Irregularities of sequences relative to long arithmetic progressions

by
A. Sárközy and C.L. Stewart

Dedicated to Klaus Friedrich Roth on the occasion of his 80th birthday

1 Introduction

K.F. Roth has written 8 papers [18]–[25] on the distribution of sequences of positive integers in arithmetic progressions and on related subjects. The starting point of this work was the famous conjecture on the sharpening of van der Waerden's theorem [37] formulated first probably by Erdős and Turán in 1936 [10]:

Conjecture 1. *If k, n are positive integers then let $r_k(n)$ denote the maximal cardinality of a subset selected from $\{1, 2, \dots, n\}$ so that it does not contain an arithmetic progression of k terms. Then for any fixed $k \geq 3$ and $n \to +\infty$ we have $r_k(n) = o(n)$.*

The first significant step in this direction was made 16 years later by Roth: first in [18] he proved the $k = 3$ special case of this conjecture (by using the Hardy–Littlewood method in a very elegant way), and then in [19] he sharpened the result to $r_3(n) = O\left(\frac{n}{\log\log n}\right)$. Unfortunately, his proof cannot be adapted to the case $k > 3$. Thus he continued the work in the papers [20]–[25] by proposing and trying other approaches for settling the conjecture for general k. These efforts did not lead to the proof of the conjecture; it was Szemerédi who settled first the case $k = 4$ [33] and then the general case [34] by using a very difficult and ingenious argument of a completely elementary combinatorial nature. Since then further proofs of the conjecture, now Szemerédi's theorem, have been found. In 1977 Furstenberg [11] used techniques from ergodic theory to prove Szemerédi's theorem. In 2001 Gowers [12] gave a third proof of Szemerédi's theorem.

Although Roth did not succeed in finding a proof for Conjecture 1, as a byproduct of his efforts he opened up new directions of research and proved results of basic importance; the real significance of some of them was realized only much later.

It would be a hopeless task to try to give a more or less complete survey of the 8 papers of Roth mentioned above and of the papers inspired by or related

to them; this would take a whole book. The best that we can do in a paper of limited extent is to split off and survey a relatively independent part of the 8 papers and the work inspired by it. Indeed, here we will focus on those results where *long* arithmetic progressions are studied, i.e., on papers [21], [22] and [23] (although for the sake of completeness we will also mention his other papers shortly) and on the 20 or so papers inspired by them. First in Section 2 we will give a survey of the main results of these 3 papers. In Section 3 we will present the very elegant proof of his basic result in [21]. In Section 4 we will survey the papers inspired by Roth's work. Finally, in Section 5 we will analyze the significance of his papers and we will also present a couple of related problems which are still open.

Throughout this paper we will use the following notation: $\mathbb{Z}$ and $\mathbb{N}$ denote the set of integers and the set of positive integers respectively. $\mathbb{R}$ and $\mathbb{C}$ denote the set of real numbers and the set of complex numbers respectively. For any real number x the integer part of x is denoted by $[x]$, and $\|x\|$ denotes the distance of x from the nearest integer so $\|x\| = \min\big\{x - [x],\, x + 1 - [x]\big\}$. We write $e(\alpha) = e^{2\pi i\alpha}$. We will use Vinogradov's notation $\ll$: we write $f(x) \ll g(x)$ if there is an absolute constant C such that $|f(x)| < C|g(x)|$ for $x > x_0$ (in other words, $f(x) = O(g(x))$. $c_1, c_2, \dots$ will denote positive absolute constants.

2 A survey of some of Roth's papers

In Section 1 we mentioned his papers [18] and [19] written on the estimate of $r_3(n)$. In [20] he extended the problem by studying systems of linear equations. Let $(a_{\mu\nu})$ be an $\ell \times n$ matrix whose elements are integers. A set $\mathcal{U}$ of positive integers is called an A-set if there are not distinct integers $x_1, x_2, \dots, x_n$ in $\mathcal{U}$ such that

$$\sum_{\nu=1}^{n} a_{\mu\nu} x_\nu = 0 \quad \text{for} \quad \mu = 1, 2, \dots, \ell.$$

Denote by $A(x)$ the greatest number of integers that can be selected from $1, 2, \dots, x$ to form an A-set. In [20] Roth proved:

Theorem 1. *Assume that*

$$\sum_{\nu=1}^{n} a_{\mu\nu} = 0 \quad \textit{for} \quad \mu = 1, 2, \dots, \ell,$$

and that among the columns of the matrix there exist ℓ linearly independent ones so that if any one of these is excluded, then the remaining $n-1$ columns of the matrix can be divided into two sets so that among the columns of each set there are ℓ linearly independent columns. Then $A(x) = o(x)$.

