REAL AND p-ADIC SIDON SEQUENCES

JAVIER CILLERUELO AND IMRE Z. RUZSA

Abstract. We investigate sequences of real numbers and p-adic numbers with the property that sums of pairs are always far apart.

1. Introduction

A set A (typically of integers) is called a *Sidon set,* if for every s the equation $x+y=s$ has at most one solution (up to ordering) with $x, y \in A$. It is a famous problem to decide how fast a Sidon sequence of integers must grow.

We investigate an analogous question for sequences of real numbers and p-adic integers. Here the requirement that sums of pairs are different is almost vacuous; we shall replace it by measuring how far they are apart.

Let $a_1, a_2, \dots$ be a sequence of real numbers modulo one and put

$$\delta_n = \min_{j,k,u,v \le n} \|a_j + a_l - a_u - a_v\|, \tag{1.1}$$

where the quadruples $u = j, v = k$ and $u = k, v = j$ are excluded, and $\| \dots \|$ denotes the distance from the nearest integer. By considering the differences $a_j - a_u$, $1 \le j, u \le n$, $j \ne u$, and 0 as the common value of $a_j - a_j$, we immediately see that

$$\delta_n \le \frac{1}{n(n-1)+1}.$$

For a fixed n this is best possible, at least for certain values of n. Indeed, if $n = q - 1$ with a prime-power q, then by taking a perfect difference set modulo $m = q^2 + q + 1 = n(n-1) + 1$ and dividing the elements by m we obtain examples of equality.

We get a slightly different question (analogous to finite Sidon sets of integers in an interval) if we assume that the a_j are real numbers in $[0, 1]$ and we consider the usual distance

$$\delta_n^* = \min_{j,k,u,v \le n} |a_j + a_l - a_u - a_v|, \tag{1.2}$$

which satisfies $\delta_n \le \delta_n^*$. It is less obvious to estimate δ_n^* than δ_n.

Theorem 1.

$$\delta_n^* \le \frac{1}{n(n - 2\sqrt{n})}.$$

Problem 1. *Is*

$$\delta_n^* \le \frac{1}{n(n - o(\sqrt{n}))}$$

true ?

1991 *Mathematics Subject Classification.* majd.

Supported by Hungarian National Foundation for Scientific Research (OTKA), Grants No. T 29759 and T 38396.

A positive answer (or even any improvement of the coefficient 2 of $\sqrt{n}$ in the theorem) would improve the best known upper bound $|A| \le N^{1/2} + N^{1/4} + 1$ for classical Sidon sets.

Problem 2. *Let a_n be an infinite sequence of reals modulo one. Does*

$$\liminf n^2 \delta_n = 0$$

necessarily hold?

A positive answer would be analogous to the classical theorem of Erdős asserting that an infinite Sidon sequence a_n of integers satisfies

$$\limsup a_n/n^2 = \infty.$$

One can ask the same question for δ_n^*. The two problems are equivalent, since given a sequence a_n which has large δ_n^* one can take the sequence $a_n/2$ to show a sequence with $\delta_n \ge \delta_n^*/2$. However, if the answer is negative, then there is no obvious connection between the extremal values.

We exhibit an infinite sequence of real numbers for which the order of magnitude of δ_n is only slightly smaller.

Theorem 2. *There is an infinite sequence a_n of real numbers modulo one such that the quantity δ_n defined by (**??**) satisfies*

$$\delta_n \ge \frac{c}{(n \log n)^2} \tag{1.3}$$

with some positive absolute constant c.

Problem 3. *Can the sequence a_n in Theorem 2 be chosen to be a sequence of rational numbers?*

Let now a_j be a sequence of p-adic integers for some prime p, and define δ_n by the same formula (**??**), with the modification that $\|\dots\|$ now means the p-adic norm, that is, $\|x\| = p^{-k}$ if $p^k | x$ but $p^{k+1} \nmid x$. If we define k by $p^k \le n(n-1) < p^{k+1}$, then similarly we find that all the differences $a_i - a_j$, $i, j \le n$ cannot be distinct modulo p^k, which yields

$$\delta_n \le p^{-k} \le C/n^2$$

with some positive constant C (which depends on the prime p).

We have analogous problems and results to the real case.

Problem 4. *Let a_n be an infinite sequence of p-adic integers. Does*

$$\liminf n^2 \delta_n = 0$$

necessarily hold?

Theorem 3. *There is an infinite sequence a_n of p-adic integers such that the quantity δ_n defined by (**??**) satisfies*

$$\delta_n \ge \frac{c}{(n \log n)^2} \tag{1.4}$$

with some positive constant c, which depends on the prime p but not on n.

Problem 5. *Can the sequence a_n in Theorem 3 be chosen to be a sequence of ordinary integers?*

In the construction of a dense Sidon sequence of integers by the second author [] the starting point was that the sequence $a_n = \log p_n$, where p_n is the n-th prime, satisfies (**??**). It is unbounded and the fractional parts do not have this property, which caused some difficulty. The proof can be simplified by using any of the sequences given in Theorem 2 or Theorem 3 instead.

