for $B_2[g]$ sets. *J. Number Theory* **122** 211–220.