Note that the matrix $(1, -2, 1)$ satisfies the conditions, thus his earlier result $r_3(n) = o(n)$ is a special case of this theorem.

Now let $N \in \mathbb{N}$, $\mathcal{A} \subset \{1, 2, \dots, N\}$. For $q \in \mathbb{N}$ and $m, h \in \mathbb{Z}$, write

$$A_{q,h}(m) = \big|\big\{a :\ 1 \le a \le m,\ a \equiv h \pmod q,\ a \in \mathcal{A}\big\}\big|,$$

in particular,

$$A(m) = A_{1,0}(m) = \big|\{a:\ 1 \le a \le m,\ a \in \mathcal{A}\}\big|,$$

and set

$$\eta = \frac{A(N)}{N}.$$

For $q \in \mathbb{N}$ and $m, h \in \mathbb{Z}$, let

$$\begin{aligned} D_{q,h}(m) = \big|\{a:\ 1 \le a \le m,\ a \equiv h \pmod q,\ a \in \mathcal{A}\}\big| \\ - \eta\big|\{a:\ 1 \le a \le m,\ a \equiv h \pmod q\}\big| \end{aligned}$$

and

$$V_q(m) = \sum_{h=0}^{q-1} D_{q,h}^2(m).$$

In [21] Roth proved:

Theorem 2. *For all $N, Q \in \mathbb{N}$ and $\mathcal{A} \subset \{1, 2, \dots, N\}$ we have*

$$\sum_{q=1}^{Q} \frac{1}{q} \sum_{m=1}^{N} V_q(m) + Q \sum_{q=1}^{Q} V_q(N) \gg \eta(1-\eta)Q^2 N \tag{2.1}$$

where the implicit constant is absolute.

As Roth writes, (2.1) says that a sequence which is neither very thin nor very dense cannot be "well-distributed simultaneously *among* and *within* all congruence classes". Roth's proof, in a slightly generalized form, will be presented in the next section.

It follows from Theorem 2 that:

Corollary 1. *Let $N, Q \in \mathbb{N}$ with $Q \le N^{1/2}$. Then for any $\mathcal{A} \subset \{1, 2, \dots, N\}$, there exist $q_1, m_1 (\le N), h_1 \in \mathbb{Z}$ such that $1 \le q_1 \le Q$ and*

$$\begin{aligned} \big|D_{q_1,h_1}(m_1)\big| &= \Big|\big|\{a:\ 1 \le a \le m_1,\ a \equiv h_1 \pmod{q_1},\ a \in \mathcal{A}\}\big| \\ &\qquad - \eta\big|\{a:\ 1 \le a \le m_1,\ a \equiv h_1 \pmod{q_1}\}\big|\Big| \\ &\gg \big(\eta(1-\eta)Q\big)^{1/2}. \end{aligned} \tag{2.2}$$

Indeed, (2.1) says that (2.2) holds on average. We get the best lower bound here if we choose $Q = [N^{1/2}]$:

Corollary 2. *For all $N \in \mathbb{N}$ and $\mathcal{A} \subset \{1, 2, \dots, N\}$, there exist q_1, m_1 $(\le N), h_1 \in \mathbb{Z}$ such that $1 \le q_1 \le N^{1/2}$ and*

$$\big|D_{q_1,h_1}(m_1)\big| \gg \big(\eta(1-\eta)\big)^{1/2} N^{1/4}.$$

Roth continued the work in this direction in a series of 4 papers [22], [23], [24], [25]. In the introduction to the first part of the series [22] he presents his motivation and goals in a very clear and compact form. Thus we will quote him:

"A well known conjecture" [a variant of the Erdős–Turán Conjecture 1] "asserts that if an integer sequence (more precisely, a strictly increasing sequence of integers) has positive upper density, then it contains arbitrarily long arithmetic progressions. This conjecture, which remains undecided, has led me to consider the following general question.

Suppose that k is a large integer, and that the integer N is large as a function of k. Let

$$s_1, s_2, \dots, s_N \tag{2.3}$$

be a set of N real numbers, and write

$$L = \sum_{n=1}^{N} s_n. \tag{2.4}$$

We ask what lower bounds can one give for the expressions

$$\sup_{n,q} \left| \sum_{\nu=0}^{k-1} (s_{n+\nu q} - LN^{-1}) \right| \tag{2.5}$$

and

$$\sup_{n,q} \sum_{\nu=0}^{k-1} (s_{n+\nu q} - LN^{-1}), \tag{2.6}$$

where each supremum is taken over all pairs n, q of integers satisfying

$$1 \le n < n + (k-1)q \le N. \tag{2.7}$$

Since we can always replace the numbers s_n by the numbers $(s_n - LN^{-1})$, we may restrict our attention to the case $L = 0$.

