



Generalized Sidon sets

Javier Cilleruelo^{a,*}, Imre Ruzsa^{b,2}, Carlos Vinuesa^{c,3}

^a *Instituto de Ciencias Matemáticas (CSIC-UAM-UC3M-UCM) and Departamento de Matemáticas, Universidad Autónoma de Madrid, 28049 - Madrid, Spain*

^b *Alfréd Rényi Institute of Mathematics, Budapest, Pf. 127, H-1364 Hungary*

^c *Departamento de Matemáticas, Universidad Autónoma de Madrid, 28049 - Madrid, Spain*

Received 28 September 2009; accepted 19 May 2010

Available online 26 May 2010

Communicated by Charles Fefferman

Abstract

We give asymptotic sharp estimates for the cardinality of a set of residue classes with the property that the representation function is bounded by a prescribed number. We then use this to obtain an analogous result for sets of integers, answering an old question of Simon Sidon.

© 2010 Elsevier Inc. All rights reserved.

MSC: 11B

Keywords: Sidon sets; $B_2[g]$ sets

1. Introduction

A *Sidon set* A in a commutative group is a set with the property that the sums $a_1 + a_2$, $a_i \in A$ are all distinct except when they coincide because of commutativity. We consider the case when, instead of that, a bound is imposed on the number of such representations. When this bound is g ,

* Corresponding author.

E-mail addresses: franciscojavier.cilleruelo@uam.es (J. Cilleruelo), ruzsa@renyi.hu (I. Ruzsa), c.vinuesa@uam.es (C. Vinuesa).

¹ During the preparation of this paper, J.C. and C.V. were supported by Grant MTM 2008-03880 of MYCIT.

² I.R. is supported by ERC-AdG Grant No. 228005 and Hungarian National Foundation for Scientific Research (OTKA), Grants Nos. K 61908, K 72731.

³ C.V. would like to thank Imre Ruzsa for his hospitality, as well as that of the Alfréd Rényi Institute of Mathematics, during his stay in Budapest.

these sets are often called $B_2[g]$ sets. This being both clumsy and ambiguous, we will avoid it, and fix our notation and terminology below.

Our main interest is in sets of integers and residue classes, but we formulate our concepts and some results in a more general setting.

Let G be a commutative group.

Definition 1.1. For $A \subset G$, we define the corresponding *representation function* as

$$r(x) = \#\{(a_1, a_2): a_i \in A, a_1 + a_2 = x\}.$$

The *restricted representation function* is

$$r'(x) = \#\{(a_1, a_2): a_i \in A, a_1 + a_2 = x, a_1 \neq a_2\}.$$

Finally, the *unordered representation function* $r^*(x)$ counts the pairs (a_1, a_2) where (a_1, a_2) and (a_2, a_1) are identified. With an ordering given on G (not necessarily in any connection with the group operation) we can write this as

$$r^*(x) = \#\{(a_1, a_2): a_i \in A, a_1 + a_2 = x, a_1 \leq a_2\}.$$

These functions are not independent; we have always the equality

$$r^*(x) = r(x) - \frac{r'(x)}{2}$$

and the inequalities

$$r'(x) \leq r(x) \leq 2r^*(x).$$

We have $r(x) = r'(x)$ except for $x = 2a$ with $a \in A$. If we are in this last case and there are no elements of order 2 in G , then necessarily $r(x) = r'(x) + 1$. So, if there are no elements of order 2 in G the quantities are more closely connected:

$$r'(x) = 2 \left\lfloor \frac{r(x)}{2} \right\rfloor, \quad r^*(x) = \left\lceil \frac{r(x)}{2} \right\rceil.$$

This is the case in \mathbb{Z} , or in \mathbb{Z}_q for odd values of q . For even q this is not necessarily true, but both for constructions and estimates the difference seems to be negligible, as we shall see. In a group with lots of elements of order 2, like in \mathbb{Z}_2^m , the difference is substantial.

Observe that r and r' make sense in a noncommutative group as well, while r^* does not.

Definition 1.2. We say that A is a *g-Sidon set*, if $r(x) \leq g$ for all x . It is a *weak g-Sidon set*, if $r'(x) \leq g$ for all x . It is an *unordered g-Sidon set*, if $r^*(x) \leq g$ for all x .

It should be noted that unordered g -Sidon sets are usually called $B_2[g]$ sets.

The strongest possible of these concepts is that of an unordered 1-Sidon set, and this is what is generally simply called a Sidon set. A weak 2-Sidon set is sometimes called a weak Sidon set.

These concepts are closely connected. If there are no elements of order 2, then $2k$ -Sidon sets and unordered k -Sidon sets coincide, in particular, a Sidon set is the same as a 2-Sidon set. Also, in this case $(2k + 1)$ -Sidon sets and weak $2k$ -Sidon sets coincide. Specially, a 3-Sidon set and a weak 2-Sidon set are the same.

Our aim is to find estimates for the maximal size of a g -Sidon set in a finite group, or in an interval of integers.

1.1. The origin of the problem: g -Sidon sets in the integers

In 1932, the analyst S. Sidon asked to a young P. Erdős about the maximal cardinality of a g -Sidon set of integers in $\{1, \dots, n\}$. Sidon was interested in this problem in connection with the study of the L_p norm of Fourier series with frequencies in these sets but Erdős was captivated by the combinatorial and arithmetical flavour of this problem and it was one of his favourite problems; not in vain it has been one of the main topics in Combinatorial Number Theory.

Definition 1.3. For a positive integer n

$$\beta_g(n) = \max |A|: A \subset \{1, \dots, n\}, \quad A \text{ is a } g\text{-Sidon set.}$$

We define $\beta'_g(n)$ and $\beta^*_g(n)$ analogously.

The behaviour of this quantity is only known for classical Sidon sets and for weak Sidon sets: we have $\beta_2(n) \sim \sqrt{n}$ and $\beta_3(n) \sim \sqrt{n}$.

The reason which makes easier the case $g = 2$ is that 2-Sidon sets have the property that the differences $a - a'$ are all distinct. Erdős and Turán [6] used this to prove that $\beta_2(n) \leq \sqrt{n} + O(n^{1/4})$ and Lindström [10] refined that to get $\beta_2(n) \leq \sqrt{n} + n^{1/4} + 1$ (see also [3] for a slight improvement of this upper bound). For weak Sidon sets Ruzsa [16] proved that $\beta_3(n) \leq \sqrt{n} + 4n^{1/4} + 11$.

For the lower bounds, the classical constructions of Sidon sets of Singer [18], Bose [1] and Ruzsa [16] in some finite groups, \mathbb{Z}_m , give $\beta_3(n) \geq \beta_2(n) \geq \sqrt{n}(1 - o(1))$. Then, $\lim_{n \rightarrow \infty} \frac{\beta_2(n)}{\sqrt{n}} = \lim_{n \rightarrow \infty} \frac{\beta_3(n)}{\sqrt{n}} = 1$.

However for $g \geq 4$ it has not even been proved that $\lim_{n \rightarrow \infty} \beta_g(n)/\sqrt{n}$ exists.