2. The finite estimate

In this section we prove Theorem 1. Any proof used to estimate finite integer Sidon sets can be adapted to this situation; perhaps the most natural is Lindström's [**?**].

Let the numbers be $0 \le a_1 < \cdots < a_n \le 1$, write $\delta = \delta_n$ and consider the sum

$$S = \sum_{i<j\le n, j-i\le k} (a_j - a_i)$$

for a positive integer k to be specified later. On one hand, S is the sum of

$$N = (n-1) + (n-2) + .. + (n-k) = \frac{k(2n-k-1)}{2}$$

distinct differences, the smallest of which is $\ge \delta$, the second is $\ge 2\delta$ and so on, hence

$$S \ge \delta(1 + 2 + \cdots + N) > \delta N^2/2.$$

On the other hand after the cancellations this sum becomes

$$S = (a_n - a_1) + 2(a_{n-1} - a_2) + \cdots + k(a_{n-k+1} - a_k) \le \frac{k(k+1)}{2}.$$

A comparison of these inequalities yields

$$\delta < \frac{k(k+1)}{N^2} = \frac{4(k+1)}{k(2n-k-1)^2}.$$

The theorem follows by putting $k = [\sqrt{n}]$.

3. The real construction

In this section we prove Theorem 2.

We will contstruct a sequence of complex numbers of modulus 1 such that the pairwise products are far apart, and this will then give a sequence of reals in a natural way.

Let $q_1 = 5 < q_2 < \ldots$ be the sequence of primes $\equiv 1 \pmod 4$, and write each in the form $q_j = \rho_j \overline{\rho}_j$ with a Gaussian prime ρ_j. Now consider the numbers $\alpha_j = \overline{\rho}_j/\rho_j$. We estimate the difference of products. We have

$$\alpha_j\alpha_k - \alpha_u\alpha_v = \frac{\overline{\rho}_j\overline{\rho}_k\rho_u\rho_v - \overline{\rho}_u\overline{\rho}_v\rho_j\rho_k}{\rho_j\rho_k\rho_u\rho_v}.$$

The enumerator is a Gaussian integer, not zero by the unique factorization, hence its modulus is ≥ 1. We obtain

$$|\alpha_j\alpha_k - \alpha_u\alpha_v| \ge \frac{1}{|\rho_j\rho_k\rho_u\rho_v|} = \frac{1}{\sqrt{p_jp_kp_up_v}} \ge \frac{c}{(n\log n)^2}$$

withe a positive constant c if $j, k, u, v \le n$.

Now define a_j by $\alpha_j = e^{2\pi i a_j}$. We have

$$|\alpha_j\alpha_k - \alpha_u\alpha_v| = |1 - \alpha_u\alpha_v/(\alpha_j\alpha_k)| = |1 - e^{2\pi i(a_u+a_v-a_j-a_k)}| \le 2\pi|a_j + a_k - a_u - a_v|.$$

On substituting this into the previous inequality we obtain the claim of the theorem.

4. The p-adic construction

We prove Theorem 3.

Put $P = p$ if p is odd, and $P = 4$ if $p = 2$. Let $q_1 < q_2 < \dots$ be the sequence of primes $\equiv 1 \pmod P$. We will use the p-adic logarithm, defined by the usual power series

$$\log(1+t) = t - \frac{t^2}{2} + \frac{t^3}{3} - \dots$$

This series is convergent when $\|t\| < 1$, it has the usual additivity property and it satisfies

$$\|\log(1+t) - t\| < \|t\|$$

and consequently

$$\|\log(1+t)\| = \|t\|$$

whenever $\|t\| \le 1/P$.

We put now $a_j = \log q_j$. We have

$$a_j + a_k - a_u - a_v = \log \frac{q_j q_k}{q_u q_v} = \log(1+t),$$

where

$$t = \frac{q_j q_k - q_u q_v}{q_u q_v}.$$

The denominator clearly has norm 1. The enumerator is nonzero, it is a multiple of P by the assumption $q_j \equiv 1 \pmod P$, and it is an integer of absolute value $< C(n \log n)^2$ if $j, k, u, v \le n$, hence

$$\frac{c}{(n \log n)^2} \le \|t\| \le \frac{1}{P}.$$

Consequently

$$\|a_j + a_k - a_u - a_v\| = \|t\| \ge \frac{c}{(n \log n)^2}$$

as claimed.

5. Concluding remarks

A positive answer to problem 2 and the construction in Theorem 2 would give an indirect proof that the primes $\equiv 1 \pmod 4$ have density zero. An answer to Promlem 4 would have similar consequences.

References

[1] B. Lindström, *An inequality for B_2-sequences*, J. Combin. Theory **6** (1969), 211–212.

Departamento de Matemáticas, Universidad Autónoma de Madrid, 28049 Madrid, Spain

E-mail address: franciscojavier.cilleruelo@uam.es

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

E-mail address: ruzsa@renyi.hu