A lower bound for (2.5) is easily obtained by means of the method of our previous paper [21]; we shall prove the following result in this way.

Theorem 3. *Let k be a natural number and suppose that the integer N satisfies $N > (10k)^7$. Then, for every set* (2.3) *of real numbers, there exist integers n, q, satisfying* (2.7)*, such that*

$$\left| \sum_{\nu=0}^{k-1} s_{n+\nu q} \right| \ge \left\{ \frac{1}{10} k N^{-1} \sum_{j=1}^{N} s_j^2 \right\}^{1/2}. \tag{2.8}$$

"One-sided" estimates, such as a lower bound for (2.6), appear to be considerably more difficult to obtain (but it is this type of result that is relevant to

the above-mentioned conjecture), and almost the entire paper will be devoted to proving a result of this kind.

We will now need to make use of the assumption that the set (2.3) satisfies (2.4) with $L = 0$. In addition, we shall need to assume that the numbers s_n all lie within a suitable set $\mathcal{S}$ of real numbers; a set $\mathcal{S}$ will be "suitable" if there exists a number Λ such that

$$\sup_{x\in\mathcal{S}} |x| \le \Lambda \inf_{x\in\mathcal{S}} |x|. \tag{2.9}$$

He points out that without the loss of generality, one may replace (2.9) by

$$1 \le |s_j| \le \Lambda \qquad (j = 1, 2, \dots, N), \tag{2.10}$$

and then he writes:

"We may therefore prove our result in the following form.

Theorem 4. *Let $\Lambda \ge 1$ and let k be an integer satisfying*

$$k > (10^2\Lambda)^4. \tag{2.11}$$

Then there exists a number $N_1 = N_1(\Lambda, k)$ such that the following statement is true.

If $N > N_1$ and the set (2.3) *of real numbers satisfies* (2.10) *and*

$$\sum_{j=1}^{N} s_j = 0, \tag{2.12}$$

then there exist integers n, q, satisfying (2.7)*, such that*

$$\sum_{\nu=0}^{k-1} s_{n+\nu q} > \left\{10^{-4}\Lambda^{-2}\sum_{\nu=0}^{k-1} s_{n+\nu q}^2\right\}^{1/2}. \tag{2.13}$$

Thus, in particular, we have

$$\sum_{\nu=0}^{k-1} s_{n+\nu q} > 10^{-2}\Lambda^{-1}k^{1/2} \tag{2.14}$$

for this pair n, q."

... "We have made no attempt at economy in relation to constants, and there is no special significance in either the constant $\frac{1}{10}$ appearing in (2.8) or the constant 10^{-4} appearing in (2.13). Our method can be adapted to yield an explicit value of N_1 (in terms of Λ and k), but this value would be extremely large."

He also writes: "An important special case arises when $\mathcal{S}$ contains only a finite number of elements; in this case $\mathcal{S}$ will certainly satisfy (2.9) for some Λ, provided only it does not contain 0. It is perhaps worth mentioning that in

this special case a famous theorem of van der Waerden [37] would enable us to choose integers n, q (satisfying (2.7)) so that the numbers

$$s_n, s_{n+q}, \dots, s_{n+(k-1)q} \tag{2.15}$$

are all equal (or, even in the general case, so that these numbers all have the same sign). But whilst such a choice would yield a very effective lower estimate for (2.5) (in view of (2.9)), it would be entirely useless for the purpose of obtaining a lower estimate for (2.6). For there would be nothing to prevent the common value of the numbers (2.15) being negative."

In the remaining part of this section we will quote again Roth repeatedly but without using some of his notation.

In [23] he proves the following "... refinement ... of Theorem 4.

Theorem 5. *Let $\Lambda \geq 1$ and let δ satisfy*

$$10^{-4}\Delta^{-2} \leq \delta \leq 10^{-4}\Lambda^{-1}.$$

Let the integer k satisfy $k > (10^2\Lambda)^6\delta$. Then there exists a number $N_1' = N_1'(\Lambda, \delta, k)$ such that the following statement is true.