For this reason we write

$$\bar{\beta}_g = \limsup_{n \rightarrow \infty} \beta_g(n)/\sqrt{n} \quad \text{and} \quad \underline{\beta}_g = \liminf_{n \rightarrow \infty} \beta_g(n)/\sqrt{n}.$$

It is very likely that these limits coincide, but this has only been proved for $g = 2, 3$. A wide literature has been written with bounds for $\bar{\beta}_g$ and $\underline{\beta}_g$ for arbitrary g . The trivial counting argument gives $\bar{\beta}_g \leq \sqrt{2g}$ while the strategy of pasting Sidon sets in \mathbb{Z}_m in the obvious way gives $\underline{\beta}_g \geq \sqrt{\lfloor g/2 \rfloor}$.

The problem of narrowing this gap has attracted the attention of many mathematicians in the last years.

For example, while for $g = 4$ the trivial upper bound gives $\bar{\beta}_4 \leq \sqrt{8}$, it was proved in [2] that $\bar{\beta}_4 \leq \sqrt{6}$, which was refined to $\bar{\beta}_4 \leq 2.3635\dots$ in [15] and to $\bar{\beta}_4 \leq 2.3218\dots$ in [8].

On the other hand, Kolountzakis [9] proved that $\underline{\beta}_4 \geq \sqrt{2}$, which was improved to $\underline{\beta}_4 \geq 3/2$ in [4] and to $\underline{\beta}_4 \geq 4/\sqrt{7} = 1.5118\dots$ in [8].

We describe below the progress done for larger values of g :

$$\begin{aligned} \frac{\bar{\beta}_g}{\sqrt{g}} &\leq \sqrt{2} = 1.4142\dots \quad (\text{trivial}) \\ &\leq 1.3180\dots \quad (\text{J. Cilleruelo–I.Z. Ruzsa–C. Trujillo, [4]}) \\ &\leq 1.3039\dots \quad (\text{B. Green, [7]}) \\ &\leq 1.3003\dots \quad (\text{G. Martin–K. O’Bryant, [12]}) \\ &\leq 1.2649\dots \quad (\text{G. Yu, [20]}) \\ &\leq 1.2588\dots \quad (\text{G. Martin–K. O’Bryant, [13]}), \\ \lim_{g \rightarrow \infty} \frac{\beta_g}{\sqrt{g}} &\geq 1/\sqrt{2} = 0.7071\dots \quad (\text{M. Kolountzakis, [9]}) \\ &\geq 0.75 \quad (\text{J. Cilleruelo–I.Z. Ruzsa–C. Trujillo, [4]}) \\ &\geq 0.7933\dots \quad (\text{G. Martin–K. O’Bryant, [11]}) \\ &\geq \sqrt{2/\pi} = 0.7978\dots \quad (\text{J. Cilleruelo–C. Vinuesa, [5]}). \end{aligned}$$

Our main result connects this problem with a quantity arising from the analogous continuous problem, first studied by Schinzel and Schmidt [17]. Consider all nonnegative real functions f satisfying $f(x) = 0$ for all $x \notin [0, 1]$, and

$$\int_0^1 f(t)f(x-t) dt \leq 1$$

for all x . Define the constant σ by

$$\sigma = \sup \int_0^1 f(x) dx \tag{1}$$

where the supremum is taken over all functions f satisfying the above restrictions.

Our main result involves this constant.

Theorem 1.4.

$$\lim_{g \rightarrow \infty} \frac{\beta_g}{\sqrt{g}} = \lim_{g \rightarrow \infty} \frac{\bar{\beta}_g}{\sqrt{g}} = \sigma.$$

In other words, the theorem above says that the maximal cardinality of a g -Sidon set in $\{1, \dots, n\}$ satisfies

$$\underline{\sigma}(g)\sqrt{gn}(1 - o(1)) \leq \beta_g(n) \leq \bar{\sigma}(g)\sqrt{gn}(1 + o(1))$$

where $\underline{\sigma}(g)$ and $\bar{\sigma}(g) \rightarrow \sigma$ when $g \rightarrow \infty$.

Schinzel and Schmidt [17] and Martin and O’Bryant [13] conjectured that $\sigma = 2/\sqrt{\pi} = 1.1283\dots$, and an extremal function was given by $f(x) = 1/\sqrt{\pi x}$ for $0 < x \leq 1$. But recently this has been disproved [14] with an explicit f which gives a greater value. The current state of the art for this constant is

$$1.1509\dots \leq \sigma \leq 1.2525\dots$$

both bounds coming from [14].

The main difficulty in Theorem 1.4 is establishing the lower bound for $\lim \frac{\beta_g}{\sqrt{g}}$. Indeed the upper bound $\lim \frac{\bar{\beta}_g}{\sqrt{g}} \leq \sigma$ was already proved in [5] using a result of Schinzel and Schmidt from [17]. We include however a complete proof of the theorem.

The usual strategy to construct large g -Sidon sets in the integers is pasting large Sidon sets modulo m in a suitable form. The strategy of pasting g -Sidon sets modulo m had not been tried before since there were no large enough known g -Sidon sets modulo m .

Precisely, the heart of the proof of this theorem is the construction of large g -Sidon sets modulo m .

1.2. g -Sidon sets in finite groups

Definition 1.5. For a finite commutative group G write

$$\alpha_g(G) = \max |A|: A \subset G, \quad A \text{ is a } g\text{-Sidon set.}$$

We define $\alpha'_g(G)$ and $\alpha^*_g(G)$ analogously. For the cyclic group $G = \mathbb{Z}_q$, with an abuse of notation, we write $\alpha_g(q) = \alpha_g(\mathbb{Z}_q)$.

An obvious estimate of this quantity is

$$\alpha_g(q) \leq \sqrt{gq}.$$

Our aim is to show that for large g , for some values of q , this is asymptotically the correct value. More exactly, write

$$\alpha_g = \limsup_{q \rightarrow \infty} \alpha_g(q)/\sqrt{q}.$$

The case $g = 2$ (Sidon sets) is well known, we have $\alpha_2 = 1$. It is also known [16] that $\alpha_3 = 1$. Very little is known about α_g for $g \geq 4$.

For $g = 2k^2$, Martin and O’Bryant [11] generalised the well known constructions of Singer [18], Bose [1] and Ruzsa [16], obtaining $\alpha_g \geq \sqrt{g/2}$ for these values of g .

We are unable to exactly determine α_g for any $g \geq 4$, but we will find its asymptotic behaviour. Our main result sounds as follows.

Theorem 1.6. We have

$$\alpha_g = \sqrt{g} + O(g^{3/10}),$$

in particular,

$$\lim_{g \rightarrow \infty} \frac{\alpha_g}{\sqrt{g}} = 1.$$

In Section 2, as a warm-up, we give a slight improvement of the obvious upper estimate.

In Section 3 we construct dense g -Sidon sets in groups \mathbb{Z}_p^2 . In Section 4 we use this to construct g -Sidon sets modulo q for certain values of q .

Section 5 is devoted to the proof of the upper bound of Theorem 1.4. In Section 6 we connect the discrete and the continuous world, combining some ideas from Schinzel and Schmidt and some probabilistic arguments used in [5]. In Section 7 we prove the lower bound of Theorem 1.4 pasting copies of the large g -Sidon sets in \mathbb{Z}_q which we constructed in Section 4 and using for that the sets obtained in Section 6.

