

# $B_2[g]$ SETS AND A CONJECTURE OF SCHINZEL AND SCHMIDT

JAVIER CILLERUELO AND CARLOS VINUESA

ABSTRACT. We obtain a new lower bound for  $F(g, n)$ , the largest cardinality of a  $B_2[g]$  set in  $\{1, \dots, n\}$ . More precisely we prove that  $\liminf_{n \rightarrow \infty} \frac{F(g, n)}{\sqrt{gn}} \geq \frac{2}{\sqrt{\pi}} - \varepsilon_g$  where  $\varepsilon_g \rightarrow 0$  when  $g \rightarrow \infty$ . We also relate this problem to a kind of continuous version introduced by Schinzel and Schmidt

## 1. INTRODUCTION

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

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

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

Then, we define

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

In the last years some progress has been done, improving the easier estimates  $1 \leq \beta(g) \leq \alpha(g) \leq 2$ . We list below the successive results obtained by several authors including the improvement obtained in this work.

---

This work was developed during the Doctcourse in Additive Combinatorics held in the Centre de Recerca Matemàtica from January to March 2007. Both authors are extremely grateful for their hospitality.

Both authors are supported by Grants CCG07-UAM/ESP-1814 and DGICYT MTM 2005-04730 (Spain) .

$$\begin{aligned}
\alpha(g) &\leq 2 \text{ (trivial)} \\
&\leq 1.864 \text{ (J. Cilleruelo - I. Ruzsa - C. Trujillo, [1])} \\
&\leq 1.844 \text{ (B. Green, [2])} \\
&\leq 1.839 \text{ (G. Martin - K. O'Bryant, [5])} \\
&\leq 1.789 \text{ (G. Yu, [9])} \\
\beta(g) &\geq 1 \text{ (M. Kolountzakis, [3])} \\
&\gtrsim 1.060 \text{ (J. Cilleruelo - I. Ruzsa - C. Trujillo, [1])} \\
&\gtrsim 1.122 \text{ (G. Martin - K. O'Bryant, [4])} \\
&\gtrsim 2/\sqrt{\pi} = 1.128\dots \text{ (Theorem 1.2)}
\end{aligned}$$

The aim of this work is not only to provide an improvement on the lower bound for  $\beta(g)$  but also to relate this problem with the one posed by Schinzel and Schmidt [7] which can be seen as the continuous version of this problem.

We define the Schinzel-Schmidt's constant  $S$  as the number

$$(1) \quad S = \sup_{f \in \mathcal{F}} \frac{1}{|f * f|_\infty}$$

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

**Remark 1.1.** *In fact they define  $S = \sup_{f \in \tilde{\mathcal{F}}} |f|_1^2 / |f * f|_\infty$  with  $\tilde{\mathcal{F}} = \{f : f \geq 0, f \not\equiv 0, \text{sop}(f) \subseteq [0, 1], f \in L_1[0, 1]\}$ , 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  $1 \leq S \leq 2$  but Schinzel and Schmidt proved in [7] that  $4/\pi \leq S \leq 1.7373$ . The witness for the lower bound is the function  $f(x) = \frac{1}{2\sqrt{x}} \in \mathcal{F}$ . Indeed they conjecture that  $S = 4/\pi$ . Our main theorem relate  $\alpha(g)$  and  $\beta(g)$  to  $S$ .

**Theorem 1.**  $\sqrt{S} \leq \liminf_{g \rightarrow \infty} \beta(g) \leq \limsup_{g \rightarrow \infty} \alpha(g) \leq \sqrt{2S}$ .

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

We conjecture that  $\lim_{g \rightarrow \infty} \beta(g) = \lim_{g \rightarrow \infty} \alpha(g) = 2/\sqrt{\pi}$ .

## 2. CONSTRUCTIONS FOR THE LOWER BOUNDS

It is convenient to introduce the following definitions:

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

**Definition 2.** We say that  $\mathcal{A}$  is a Sidon set  $(\text{mod } m)$  if  $a + a' \equiv a'' + a''' \pmod{m} \implies \{a, a'\} = \{a'', a'''\}$ .

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

**Lemma 1.** If  $\mathcal{A} = \{0 = a_1 < \dots < a_k\}$  is a  $B_2^*[g]$  set and  $\mathcal{C} \subseteq [1, m]$  is a Sidon set  $(\text{mod } m)$ , 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 2.1.** The lemma says that the way of obtaining  $B_2[g]$  sets is “pasting properly” (with a dilation of a  $B_2^*[g]$  set) copies of a Sidon set  $(\text{mod } m)$ .

*Proof.* To prove that  $B$  is a  $B_2[g]$  set, suppose that we have

$$(2) \quad b_{1,1} + b_{2,1} = \dots = b_{1,g+1} + b_{2,g+1}$$

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 only one 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  $c_{1,j} \leq c_{2,j}$ , and when  $c_{1,j} = c_{2,j}$  we order them so  $a_{1,j} \leq a_{2,j}$ .