Suppose that $N > N_1'$ and the set (2.3)*, in addition to satisfying* (2.10)*,* (2.12)*, is such that*

$$\sum_{u=0}^{k-1} s_{n+uq}^2 \leq \max\left\{10^{-4}\delta^{-1}k, \frac{1}{6}\left(\sum_{u=0}^{k-1} s_{n+uq}\right)^2\right\} \tag{2.16}$$

for every arithmetic progression $\{n, n+q, \dots, n+(k-1)q\}$. Then there exists an arithmetic progression $\{n_0, n_0+q, \dots, n_0+(k-1)q_0\}$ for which

$$\sum_{u=0}^{k-1} s_{n_0+uq_0} > \left\{\delta \sum_{u=0}^{k-1} s_{n_0+uq_0}^2\right\}^{1/2}.$$

We note that Theorem 4 is simply the special case $\delta = 10^{-4}\Lambda^{-2}$ of Theorem 5. For in this case (2.10) ensures that (2.16) holds for all arithmetic progressions $\{n, n+q, \dots, n+(k-1)q\}$, so that the additional premise becomes void."

From Theorem 5 Roth deduces:

Theorem 6. *Let $0 < \beta < 1/2$, and suppose that $k > k_1(\beta)$ and $N > N_1(\beta, k)$ where k_1 and N_1 are sufficiently large. Then, if the sequence $\mathcal{A} \subset \{1, 2, \dots, N\}$ is such that $\beta \leq \frac{|\mathcal{A}|}{N} \leq 1 - \beta$, there exists an arithmetic progression $\{n, n+q, \dots, n+(k-1)q\}$, such that*

$$\left|\mathcal{A} \cap \{n, n+q, \dots, n+(k-1)q\}\right| - \frac{|\mathcal{A}|}{N}k > c\beta k^{1/2} \tag{2.17}$$

where c is a positive constant.

The significance of this result is that Roth shows that the Erdős–Turán Conjecture 1 and the following conjecture on the sharpening of the statement of Theorem 6 are equivalent:

"**Conjecture 2.** *Let $0 < \beta < 1/2$. Then there exists a positive number $b = b(\beta)$ depending only on β, such that the following statement is true.*

Suppose that $k > k_1(\beta)$ and $N > N_1(\beta, k)$, where k_1 and N_1 are sufficiently large. Then, if the sequence $\mathcal{A} \subset \{1, 2, \ldots, N\}$ is such that $\beta \leq \frac{|\mathcal{A}|}{N} \leq 1 - \beta$, there exists an arithmetic progression $\{n, n+q, \ldots, n+(k-1)q\}$ such that

$$\left|\mathcal{A} \cap \{n, n+q, \ldots, n+(k-1)q\}\right| - \frac{|\mathcal{A}|}{N}k > bk." \tag{2.18}$$

In other words, in order to prove the Erdős–Turán Conjecture 1 it would be sufficient to replace (2.17) in Theorem 6 by (2.18). However, there is a long way to go from (2.17) to (2.18) and Roth has not been able to bridge this gap.

These last results appeared in 1967 in Part II [23] of his series "Irregularities of sequences relative to arithmetic progressions". Part III [24] of the series appeared in 1970. He writes in the introduction: "Szemerédi has recently proved [33], by a remarkably ingenious elementary method, that an integer sequence containing no four consecutive terms of any arithmetic progression must have zero density. Our purpose is to develop a new method, embodying a number of Szemerédi's ideas but analytic in nature, for proving the above theorem and certain generalizations of it. We intend to carry out that task in the next paper of this series. In the present paper we prove a theorem which will constitute the basic tool for the analytic method. ... Szemerédi proved that

$$\lim_{N\to\infty} N^{-1} r_4(N) = 0,$$

but a quantitative result would give information regarding the rate at which $N^{-1}r_4(N)$ tends to 0 as $N \to \infty$. Our method can be adapted to give quantitative results, but the proofs then become complicated and the resulting estimates would be poor."

After the technical preparation of Part III, in Part IV [25] Roth considers the same generalization of the problem as in [20], i.e., he considers $\ell \times n$ integer matrices $(a_{\mu\nu})$ and the solvability of the system of linear equations

$$\sum_{\nu=1}^{n} a_{\mu\nu} x_\nu = 0 \quad \text{for} \quad \mu = 1, 2, \ldots, \ell$$

in distinct integers. In [20] he could handle this system only for $n > 2\ell$ (this follows from the linear independence condition on the column vectors in Theorem 1) which excludes the matrix $\begin{pmatrix} 1 & -2 & 1 & 0 \\ 0 & 1 & -2 & 1 \end{pmatrix}$, i.e., the case of the four term arithmetic progressions. Here in [25] he also covers the case $n = 2\ell$ which includes the four term arithmetic progressions.