2. An upper estimate

The representation function $r(x)$ behaves differently at elements of $2 \cdot A = \{2a : a \in A\}$ and the rest; in particular, it can be odd only on this set. Hence we formulate our result in a flexible form that takes this into account.

Theorem 2.1. *Let G be a finite commutative group with $|G| = q$. Let $k \geq 2$ and $l \geq 0$ be integers and $A \subset G$ a set such that the corresponding representation function satisfies*

$$r(x) \leq \begin{cases} k, & \text{if } x \notin 2 \cdot A, \\ k + l, & \text{if } x \in 2 \cdot A. \end{cases}$$

We have

$$|A| < \sqrt{(k - 1)q} + 1 + \frac{l}{2} + \frac{l(l + 1)}{2(k - 1)}. \tag{2}$$

Corollary 2.2. *Let G be a finite commutative group with $|G| = q$, and let $A \subset G$ be a g -Sidon set. If g is even, then*

$$|A| \leq \sqrt{(g - 1)q} + 1.$$

If g is odd, then

$$|A| \leq \sqrt{(g - 2)q} + \frac{3}{2} + \frac{1}{g - 2}.$$

Indeed, these are cases $k = g, l = 0$ and $k = g - 1, l = 1$ of the previous theorem.

Corollary 2.3. *Let $A \subset \mathbb{Z}_q$ be a weak g -Sidon set. If q is even, then*

$$|A| \leq \sqrt{(g - 1)q} + 2 + \frac{3}{g - 1}.$$

If q is odd, then

$$|A| \leq \sqrt{(g-1)q} + \frac{3}{2} + \frac{1}{g-1}.$$

To deduce this, we put $k = g$ and $l = 2$ if q is even, $l = 1$ if q is odd.

Proof of Corollary 2.3. Write $|A| = m$. We shall estimate the quantity

$$R = \sum r(x)^2$$

in two ways.

First, observe that

$$r(x)^2 - kr(x) = r(x)(r(x) - k) \leq \begin{cases} 0, & \text{if } x \notin 2 \cdot A, \\ l(k+l), & \text{if } x \in 2 \cdot A, \end{cases}$$

hence

$$R \leq k \sum r(x) + l(k+l)|2 \cdot A|.$$

Since clearly $\sum r(x) = m^2$ and $|2 \cdot A| \leq m$, we conclude

$$R \leq km^2 + l(k+l)m. \tag{3}$$

Write

$$d(x) = \#\{(a_1, a_2): a_i \in A, a_1 - a_2 = x\}.$$

Clearly $d(0) = m$. We also have $\sum d(x) = m^2$, and, since the equations $x + y = u + v$ and $x - u = v - y$ are equivalent,

$$\sum d(x)^2 = R.$$

We separate the contribution of $x = 0$ and use the inequality of the arithmetic and quadratic mean to conclude

$$R = m^2 + \sum_{x \neq 0} d(x)^2 \geq m^2 + \frac{1}{q-1} \left(\sum_{x \neq 0} d(x) \right)^2 > m^2 + \frac{m^2(m-1)^2}{q}.$$

A comparison with the upper estimate (3) yields

$$\frac{m^2(m-1)^2}{q} < (k-1)m^2 + l(k+l)m.$$

This can be rearranged as

$$(m - 1)^2 < (k - 1)q + \frac{l(k + l)q}{m}.$$

Now if $m < \sqrt{(k - 1)q}$, then we are done; if not, we use the opposite inequality to estimate the second summand and we get

$$(m - 1)^2 < (k - 1)q + \frac{l(k + l)\sqrt{q}}{\sqrt{k - 1}}.$$

We take square root and use the inequality $\sqrt{x + y} \leq \sqrt{x} + \frac{y}{2\sqrt{x}}$ to obtain

$$m - 1 < \sqrt{(k - 1)q} + \frac{l(k + l)}{2(k - 1)}$$

which can be written as (2). \square

3. Construction in certain groups

In this section we construct large g -Sidon sets in groups $G = \mathbb{Z}_p^2$, for primes p . We shall establish the following result.

Theorem 3.1. *Given k , for every sufficiently large prime $p \geq p_0(k)$ there is a set $A \subseteq \mathbb{Z}_p^2$ with $kp - k + 1$ elements which is a g -Sidon set for $g = \lfloor k^2 + 2k^{3/2} \rfloor$.*

Observe that the trivial upper bound in this case is

$$|A| \leq \sqrt{gq} \leq kp \sqrt{1 + \frac{2}{\sqrt{k}}} < (k + \sqrt{k})p.$$

Proof of Theorem 3.1. Let p be a prime. For every $u \neq 0$ in \mathbb{Z}_p consider the set

$$A_u = \left\{ \left(x, \frac{x^2}{u} \right) : x \in \mathbb{Z}_p \right\} \subset \mathbb{Z}_p^2.$$

Clearly $|A_u| = p$.

We are going to study the sumset of two such sets. For any $\underline{a} = (a, b) \in \mathbb{Z}_p^2$ we shall calculate the representation function

$$r_{u,v}(\underline{a}) = \#\{(\underline{a}_1, \underline{a}_2) : \underline{a}_1 \in A_u, \underline{a}_2 \in A_v, \underline{a}_1 + \underline{a}_2 = \underline{a}\}.$$

The most important property for us sounds as follows.

Lemma 3.2. *If $u + v \equiv u' + v'$ and $(\frac{uvu'v'}{p}) = -1$ then $r_{u,v}(\underline{a}) + r_{u',v'}(\underline{a}) = 2$ for all $\underline{a} = (a, b) \in \mathbb{Z}_p^2$.*

Proof. If $a \equiv x + y$ and $b \equiv \frac{x^2}{u} + \frac{y^2}{v}$, with $uv \neq 0$, then $y \equiv a - x$ and we have $b \equiv \frac{x^2}{u} + \frac{(a-x)^2}{v}$. We can rewrite this equation as $(u + v)x^2 - 2aux + ua^2 - buv \equiv 0$. The discriminant of this quadratic equation is $\Delta \equiv 4uv((u + v)b - a^2)$. The number of solutions is

$$r_{u,v}(a, b) = \begin{cases} 1 & \text{if } \left(\frac{\Delta}{p}\right) = 0, \\ 2 & \text{if } \left(\frac{\Delta}{p}\right) = +1 \text{ } (\Delta \text{ quadratic residue}), \\ 0 & \text{if } \left(\frac{\Delta}{p}\right) = -1 \text{ } (\Delta \text{ quadratic nonresidue}). \end{cases}$$

We can express this as

$$r_{u,v}(a, b) = 1 + \left(\frac{\Delta}{p}\right).$$

Now, since $u + v \equiv u' + v'$,

$$\Delta\Delta' \equiv 4uv((u + v)b - a^2)4u'v'((u' + v')b - a^2) \equiv 16uvu'v'((u + v)b - a^2)^2$$

and we have

$$\left(\frac{\Delta}{p}\right)\left(\frac{\Delta'}{p}\right) = \left(\frac{\Delta\Delta'}{p}\right) = \left(\frac{uvu'v'}{p}\right)\left(\frac{((u + v)b - a^2)^2}{p}\right) = -\left(\frac{((u + v)b - a^2)^2}{p}\right).$$

If $(u + v)b - a^2 \equiv 0$, we have $\left(\frac{\Delta}{p}\right) = \left(\frac{\Delta'}{p}\right) = 0$. If not, we have $\left(\frac{\Delta}{p}\right)\left(\frac{\Delta'}{p}\right) = -1$. In any case get

$$\left(\frac{\Delta}{p}\right) + \left(\frac{\Delta'}{p}\right) = 0. \quad \square$$

We resume the proof of the theorem.