To see that  $\mathcal{B} \in B_2[g]$  we have to see that there exist  $j$  and  $j'$  such that  $b_{1,j} = b_{1,j'}$ ,  $b_{2,j} = b_{2,j'}$ .

Considering the equalities (2)  $(\text{mod } m)$  and because  $\mathcal{C}$  is a Sidon set  $(\text{mod } m)$  we obtain that  $\{c_{1,1}, c_{2,1}\} = \{c_{1,j}, c_{2,j}\}$  for every  $1 \leq j \leq g + 1$ . Moreover, since 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) imply these other equalities

$$(3) \quad a_{1,1} + a_{2,1} = a_{1,2} + a_{2,2} = \dots = a_{1,g+1} + a_{2,g+1}.$$

And 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  $B \subset [1, \dots, (a_k + 1)m]$  and  $|\mathcal{B}| = k|\mathcal{C}|$ .  $\square$

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

Given  $N$ , we write  $(a_k + 1)p_n(p_n - 1) < N \leq (a_k + 1)p_{n+1}(p_{n+1} - 1)$  for suitable consecutive primes  $p_n, p_{n+1}$ . Clearly

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

Thus

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

Since  $\liminf_{n \rightarrow \infty} \frac{p_n}{p_{n+1}} = 1$  as a consequence of the prime number theorem, we get

$$(4) \quad \beta(g) \geq \frac{k}{\sqrt{g(a_k + 1)}}.$$

So, in order to improve the lower bound for  $\beta(g)$ , we are looking for  $\mathcal{A} = \{0 = a_1 < \dots < a_k\}$  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)  $\mathcal{A} = [0, \lfloor g/3 \rfloor] \cup (g - \lfloor g/3 \rfloor + 2 \cdot [0, \lfloor g/6 \rfloor])$   
 $\cup [g, g + \lfloor g/3 \rfloor] \cup (2g - \lfloor g/3 \rfloor, 3g - \lfloor g/3 \rfloor]$

provide, respectively, the lower bounds

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

cited in the introduction.

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

### 3. SCHINZEL'S CONJECTURE

The convolution  $f * f$  in the Schinzel-Schmidt's problem can be thought as the continuous version of the function  $r_{\mathcal{A}}^*(n)$  and  $|f * f|_{\infty}$  as the analogous of the maximum of  $r_{\mathcal{A}}^*(n)$ .

The idea is to take a function  $f \in \mathcal{F}$  such that  $1/|f * f|_{\infty}$  is close to  $S$  (see definition in formula (1)) and use  $f$  as a model to construct our set  $\mathcal{A}$ . We will do it using 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 2.** *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*

$$i) \quad \sum_{j=0}^{n-1} c_j = \sqrt{n}.$$

- ii)  $c_j \leq n^{-1/6}(1 + \varepsilon)$  for all  $j = 0, \dots, n - 1$ .
- iii)  $\sum_{j < m/2} c_j c_{m-j} \leq \frac{1}{2S}(1 + \varepsilon)$  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  $|f * f|_\infty \leq 1/S + 1/n$ , 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

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

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

In particular, we can deduce  $a_j \leq (2n/t)^{1/2}$ . The core of the proof of theorem 1 (iii) in [7] consists of showing that  $\sum_{j=0}^{n-1} a_j \geq n + o(n)$  and  $\sum_{j=0}^m a_j a_{m-j} \leq (1/S)(n + o(n))$  for all  $m$ . The details can be checked there.

Now we define  $c_j = a_j \rho$  with  $\rho = \frac{\sqrt{n}}{\sum_{j=0}^{n-1} a_j}$ . Clearly  $\rho \leq (1/\sqrt{n})(1 + o(1))$ , so  $c_j \leq n^{-1/6}(1 + o(1))$ ,  $\sum_{j=0}^{n-1} c_j = \sqrt{n}$  and  $\sum_{j=0}^m c_j c_{m-j} \leq (1/S)(1 + o(1))$ .  $\square$

#### 4. THE PROOF

We will use in the proof an special case of Chernoff's inequality (see corollary 1.9 in [8]):

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

$$(5) \quad \mathbb{P}(|X - \mathbb{E}(X)| \geq \delta \mathbb{E}(X)) \leq 2e^{-\min(\delta^2/4, \delta/2)\mathbb{E}(X)}.$$

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

**Lemma 2.** *With the conditions above, given  $\varepsilon > 0$ , there exists  $n_0$  such that for all  $n \geq n_0$*

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

*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

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

for  $n$  large enough.  $\square$

**Lemma 3.** *Again with the same conditions, given  $0 < \varepsilon < 1$ , there exists  $n_1$  such that for all  $n \geq n_1$*

$$r_{\mathcal{A}}^*(m) \leq \frac{\lambda_n^2}{S}(1 + \varepsilon)^3 \quad \text{for all } m$$

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, its convenient to define a new variable  $r_{\mathcal{A}}^{*'}(m) = \frac{1}{2}r_{\mathcal{A}}^*(m) - \frac{1}{2}\mathbb{I}(m/2 \in \mathcal{A}) = \sum_{j < m/2} \mathbb{I}(j \in \mathcal{A})\mathbb{I}(m - j \in \mathcal{A})$ . Now we can apply Chernoff's inequality to this variable.