3 Proof of Theorem 2

In this section we will present the proof of Theorem 2. More exactly, we will prove the result in a slightly generalized form inspired by Theorem 3 (but this version does not follow from Theorem 3). This more general form of the result appears in [29] but its proof follows Roth's original proof closely and no additional effort is needed, thus it can be considered as a variant of Theorem 2.

Theorem 2'. *Let $N \in \mathbb{N}$, $Q \in \mathbb{N}$ with $Q \geq 2$, and let $s_1, s_2, \ldots, s_N \in \mathbb{C}$. Set $Q_1 = [Q/2]$ and $s_i = 0$ for $i \in \mathbb{Z}$, $i < 1$ and $i > N$. For $n \in \mathbb{Z}$ and $q, k \in \mathbb{N}$ write*

$$D(n, q, k) = s_n + s_{n+q} + s_{n+2q} + \cdots + s_{n+(k-1)q}.$$

Then we have

$$\sum_{q=1}^{Q} \sum_{n=1-(Q_1-1)q}^{N} \left|D(n, q, Q_1)\right|^2 \geq \left(\frac{2}{\pi} Q_1\right)^2 \sum_{m=1}^{N} |s_m|^2. \tag{3.1}$$

Note that Theorem 2 follows from Theorem 2' by taking

$$s_n = \begin{cases} 1 - \eta & \text{for } n \in \mathcal{A} \\ -\eta & \text{for } n \notin \mathcal{A} \end{cases}$$

(for $1 \leq n \leq N$).

Proof of Theorem 2'. The proof will be based on a very elegant use of the complex version of the Fejér kernel. Write

$$F(\beta) = \sum_{j=0}^{Q_1-1} e(j\beta)$$

and

$$S(\alpha) = \sum_{n=1}^{N} s_n e(n\alpha) = \sum_{n=-\infty}^{+\infty} s_n e(n\alpha).$$

Following Roth's method, consider the integral

$$E = \int_0^1 \sum_{q=1}^{Q} \left|F(q\alpha)S(\alpha)\right|^2 d\alpha.$$

Then by Parseval's formula (and using $s_i = 0$ for $i < 1$, $i > N$) we have

(3.2)

$$E = \sum_{q=1}^{Q} \int_0^1 \left|F(q\alpha)S(\alpha)\right|^2 d\alpha =$$

$$= \sum_{q=1}^{Q} \int_0^1 \Big| \sum_{j=0}^{Q_1-1} e(jq\alpha) \sum_{n=1}^{N} s_n e(n\alpha) \Big|^2 d\alpha =$$

$$= \sum_{q=1}^{Q} \int_0^1 \Big| \sum_{m=1}^{N+(Q_1-1)q} \Big(\sum_{j=1}^{Q_1-1} s_{m-jq} \Big) e(m\alpha) \Big|^2 d\alpha =$$

$$= \sum_{q=1}^{Q} \int_0^1 \Big| \sum_{m=1}^{N+(Q_1-1)q} D\big(m-(Q_1-1)q, q, Q_1\big) e(m\alpha) \Big|^2 d\alpha =$$

$$= \sum_{q=1}^{Q} \sum_{m=1}^{N+(Q_1-1)q} \big| D\big(m-(Q_1-1)q, q, Q_1\big) \big|^2 = \sum_{q=1}^{Q} \sum_{n=1-(Q_1-1)q}^{N} \big| D(n, q, Q_1) \big|^2.$$

On the other hand, for $|\beta| \le 1/Q$ (so that $|Q_1\beta| \le 1/2$) we have

$$|F(\beta)| = Q_1 \left| \frac{\sin \pi Q_1 \beta}{\pi Q_1 \beta} \right| \left| \frac{\pi\beta}{\sin \pi\beta} \right| \ge Q_1 \cdot \frac{2}{\pi} \cdot 1 = \frac{2}{\pi} Q_1.$$

Moreover, by Dirichlet's theorem for every $\alpha \in \mathbb{R}$ there exist $q_0 \in \mathbb{N}$ and $p_0 \in \mathbb{Z}$ with $1 \le q_0 \le Q$ and

$$|q_0\alpha - p_0| < \frac{1}{Q}$$

so that

$$\sum_{q=1}^{Q} \big| F(q\alpha) \big|^2 \ge \big| F(q_0\alpha) \big|^2 = \big| F(q_0\alpha - p_0) \big|^2 > \left(\frac{2}{\pi} Q_1 \right)^2.$$