We put

$$A = \bigcup_{u=t+1}^{t+k} A_u$$

and we will show that for a suitable choice of t this will be a good set.

Since $(0, 0) \in A_u$ for all u and the rest of the A_u 's are disjoint, we have $|A| = k(p - 1) + 1$.

We can estimate the corresponding representation function as

$$r(\underline{a}) \leq \sum_{u,v=t+1}^{t+k} r_{u,v}(\underline{a})$$

(equality fails sometimes, because representations involving $(0, 0)$ are counted once on the left and several times on the right).

We parametrise the variables of summation as $u = t + i, v = t + j$ with $1 \leq i, j \leq k$. So $2 \leq i + j \leq 2k$ and we can write $i + j = k + 1 + l$ with $|l| \leq k - 1$.

For fixed l , we have $k - |l|$ pairs i, j (which means $k - |l|$ pairs u, v). These pairs can be split into two groups: n^+ of them will have $(\frac{uv}{p}) = 1$ and n^- will have $(\frac{uv}{p}) = -1$. Clearly

$$n^+ + n^- = k - |l|, \quad n^+ - n^- = \sum \left(\frac{uv}{p} \right).$$

Of these $n^+ + n^-$ pairs we can combine $\min\{n^+, n^-\}$ into pairs of pairs with opposite quadratic character, that is, with $(\frac{uvu'v'}{p}) = -1$. For these we use Lemma 3.2 to estimate the sum of the corresponding representation functions $r_{u,v} + r_{u',v'}$ by 2. For the uncoupled pairs we can only estimate the individual values by 2. Altogether this gives

$$\begin{aligned} \sum_{i+j=k+1+l} r_{u,v}(\underline{a}) &\leq 2(\min\{n^+, n^-\}) + 2(\max\{n^+, n^-\} - \min\{n^+, n^-\}) \\ &= 2(\max\{n^+, n^-\}) \\ &= n^+ + n^- + |n^+ - n^-| \\ &= k - |l| + \left| \sum \left(\frac{uv}{p} \right) \right|. \end{aligned}$$

Adding this for all possible value of l , for a fixed t we obtain

$$r(\underline{a}) \leq k^2 + \sum_{|l| \leq k-1} \left| \sum_{i+j=k+1+l} \left(\frac{(t+i)(t+j)}{p} \right) \right| = k^2 + S_t.$$

We are going to show that S_t is small on average. Since we need values with $u, v \neq 0$, we can use only $0 \leq t \leq p - 1 - k$; however, the complete sum is easier to work with. Applying the Cauchy–Schwarz inequality we get

$$\begin{aligned} \sum_{t=0}^{p-1} S_t &= \sum_{t,l} \left| \sum_{i+j=k+1+l} \left(\frac{(t+i)(t+j)}{p} \right) \right| \\ &\leq \sqrt{2kp \sum_{l,t} \left(\sum_{i+j=k+1+l} \left(\frac{(t+i)(t+j)}{p} \right) \right)^2} \\ &\leq \sqrt{2kp \sum_{i+j=i'+j'} \sum_t \left(\frac{(t+i)(t+j)(t+i')(t+j')}{p} \right)}. \end{aligned}$$

To estimate the inner sum we use Weil’s Theorem that asserts

$$\left| \sum_{t=0}^{p-1} \left(\frac{f(t)}{p} \right) \right| \leq \deg f \sqrt{p}$$

for any polynomial f which is not a constant multiple of a square. Hence

$$\sum_{t=0}^{p-1} \left(\frac{(t+i)(t+j)(t+i')(t+j')}{p} \right) \leq 4\sqrt{p}$$

except when the numerator as a polynomial of t is a square.

The numerator will be a square if the four numbers i, i', j, j' form two equal pairs. This happens exactly $k(2k - 1)$ times. Indeed, we may have $i = i', j = j', k^2$ cases, or $i = j', j = i',$ another k^2 cases. The k cases when all four coincide have been counted twice. Finally, if $i = j$ and $i' = j',$ then the equality of sums implies that all are equal, so this gives no new case. In these cases for the sum we use the trivial upper estimate p .

The total number of quadruples i, i', j, j' is $\leq k^3,$ since three of them determine the fourth uniquely.

Combining our estimates we obtain

$$\sum_{t=0}^{p-1} S_t \leq \sqrt{2p^2k^2(2k - 1) + 8p^{3/2}k^4}.$$

This implies that there is a value of $t, 0 \leq t \leq p - k - 1$ such that

$$S_t \leq \frac{\sqrt{2p^2k^2(2k - 1) + 8p^{3/2}k^4}}{p - k} < 2k^{3/2}$$

if p is large enough. This yields that $r(a) < k^2 + 2k^{3/2}$ as claimed. \square

4. Construction in certain cyclic groups

In this section we show how to project a set from \mathbb{Z}_p^2 into \mathbb{Z}_q with $q = p^2s$.

Theorem 4.1. *Let $A \subseteq \mathbb{Z}_p^2$ be a g -Sidon set with $|A| = m,$ and put $q = p^2s$ with a positive integer $s.$ There is a g' -Sidon set $A' \subseteq \mathbb{Z}_q$ with $|A'| = ms$ and $g' = g(s + 1).$*

Proof. An element of A is a pair of residues modulo $p,$ which we shall represent by integers in $[0, p - 1].$ Given an element $(a, b) \in A,$ we put into A' all numbers of the form $a + cp + bsp$ with $0 \leq c \leq s - 1.$ Clearly $|A'| = sm.$

To estimate the representation function of A' we need to tell, given $a, b, c,$ how many $a_1, b_1, c_1, a_2, b_2, c_2$ are there such that

$$a + cp + bsp \equiv a_1 + c_1p + b_1sp + a_2 + c_2p + b_2sp \pmod{p^2s} \tag{4}$$

with $(a_1, b_1), (a_2, b_2) \in A$ and $0 \leq c_1, c_2 \leq s - 1.$

First consider congruence (4) modulo $p.$ We have

$$a \equiv a_1 + a_2 \pmod{p},$$

hence $a_1 + a_2 = a + \delta p$ with $\delta = 0$ or 1 . We substitute this into (4), subtract a and divide by p to obtain

$$c + bs \equiv \delta + c_1 + c_2 + (b_1 + b_2)s \pmod{ps}.$$

We take this modulo s :

$$c \equiv \delta + c_1 + c_2 \pmod{s},$$

consequently $\delta + c_1 + c_2 = c + \eta s$ with $\eta = 0$ or 1 . Again substituting back, subtracting c and dividing by s we obtain

$$b \equiv \eta + b_1 + b_2 \pmod{p}.$$

So $(a, b) = (a_1, b_1) + (a_2, b_2) + (0, \eta)$ which means that for a, b, η given, we have $\leq g$ possible values of a_1, b_1, a_2, b_2 .