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

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

by theorem 2 iii).

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

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

- If  $\mu_m = 0$  then  $r_{\mathcal{A}}^{*'}(m) = 0$ .

- If  $0 < \mu_m < \frac{\lambda_n^2}{6S}(1 + \varepsilon)$ , for  $\delta = \frac{\lambda_n^2}{\mu_m 2S}(1 + \varepsilon)^2 - 1 \geq 2$  (now  $\delta/2 \leq \delta^2/4$ ) we obtain

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

Then

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

for  $n$  large enough.

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

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

So, finally,

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

for  $n$  large enough. □

Lemmas 1 and 2 imply that for any  $0 < \varepsilon < 1$ , for  $n \geq n(\varepsilon) = \max(n_0, n_1)$  the probability that  $|\mathcal{A}| \geq \lambda_n \sqrt{n}(1 - \varepsilon)$  and  $r_{\mathcal{A}}^*(m) \leq \frac{\lambda_n^2}{S}(1 + \varepsilon)^3$  for all  $m$  is greater than 0.8. Finally we will consider any of these sets  $\mathcal{A} \subset \{0, \dots, n-1\}$  for a suitable  $n$ .

Write  $g_\varepsilon = \lfloor \frac{\lambda_n(\varepsilon)}{S}(1 + \varepsilon)^3 \rfloor$ . For any  $g \geq g_\varepsilon$  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 slower than  $n$ ). Thus, for  $g \geq g_\varepsilon$ ,

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

which completes the proof of the left inequality of theorem 1 since we can take  $\varepsilon$  arbitrary small.

For the right inequality of theorem 1, we can use the next theorem (assertion (ii) of theorem 1 in [7]):

**Theorem 3.** *Let  $S$  be the Schinzel-Schmidt's constant and  $\mathcal{Q} = \{Q : Q \in \mathbb{R}_{\geq 0}[x], Q \neq 0, \deg(Q) < n\}$ . Then*

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

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  $Q_{\mathcal{A}}^2(x) = \sum_n r_{\mathcal{A}}^*(n)x^n$ . The theorem says that, in particular,

$$S \geq \frac{1}{n} \sup_{\mathcal{A} \subseteq \{0, \dots, n-1\}} \frac{|\mathcal{A}|^2}{2g} = \frac{F^2(g, n)}{2gn},$$

and so  $\frac{F(g, n)}{\sqrt{gn}} \leq \sqrt{2S}$ .

#### REFERENCES

- [1] J. CILLERUELO, I. RUZSA, C. TRUJILLO, *Upper and lower bounds for finite  $B_2[g]$  sequences*, J. Number Theory **97**, no. 1, 26-34 (2002).
- [2] B. GREEN *The number of squares and  $B_h[g]$  sequences*, Acta Arithmetica **100**, no. 4, 365-390 (2001)
- [3] M. KOLOUNTZAKIS, *The density of  $B_h[g]$  sequences and the minimum of dense cosine sums*, J. Number Theory **56**, 4-11 (1996).
- [4] G. MARTIN, K. O'BRYANT, *Constructions of generalized Sidon sets*, J. Comb. Theory, Ser. A **113**, no 4, 591-607 (2006).
- [5] G. MARTIN, K. O'BRYANT, *The Symmetric Subset Problem in Continuous Ramsey Theory*, Experiment. Math. Volume **16**, no 2, 145-166 (2007).
- [6] I. RUZSA, *Solving a linear equation in a set of integers I*, Acta Arithmetica, **65**, 259-282 (1993).
- [7] A. SCHINZEL, W. M. SCHMIDT, *Comparison of  $L^1$ - and  $L^\infty$ - norms of squares of polynomials*, Acta Arithmetica, **104**, no 3 (2002).
- [8] T. TAO, V. VU, *Additive Combinatorics*. Cambridge Studies in Advanced Mathematics, **105** (2006).
- [9] G. YU *An upper bound for  $B_2[g]$  sets*, Journal of Number Theory, **122**, 211-220 (2007)

DEPARTAMENTO DE MATEMÁTICAS, UNIVERSIDAD AUTÓNOMA DE MADRID, 28049-MADRID.

*E-mail address:* franciscojavier.cilleruelo@uam.es, c.vinuesa@uam.es.