Thus we have

$$E = \int_0^1 \Big(\sum_{q=1}^{Q} \big| F(q\alpha) \big|^2 \Big) |S(\alpha)|^2 d\alpha \ge \tag{3.3}$$

$$\ge \left(\frac{2}{\pi} Q_1 \right)^2 \int_0^1 |S(\alpha)|^2 d\alpha = \left(\frac{2}{\pi} Q_1 \right)^2 \sum_{m=1}^{N} |s_m|^2.$$

(3.1) follows from (3.2) and (3.3), and this completes the proof of the theorem. □

4 Work inspired by Roth's papers

Montgomery [17] discussed Theorem 2 in connection with the large sieve. In Theorem 2 and in the arithmetic form of the large sieve similar quantities are estimated but from the opposite sides. Montgomery gave a different proof for

Theorem 2 and improved slightly on it. He replaced the second term on the left-hand side of (2.1) by

$$\sum_{q=1}^{Q} qV_q(N).$$

He also showed by using the Rudin–Shapiro construction in harmonic analysis that the lower bound in (2.1) is the best possible apart from the implicit constant.

For $N \in \mathbb{N}$ and $E_N = (e_1, \dots, e_N) \in \{-1, +1\}^N$ write

$$f(E_N) = \max_{1 \le n \le n+(k-1)q \le N} \left| \sum_{i=0}^{k-1} e_{n+iq} \right|, \tag{4.1}$$

and let

$$F(N) = \min_{E_N \in \{-1,+1\}^N} f(E_N). \tag{4.2}$$

Then it follows from Corollary 2 that

$$F(N) \gg N^{1/4}. \tag{4.3}$$

From the opposite side Erdős [8] proved that

$$F(N) \ll N^{1/2},$$

and Spencer [32] improved this to

$$F(N) \ll \left(\frac{N \log\log N}{\log N} \right)^{1/2}.$$

Sárközy [9] constructed a sequence $E_N \in \{-1, +1\}^N$ with

$$f(E_N) \ll N^{1/3} (\log N)^{2/3} \tag{4.4}$$

whence

$$F(N) \ll N^{1/3} (\log N)^{2/3}.$$

(Note that this is the only upper bound proved constructively, all the other proofs are existence proofs.) Beck [2] improved the upper bound further to

$$F(N) \ll N^{1/4} (\log N)^{5/2},$$

and finally Matoušek and Spencer [16] proved that

$$F(N) \ll N^{1/4} \tag{4.5}$$

so that (4.3) and thus also Corollaries 1 and 2 are the best possible.

Huxley [13] extended Roth's work to sequences which have been sifted. He showed that a sifted sequence cannot be too evenly distributed in those arithmetic progressions in which it lies.

Choi [4] improved on the constant $\frac{1}{10}$ on the right-hand side of (2.8) in Theorem 3. In [5] Choi showed that the statement of Theorem 4 is valid with $N_1(\Lambda,k) = 2\big(2(\Lambda^{-1}s)^{2s+5^s}\big)^6$ where $s = 2\Lambda\big((2k^2)!\big)^2k^8$. This value of $N_1(\Lambda,k)$ is extremely large and, indeed, for Λ fixed and k large, $N > N_1$ implies that $k = O\big((\log\log\log N/\log\log\log\log N)^{1/2}\big)$ so that even this sharper form of Theorem 4 gives only

$$\max_{n,q,k}\sum_{\nu=0}^{k-1} s_{n+\nu q} > c(\Lambda)\left(\frac{\log\log\log N}{\log\log\log\log N}\right)^{1/4}.$$

Sárközy [28] showed that a much better one-sided estimate can be given for this maximum if we estimate the sums $\sum_{\nu=0}^{k-1} s_{n+\nu q}$ in terms of Q, the upper bound for q, instead of k. Indeed, he proved that if $Q, N \in \mathbb{N}$,

$$Q \le \frac{1}{5}\left(\frac{N}{\Lambda}\right)^{2/5}, \tag{4.6}$$

and $s_1,\dots,s_N$ are real numbers satisfying (2.10) and (2.12), then there exist $n,k,q \in \mathbb{N}$ with $q \le Q$, $n+(k-1)q \le N$ and

$$\sum_{\nu=0}^{k-1} s_{n+\nu q} \ge \frac{1}{40}Q^{1/2}.$$

This lower bound is nearly best possible for any Q satisfying (4.6) (but, perhaps, the upper bound in (4.6) can be replaced by $c(\Lambda)N^{1/2}$). It follows from this result that

$$\max_{n,q,k}\sum_{\nu=0}^{k-1} s_{n+\nu q} > c(\Lambda)N^{1/5} \tag{4.7}$$

(for $s_1,\dots,s_N$ satisfying (2.10) and (2.12)).