Now we are going to find the number of possible values of c_1, c_2 for $a, b, c, \eta, a_1, b_1, a_2, b_2$ given.

Observe that from these data we can calculate $\delta = (a_1 + a_2 - a)/p$. For c_1, c_2 we have the equation $c_1 + c_2 = c - \delta + \eta s$.

If $\eta = 0$, we have $c_1 \leq c$, at most $c + 1$ possibilities.

If $\eta = 1$, we have $c_1 + c_2 \geq c + s - 1$, hence $c - 1 < c_1 \leq s - 1$, which gives at most $s - c$ possibilities.

Hence, if a, b, c, η are given, our estimate is $g(c + 1)$ or $g(s - c)$, depending on η . Adding the two estimates we get the claimed bound $g(s + 1)$. \square

On combining this result with Theorem 3.1 we obtain the following result.

Theorem 4.2. *For any positive integers k, s , for every sufficiently large prime p , there is a set $A \subseteq \mathbb{Z}_{p^2s}$ with $(kp - k + 1)s$ elements which is a $\lfloor k^2 + 2k^{3/2} \rfloor (s + 1)$ -Sidon set.*

Put $q = p^2s$ and $g = \lfloor k^2 + 2k^{3/2} \rfloor (s + 1)$. Thus,

$$\begin{aligned} \frac{\alpha_g(q)}{\sqrt{gq}} &\geq \frac{|A|}{\sqrt{gq}} = \frac{(kp - k + 1)s}{\sqrt{\lfloor k^2 + 2k^{3/2} \rfloor (s + 1)p^2s}} \\ &\geq \frac{(kp - k)s}{\sqrt{(k^2 + 2k^{3/2})(s + 1)p^2s}} \\ &\geq \frac{p - 1}{p\sqrt{(1 + 2/\sqrt{k})(1 + 1/s)}}. \end{aligned}$$

A convenient choice of the parameters is $k = 4s^2$ (so $s = \Theta(g^{1/5})$). Assuming that, we get

$$\frac{\alpha_g(q)}{\sqrt{gq}} \geq \frac{p - 1}{p} \cdot \frac{1}{1 + 1/s}.$$

Thus, the Prime Number Theorem says that

$$\frac{\alpha_g}{\sqrt{g}} = \limsup_{q \rightarrow \infty} \frac{\alpha_g(q)}{\sqrt{gq}} \geq \limsup_{p \rightarrow \infty} \frac{p-1}{p} \cdot \frac{1}{1+1/s} = 1 + O(g^{-1/5}),$$

which completes the proof of Theorem 1.6.

5. Upper bound

We turn now to the proof of Theorem 1.4, which says:

$$\lim_{g \rightarrow \infty} \liminf_{N \rightarrow \infty} \frac{\beta_g(N)}{\sqrt{g}\sqrt{N}} = \lim_{g \rightarrow \infty} \limsup_{N \rightarrow \infty} \frac{\beta_g(N)}{\sqrt{g}\sqrt{N}} = \sigma.$$

We will prove it in two stages:

Part A.

$$\limsup_{g \rightarrow \infty} \limsup_{N \rightarrow \infty} \frac{\beta_g(N)}{\sqrt{g}\sqrt{N}} \leq \sigma.$$

Part B.

$$\liminf_{g \rightarrow \infty} \liminf_{N \rightarrow \infty} \frac{\beta_g(N)}{\sqrt{g}\sqrt{N}} \geq \sigma.$$

For Part A we will use the ideas of Schinzel and Schmidt [17], which give a connection between convolutions and number of representations, between the continuous and the discrete world. For the sake of completeness we rewrite the results and the proofs in a more convenient way for our purposes.

Remember from (1) the definition of σ :

$$\sigma = \sup_{f \in \mathcal{F}} |f|_1,$$

where $\mathcal{F} = \{f: f \geq 0, \text{supp}(f) \subseteq [0, 1], |f * f|_\infty \leq 1\}$.

We will use the next result, which is assertion (ii) of Theorem 1 in [17] (essentially the same result appears in [13] as Corollary 1.5):

Theorem 5.1. *Let σ be the constant defined above and $\mathcal{Q}_N = \{Q \in \mathbb{R}_{\geq 0}[x]: Q \neq 0, \text{deg } Q < N\}$. Then*

$$\sup_{Q \in \mathcal{Q}_N} \frac{|Q|_1}{\sqrt{N}\sqrt{|Q^2|_\infty}} \leq \sigma,$$

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

Proof. First of all, observe that the definition of σ is equivalent to this one:

$$\sigma = \sup_{g \in \mathcal{G}} \frac{|g|_1}{\sqrt{|g * g|_\infty}},$$

where $\mathcal{G} = \{g: g \geq 0, \text{supp}(g) \subseteq [0, 1]\}$.

Given a polynomial $Q = a_0 + a_1x + \dots + a_{N-1}x^{N-1}$ in \mathcal{Q}_N , we define the step function g with support in $[0, 1)$ having

$$g(x) = a_i \quad \text{for } \frac{i}{N} \leq x < \frac{i+1}{N}, \text{ for every } i = 0, 1, \dots, N-1.$$

The convolution of this step function with itself is the polygonal function:

$$g * g(x) = \sum_{i=0}^j a_i a_{j-i} \left(x - \frac{j}{N}\right) + \sum_{i=0}^{j-1} a_i a_{j-1-i} \left(\frac{j+1}{N} - x\right) \quad \text{if } x \in \left[\frac{j}{N}, \frac{j+1}{N}\right)$$

for every $j = 0, 1, \dots, 2N-1$, where we define $a_N = a_{N+1} = \dots = a_{2N-1} = 0$.

So,

$$\sup_x (g * g)(x) = \frac{1}{N} \sup_{0 \leq j \leq 2N-2} \left(\sum_{i=0}^j a_i a_{j-i} \right).$$

Since, obviously, $\int_0^1 g(x) dx = \frac{1}{N} \sum_{i=0}^{N-1} a_i$, we have:

$$\frac{|Q|_1}{\sqrt{N} \sqrt{|Q^2|_\infty}} = \frac{\int_0^1 g(x) dx}{\sqrt{\sup_x (g * g)(x)}} \leq \sigma.$$

And because we have this for every Q , the theorem is proved. \square

Now, given a g -Sidon set $A \subseteq \{0, 1, \dots, N-1\}$, we define the polynomial $Q_A(x) = \sum_{a \in A} x^a$, so $Q_A^2(x) = \sum_n r(n)x^n$. Then, Theorem 5.1 says that

$$\sigma \geq \frac{|Q_A|_1}{\sqrt{|Q_A^2|_\infty} \sqrt{N}} \geq \frac{|A|}{\sqrt{g} \sqrt{N}}.$$

Since this happens for every g -Sidon set in $\{0, 1, \dots, N-1\}$, we have that

$$\frac{\beta_g(N)}{\sqrt{g} \sqrt{N}} \leq \sigma.$$

This proves Part A of Theorem 1.4, which is the easy part.

Remark 5.2. In fact, not only Schinzel and Schmidt prove the result above in [17], but they also prove (see Theorem 6.1) that

$$\lim_{N \rightarrow \infty} \sup_{Q \in \mathcal{Q}_N} \frac{|Q|_1}{\sqrt{N} \sqrt{|Q^2|_\infty}} = \sigma.$$

Newman polynomials are polynomials all of whose coefficients are 0 or 1. In [20], Gang Yu conjectured that for every sequence of Newman polynomials Q_N with $\deg Q_N = N - 1$ and $|Q_N|_1 = o(N)$

$$\limsup_{N \rightarrow \infty} \frac{|Q_N|_1}{\sqrt{N} \sqrt{|Q_N^2|_\infty}} \leq 1.$$

Greg Martin and Kevin O’Bryant [13] disproved this conjecture, finding a sequence of Newman polynomials with $\deg Q_N = N - 1$, $|Q_N|_1 = o(N)$ and

$$\limsup_{N \rightarrow \infty} \frac{|Q_N|_1}{\sqrt{N} \sqrt{|Q_N^2|_\infty}} = \frac{2}{\sqrt{\pi}}.$$

In fact, with the probabilistic method it can be proved without much effort that there is a sequence of Newman polynomials, with $\deg Q_N = N - 1$ and $|Q_N|_1 = O(N^{1/2}(\log N)^\beta)$ for any given $\beta > 1/2$, such that

$$\limsup_{N \rightarrow \infty} \frac{|Q_N|_1}{\sqrt{N} \sqrt{|Q_N^2|_\infty}} = \sigma.$$

While this is the smallest possible growth we can get for $|Q_N|_1$ using the probabilistic method, our Theorem 1.4 shows that given $\varepsilon > 0$, there exists a constant c_ε and a sequence of polynomials, Q_N , with $\deg Q_N = N - 1$ and $|Q_N|_1 \leq c_\varepsilon N^{1/2}$ such that

$$\limsup_{N \rightarrow \infty} \frac{|Q_N|_1}{\sqrt{N} \sqrt{|Q_N^2|_\infty}} \geq \sigma - \varepsilon.$$

Observe that this growth is close to the best possible, since taking $|Q_N|_1 = o(N^{1/2})$ makes $\frac{|Q_N|_1}{\sqrt{N} \sqrt{|Q_N^2|_\infty}} \rightarrow 0$.

6. Connecting the discrete and the continuous world

For Part B of the proof of Theorem 1.4 we will need another result of Schinzel and Schmidt (assertion (iii) of Theorem 1 in [17]) which we state in a more convenient form for our purposes:

Theorem 6.1. *For every $0 < \alpha < 1/2$, for any $0 < \varepsilon < 1$ and for every $n > n(\varepsilon)$, there exist nonnegative real numbers a_0, a_1, \dots, a_n such that*

1. $a_i \leq n^\alpha (1 - \varepsilon)$ for every $i = 0, 1, \dots, n$.
2. $\sum_{i=0}^n a_i \geq n\sigma (1 - \varepsilon)$.
3. $\sum_{0 \leq i, m-i \leq n} a_i a_{m-i} \leq n(1 + \varepsilon)$ for every $m = 0, 1, \dots, 2n$.

Proof. We start with a real nonnegative function defined in $[0, 1]$, g , with $|g * g|_\infty \leq 1$ and $|g|_1$ close to σ , say $|g|_1 \geq \sigma (1 - \varepsilon/2)$.

For $r < s$ we have the estimation

$$\begin{aligned} \left(\int_r^s g(x) dx \right)^2 &= \int_r^s \int_r^s g(x)g(y) dx dy \\ &= \int_{r+x}^{s+x} \int_r^s g(x)g(z-x) dx dz \\ &\leq \int_{2r}^{2s} \int_r^s g(x)g(z-x) dx dz \leq 2(s-r) \end{aligned} \tag{5}$$

which implies that

$$\int_r^s g(x) dx \leq \sqrt{2(s-r)}. \tag{6}$$

Trying to “discretize” our function g , we define for $i = 0, 1, 2, \dots, n$:

$$a_i = \frac{n}{2L} \int_{(i-L)/n}^{(i+L)/n} g(x) dx$$

where $1 \leq L \leq n/2$ is an integer that will be determined later.

Estimation (6) proves that

$$a_i \leq \sqrt{n/L} \quad \text{for } i = 0, 1, 2, \dots, n. \tag{7}$$

Now we give a lower bound for the sum $\sum_{i=0}^n a_i$:

$$\sum_{i=0}^n a_i = \frac{n}{2L} \int_0^1 v(x)g(x) dx,$$

where

$$\begin{aligned}
 v(x) &= \#\left\{i \in [0, n]: \frac{i-L}{n} \leq x \leq \frac{i+L}{n}\right\} \\
 &= \#\{i: \max\{0, nx-L\} \leq i \leq \min\{n, nx+L\}\}.
 \end{aligned}$$

Taking in account that an interval of length M has $\geq [M]$ integers and an interval of length M starting or finishing at an integer has $\lceil M \rceil$ integers, and since $L \in \mathbb{Z}$ and $1 \leq L \leq n/2$, we have

$$v(x) \geq \begin{cases} nx+L=2L-(L-nx) & \text{if } 0 \leq x \leq L/n, \\ 2L & \text{if } L/n \leq x \leq 1-L/n, \\ n-nx+L=2L-(L-n(1-x)) & \text{if } 1-L/n \leq x \leq 1 \end{cases}$$

and so

$$\sum_{i=0}^n a_i \geq n \int_0^1 g(x) dx - \frac{n}{2L} \int_0^{L/n} (L-nx)g(x) dx - \frac{n}{2L} \int_{1-L/n}^1 (L-n(1-x))g(x) dx.$$

Now, using the fact that $|g|_1 \geq \sigma(1-\varepsilon/2)$ and estimation (6),

$$\sum_{i=0}^n a_i \geq n\sigma(1-\varepsilon/2) - \sqrt{2nL}. \tag{8}$$

Also, for every $m \leq 2n$ we give an upper bound for the sum $\sum_{0 \leq i, m-i \leq n} a_i a_{m-i}$. First we write:

$$\sum_{0 \leq i, m-i \leq n} a_i a_{m-i} = \left(\frac{n}{2L}\right)^2 \sum_{0 \leq i, m-i \leq n} \int_{(m-i-L)/n}^{(m-i+L)/n} \int_{(i-L)/n}^{(i+L)/n} g(x)g(y) dx dy.$$

Now, as in (5), we set $z = x + y$ and we consider the set:

$$S_i = \left\{ (x, z): \frac{i-L}{n} \leq x \leq \frac{i+L}{n} \text{ and } \frac{m-i-L}{n} \leq z-x \leq \frac{m-i+L}{n} \right\}.$$

Then,

$$\sum_{0 \leq i, m-i \leq n} a_i a_{m-i} = \left(\frac{n}{2L}\right)^2 \sum_{0 \leq i, m-i \leq n} \iint_{S_i} g(x)g(z-x) dx dz$$

and, defining $\mu(x, z) = \#\{\max\{0, m-n\} \leq i \leq \min\{m, n\}: i-L \leq nx \leq i+L \text{ and } m-i-L \leq n(z-x) \leq m-i+L\}$,

$$\sum_{0 \leq i, m-i \leq n} a_i a_{m-i} = \left(\frac{n}{2L}\right)^2 \iint \mu(x, z)g(x)g(z-x) dx dz.$$

If we write $h = i - nx$ then we are imposing $-L \leq h \leq L$ and $m - L - nz \leq h \leq m + L - nz$, so

$$-L + \max\{0, m - nz\} \leq h \leq L + \min\{0, m - nz\},$$

and $\mu(x, z) \leq \lambda(z)$, which is the number of h 's in this interval (it could be empty), and this number is clearly $\leq 2L + 1$. Also, for each fixed h , z moves in an interval of length $2L/n$.