As we remarked after Theorem 2 (quoting Roth), the theorem says that a sequence cannot be well-distributed simultaneously *among* and *within* all congruence classes. We are usually more interested in the irregularities of the distribution *among* the congruence classes. However, to ensure the existence of irregularities of this type, one needs an additional assumption. This problem was studied by Sárközy [26], [27], and he proved such a result under the condition that $\big|\{n:\ 1\le n\le N,\ n-1\notin\mathcal{A},\ n\in\mathcal{A}\}\big|$ is "large", i.e., $\mathcal{A}$ consists of many blocks.

The applicability of Theorem 2 and its corollaries is restricted by the fact that only irregularities of size $N^{1/4}$ can be guaranteed, while for a truly random sequence there are irregularities of size $N^{1/2}$. Sárközy [29] showed that

for periodic sequences this gap disappears: if the period is N, then there are irregularities of size $cN^{1/2}$ with a nice explicit constant c, and this lower bound is the best possible apart from the value of c. He applied this result to give lower bounds for character sums, and improved on the earlier constant of Linnik and Rényi. (Later his constant was improved further by Sokolovskii [31].)

Sárközy and Stewart [30] considered the following generalization of the problem studied in Theorem 2: Let $b_1 < b_2 < \dots$ be a sequence of positive integers, $N \in \mathbb{N}$, $s_1, s_2, \dots, s_n \in \mathbb{C}$. Then estimate

$$\max_{a\in\mathbb{Z},q,t\in\mathbb{N}} \left| \sum_{j=1}^{t} s_{a+b_j q} \right|. \tag{4.8}$$

They gave a lower bound for this quantity if the sequence $b_1, b_2, \dots$ does not increase very fast, and also in the special case $b_j = j^2$. The case of general sequences $b_1, b_2, \dots$ was studied by Beck, Sárközy and Stewart in [3]. They proved that if $N, t, Q \in \mathbb{N}$,

$$2t \le Q, \tag{4.9}$$

$b_1 < b_2 < \dots < b_t$ are positive integers, $s_1 s_2, \dots, s_N \in \mathbb{C}$ and we put $s_i = 0$ for $i < 1$ and $i > N$, then we have

$$\sum_{q=1}^{Q} \sum_{a=-Qb_t+1}^{N} \left| \sum_{j=1}^{t} s_{a+b_j q} \right|^2 \ge \frac{tQ}{4} \sum_{n=1}^{N} |s_n|^2.$$

A condition of type (4.9) is necessary, and (4.9) is the best possible apart from the constant factor 2. It follows from this theorem that if also $2tb_t \le N$ is assumed, then the maximum in (4.8) is

$$\ge \frac{t^{1/2}}{\sqrt{8}} \left(\frac{1}{N} \sum_{n=1}^{N} |s_n|^2 \right)^{1/2}.$$

Knieper [14] and Valkó [36] studied different several dimensional generalizations of the problem in Theorem 2, and they gave lower bounds which are the best possible apart from logarithmic factors.

In [35] Valkó studied the irregularities of the distribution of sums $a_i + a_j$ relative to arithmetic progressions.

Lovász [15] gave a new proof for Roth's lower bound $\gg N^{1/4}$ for the maximum of the irregularities in the case of two-colourings, or equivalently sequences whose terms are ± 1, by using standard arguments from the field of semidefinite optimization. Doerr and Srivastav [6] extended the problem to multicolourings, and they gave Roth type lower bounds in this case. Doerr, Srivastav and Wehr [7] studied the same several dimensional generalization of Roth's problem as Knieper [14] and they sharpened some of her results.

5 Summary and open problems

As the quotations from Roth's papers show his main motivation in working in this field was to try to get closer to proving Conjecture 1 of Erdős and Turán. His efforts did not lead to the proof of the conjecture (which was proved later by Szemerédi), however, he opened up a new direction of investigation by studying the irregularities of distribution relative to *long* arithmetic progressions. His papers inspired numerous interesting generalizations and extensions by others, and important applications. These results also help us to understand the nature and limitations of pseudorandomness (see, e.g., [1]) which plays so important a role in cryptography and elsewhere.

The strong impact of Roth's work is due not only to his results but also to the methods developed by him. The ideas and tools which he introduced in [19] and [21] have many applications (these two beautiful papers largely contributed to the present research interest of the first author of this paper).

Finally, to indicate that in spite of the intensive work in this field there is still a long way to go, we conclude this paper by presenting two open problems.