This means (remember that $|g * g|_\infty \leq 1$)

$$\begin{aligned} \sum_{0 \leq i, m-i \leq n} a_i a_{m-i} &\leq \left(\frac{n}{2L}\right)^2 \int \lambda(z) \int g(x)g(z-x) dx dz \\ &\leq \left(\frac{n}{2L}\right)^2 \int \lambda(z) dz \\ &\leq \left(\frac{n}{2L}\right)^2 \frac{2L(2L+1)}{n} \end{aligned}$$

so the sum

$$\sum_{0 \leq i, m-i \leq n} a_i a_{m-i} \leq n \left(1 + \frac{1}{2L}\right). \tag{9}$$

Finally, looking at (7), (8) and (9), and choosing the integer $L = \lceil n^{1-2\alpha}/(1-\varepsilon)^2 \rceil$ with $0 < \alpha < 1/2$, for sufficiently large n we'll have:

$$a_i \leq n^\alpha (1 - \varepsilon), \quad \sum_{i=0}^n a_i \geq n\sigma (1 - \varepsilon) \quad \text{and} \quad \sum_{0 \leq i, m-i \leq n} a_i a_{m-i} \leq n(1 + \varepsilon). \quad \square$$

Remark 6.2. Now, we will construct random sets. We want to use the numbers obtained in Theorem 6.1 to define probabilities, p_i , and it will be convenient to know the sum of the p_i 's. This is the motivation for defining

$$p_i = a_i \cdot \frac{\sigma n^{1-\alpha}}{\sum_{i=0}^n a_i} \quad \text{for } i = 0, 1, \dots, n.$$

Now we fix $\alpha = 1/3$, although any $\alpha \in (0, 1/2)$ would work. Then we have $p_i = a_i \cdot \frac{\sigma n^{2/3}}{\sum_{i=0}^n a_i}$, so for any $0 < \varepsilon < 1$ and for every $n > n(\varepsilon)$, we have p_0, p_1, \dots, p_n such that:

$$p_i \leq 1, \quad \sum_{i=0}^n p_i = \sigma n^{2/3} \quad \text{and} \quad \sum_{0 \leq i, m-i \leq n} p_i p_{m-i} \leq n^{1/3} \frac{1 + \varepsilon}{(1 - \varepsilon)^2}.$$

Using Chernoff's inequality (see for example Corollary 1.9 in [19]) it is not difficult to prove that the number of elements and the number of representations in our probabilistic sets are what we expect with high probability.

More concretely:

Lemma 6.3. *We consider the probability space of all the subsets $A \subseteq \{0, 1, \dots, n\}$ defined by $\mathbb{P}(i \in A) = p_i$. With the p_i 's defined above, given $0 < \varepsilon < 1$:*

- *there exists $n_0(\varepsilon)$ such that, for all $n \geq n_0$,*

$$\mathbb{P}(|A| \geq \sigma n^{2/3}(1 - \varepsilon)) > 0.9;$$

- *there exists $n_1(\varepsilon)$ such that, for all $n \geq n_1$,*

$$r(m) \leq n^{1/3} \left(\frac{1 + \varepsilon}{1 - \varepsilon} \right)^3 \quad \text{for all } m = 0, 1, \dots, 2n$$

with probability > 0.9 .

We omit the proof of this lemma because it is straightforward and the details can be found in Lemmas 4.2 and 4.3 of [5].

Lemma 6.3 implies that, given $0 < \varepsilon < 1$, for $n \geq \max\{n_0, n_1\}$, the probability that our random set A satisfies $|A| \geq \sigma n^{2/3}(1 - \varepsilon)$ and $r(m) \leq n^{1/3} \left(\frac{1+\varepsilon}{1-\varepsilon}\right)^3$ for every m is greater than 0.8. In particular, for every $n \geq \max\{n_0, n_1\}$ we have a set $A \subseteq \{0, 1, \dots, n\}$ satisfying these conditions.

7. From residues to integers

In order to prove Part B of Theorem 1.4, we will also need the next lemma, which allows us to “paste” copies of a g_2 -Sidon set in a cyclic group with a dilation of a g_1 -Sidon set in the integers.

Lemma 7.1. *Let $A = \{0 = a_1 < \dots < a_k\}$ be a g_1 -Sidon set in \mathbb{Z} and let $C \subseteq [1, q]$ be a g_2 -Sidon set (mod q). Then $B = \bigcup_{i=1}^k (C + qa_i)$ is a g_1g_2 -Sidon set in $[1, q(a_k + 1)]$ with $k|C|$ elements.*

Proof. Suppose we have $g_1g_2 + 1$ representations of an element as the sum of two

$$b_{1,1} + b_{2,1} = b_{1,2} + b_{2,2} = \dots = b_{1,g_1g_2+1} + b_{2,g_1g_2+1}.$$

Each $b_{i,j} = c_{i,j} + qa_{i,j}$ in a unique way. Now we can look at the equality modulo q to have

$$c_{1,1} + c_{2,1} = c_{1,2} + c_{2,2} = \dots = c_{1,g_1g_2+1} + c_{2,g_1g_2+1} \pmod{q}.$$

Since C is a g_2 -Sidon set (mod q), by the pigeonhole principle, there are at least $g_1 + 1$ pairs $(c_{1,i_1}, c_{2,i_1}), \dots, (c_{1,i_{g_1+1}}, c_{2,i_{g_1+1}})$ such that:

$$c_{1,i_1} = \dots = c_{1,i_{g_1+1}} \quad \text{and} \quad c_{2,i_1} = \dots = c_{2,i_{g_1+1}}.$$

So the corresponding a_i 's satisfy

$$a_{1,i_1} + a_{2,i_1} = \dots = a_{1,i_{g_1+1}} + a_{2,i_{g_1+1}},$$

and since A is a g_1 -Sidon set, there must be an equality

$$a_{1,k} = a_{1,l} \quad \text{and} \quad a_{2,k} = a_{2,l}$$

for some $k, l \in \{i_1, \dots, i_{g_1+1}\}$.

Then, for these k and l we have

$$b_{1,k} = b_{1,l} \quad \text{and} \quad b_{2,k} = b_{2,l},$$

which completes the proof. \square

With all these weapons, we are ready to finish our proof.

Given $0 < \varepsilon < 1$ we have that:

- (a) For every large enough g we can define $n = n(g)$ as the least integer such that $g = \lfloor n^{1/3} (\frac{1+\varepsilon}{1-\varepsilon})^3 \rfloor$, and such an n exists because $n^{1/3} (\frac{1+\varepsilon}{1-\varepsilon})^3$ grows more slowly than n . Observe that $n(g) \rightarrow \infty$ when $g \rightarrow \infty$.

Now, by Lemma 6.3, there is $g_0 = g_0(\varepsilon)$ such that for every $g_1 \geq g_0$ we can consider $n = n(g_1)$ and we have a g_1 -Sidon set $A \subseteq \{0, 1, \dots, n\}$ such that

$$\frac{|A|}{\sqrt{g_1} \sqrt{n+1}} \geq \sigma \sqrt{\frac{n}{n+1}} \cdot \frac{(1-\varepsilon)^{5/2}}{(1+\varepsilon)^{3/2}}.$$

- (b) By Theorem 4.2, there are $g_2 = g_2(\varepsilon)$, $s = s(\varepsilon)$ and a sequence $q_0 = p_r^2 s$, $q_1 = p_{r+1}^2 s$, $q_2 = p_{r+2}^2 s$, ... (where p_i is the i -th prime and $r = r(\varepsilon)$) such that for every $i = 0, 1, 2, \dots$ there is a g_2 -Sidon set $A_i \subseteq \mathbb{Z}_{q_i}$ with

$$\frac{|A_i|}{\sqrt{g_2 q_i}} \geq 1 - \varepsilon.$$

So, given $0 < \varepsilon < 1$:

- (1) For every $g \geq g_0(\varepsilon)g_2(\varepsilon)$ there is a $g_1 = g_1(g)$ such that

$$g_1 g_2 \leq g < (g_1 + 1)g_2,$$

and we have $n = n(g_1)$ with $g_1 = \lfloor n^{1/3} (\frac{1-\varepsilon}{1+\varepsilon})^3 \rfloor$ and a g_1 -Sidon set $A \subseteq \{0, 1, \dots, n\}$ with

$$\frac{|A|}{\sqrt{g_1} \sqrt{n+1}} \geq \sigma \sqrt{\frac{n}{n+1}} \cdot \frac{(1-\varepsilon)^{5/2}}{(1+\varepsilon)^{3/2}}.$$

- (2) For any $N \geq (n+1)q_0$, there is an $i = i(N)$ such that

$$(n+1)q_i \leq N < (n+1)q_{i+1},$$

and we have a g_2 -Sidon set (mod q_i), A_i , with

$$\frac{|A_i|}{\sqrt{g_2 q_i}} \geq 1 - \varepsilon.$$

Then, for any g and N large enough, applying Lemma 7.1 we can construct a $g_1 g_2$ -Sidon set from A and A_i with $|A||A_i|$ elements in $[1, N]$.

So we have that $\beta_g(N) \geq \beta_{g_1 g_2}(N) \geq |A||A_i|$ and then

$$\begin{aligned} \frac{\beta_g(N)}{\sqrt{g}\sqrt{N}} &\geq \frac{\beta_{g_1 g_2}(N)}{\sqrt{(g_1+1)g_2}\sqrt{(n+1)q_{i+1}}} \\ &\geq \frac{|A||A_i|}{\sqrt{g_1 g_2}\sqrt{(n+1)q_i}} \sqrt{\frac{g_1}{g_1+1}} \sqrt{\frac{q_i}{q_{i+1}}} \\ &\geq \sigma \frac{(1-\varepsilon)^{7/2}}{(1+\varepsilon)^{3/2}} \sqrt{\frac{n}{n+1}} \sqrt{\frac{g_1}{g_1+1}} \sqrt{\frac{p_{r+i}}{p_{r+i+1}}}. \end{aligned}$$

Finally, as a consequence of the Prime Number Theorem, this means that, given $0 < \varepsilon < 1$, for g and N large enough

$$\frac{\beta_g(N)}{\sqrt{g}\sqrt{N}} \geq \sigma \frac{(1-\varepsilon)^{9/2}}{(1+\varepsilon)^{3/2}},$$

i.e.

$$\liminf_{g \rightarrow \infty} \liminf_{N \rightarrow \infty} \frac{\beta_g(N)}{\sqrt{g}\sqrt{N}} \geq \sigma.$$

References

- [1] R.C. Bose, An affine analogue of Singer's theorem, *J. Indian Math. Soc. (N.S.)* 6 (1942) 1–15.
- [2] J. Cilleruelo, An upper bound for $B_2[2]$ sequences, *J. Combin. Theory Ser. A* 89 (1) (2000) 141–144.
- [3] J. Cilleruelo, Sidon sets in \mathbb{N}^d , *J. Combin. Theory Ser. A* 117 (7) (2010) 857–871.
- [4] J. Cilleruelo, I.Z. Ruzsa, C. Trujillo, Upper and lower bounds for finite $B_h[g]$ sequences, *J. Number Theory* 97 (2002) 26–34.
- [5] J. Cilleruelo, C. Vinuesa, $B_2[g]$ sets and a conjecture of Schinzel and Schmidt, *Combin. Probab. Comput.* 17 (6) (2008) 741–747.
- [6] P. Erdős, P. Turán, On a problem of Sidon in additive number theory, and on some related problems, *J. London Math. Soc.* 16 (1941) 212–215.
- [7] B. Green, The number of squares and $B_h[g]$ sets, *Acta Arith.* 100 (2001) 365–390.
- [8] L. Habsieger, A. Plagne, Ensembles $B_2[2]$: l'état se resserre, *Integers* 2, Paper A2, 20 pp., electronic (2002).
- [9] M. Kolountzakis, The density of sets and the minimum of dense cosine sums, *J. Number Theory* 56 (1) (1996) 4–11.
- [10] B. Lindström, An inequality for B_2 -sequences, *J. Combin. Theory* 6 (1969) 211–212.
- [11] G. Martin, K. O'Bryant, Constructions of generalized Sidon sets, *J. Combin. Theory Ser. A* 113 (4) (2006) 591–607.
- [12] G. Martin, K. O'Bryant, The symmetric subset problem in continuous Ramsey theory, *Experiment. Math.* 16 (2) (2007) 145–166.
- [13] G. Martin, K. O'Bryant, The supremum of autoconvolutions, with applications to additive number theory, arXiv: 0807.5121v2.
- [14] M. Matolcsi, C. Vinuesa, Improved bounds on the supremum of autoconvolutions, *J. Math. Anal. Appl.*, in press.
- [15] A. Plagne, A new upper bound for $B_2[2]$ sets, *J. Combin. Theory Ser. A* 93 (2001) 378–384.

- [16] I.Z. Ruzsa, Solving a linear equation in a set of integers, *Acta Arith.* LXV.3 (1993) 259–282.
- [17] A. Schinzel, W.M. Schmidt, Comparison of L^1 - and L^∞ -norms of squares of polynomials, *Acta Arith.* 104 (3) (2002).
- [18] J. Singer, A theorem in finite projective geometry and some applications to number theory, *Trans. Amer. Math. Soc.* 43 (1938) 377–385.
- [19] T. Tao, V. Vu, *Additive combinatorics*, Cambridge Stud. Adv. Math. 105 (2006).
- [20] G. Yu, An upper bound for $B_2[g]$ sets, *J. Number Theory* 122 (1) (2007) 211–220.