Problem 1. Recall that if $f(E_N)$ and $F(N)$ are defined by (4.1) and (4.2), then by the results of Roth [21], and Matoušek and Spencer [16] we know that $F(N) \asymp N^{1/4}$. However, all the upper estimates given by Erdős, Spencer, Beck and Matoušek are proved by existence proofs. The best construction is still the one in (4.4) with $f(E_N) < N^{\frac{1}{3}+\varepsilon}$. The problem is to improve on this. $f(E_N) = O(N^{1/4})$ will be, perhaps, very difficult but, at least, one might like to give an explicit construction with $f(E_N) < N^{\frac{1}{4}+\varepsilon}$.

Problem 2. While for the absolute values of the irregularities we know the order of magnitude of the best possible estimate, it is not so in the case of one-sided estimates. Recall that the best known lower bound is the one in (4.7): $> c(\Lambda)N^{1/5}$. Almost certainly, the best possible estimate is $> c(\Lambda)N^{1/4}$; the problem is to prove at least $> c(\Lambda)N^{\frac{1}{4}-\varepsilon}$ for $N > N_0(\Lambda, \varepsilon)$.

References

[1] N. Alon, Y. Kohayakawa, C. Mauduit, C.G. Moreira and V. Rödl, Measures of pseudorandomness for finite sequences: minimal values, *Combin. Probab. Comput.* **15** (2006), 1–29.

[2] J. Beck, Roth's estimate of the discrepancy of integer sequences is nearly sharp, *Combinatorica* **1** (1981), 319–325.

[3] J. Beck, A. Sárközy and C.L. Stewart, On irregularities of distribution in shifts and dilations of integer sequences, II, in: *Number Theory in Progress, Proceedings of the International Conference on Number Theory organized by the Stefan Banach International Mathematical Center in Honor of the 60^{th} Birthday of Andrzej Schinzel, Zakopane, Poland, June 30 – July 9,*

1997, eds. K. Győry et al., Walter de Gruyter, Berlin–New York, 1999; 633–638.

[4] S.L.G. Choi, On a theorem of Roth, *Math. Ann.* **179** (1969), 319–328.

[5] S.L.G. Choi, A direct proof of a theorem of Roth, *Math. Ann.* **205** (1973), 1–8.

[6] B. Doerr and A. Srivastav, Multicolour discrepancies, *Combin. Probab. Comput.* **12** (2003), 365–399.

[7] B. Doerr, A. Srivastav and P. Wehr, Discrepancy of Cartesian products of arithmetic progressions, *Electron. J. Combin.* **11** (2004), Research Paper 5, 16 pp.

[8] P. Erdős, Remarks on number theory. V, Extremal problems in number theory, II (in Hungarian), *Mat. Lapok* **17** (1966), 135–155.

[9] P. Erdős and A. Sárközy, Some solved and unsolved problems in combinatorial number theory, *Math. Slovaca* **28** (1978), 407–421.

[10] P. Erdős and P. Turán, On some sequences of integers, *J. London Math. Soc.* **11** (1936), 261–264.

[11] H. Furstenberg, Ergodic behaviour of diagonal measures and a theorem of Szemerédi on arithmetic progressions, *J. d'Analyse Math.* **31** (1977), 204–256.

[12] W.T. Gowers, A new proof of Szemerédi's Theorem, *Geom. Funct. Anal.* **11** (2001), 465–588.

[13] M.N. Huxley, Irregularity in sifted sequences, *J. Number Theory* **4** (1972), 437–454.

[14] P. Knieper, *Discrepancy of Arithmetic Progressions*, Ph. D. thesis, Institut für Informatik, Humboldt-Universität zu Berlin, 1997.

[15] L. Lovász, Integer sequences and semidefinite programming, *Publ. Math. Debrecen* **56** (2000), 475–479.

[16] J. Matoušek and J. Spencer, Discrepancy in arithmetic progressions, *J. Amer. Math. Soc.* **9** (1996), 195–204.

[17] H.L. Montgomery, *Topics in Multiplicative Number Theory*, Springer-Verlag, Berlin, 1971.

[18] K.F. Roth, Sur quelques ensembles d'entiers, *C.R. Acad. Sci. Paris* **234** (1952), 388–390.

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

[20] K.F. Roth, On certain sets of integers, II, *J. London Math. Soc.* **29** (1954), 20–26.

[21] K.F. Roth, Remark concerning integer sequences, *Acta Arith.* **9** (1964), 257–260.

[22] K.F. Roth, Irregularities of sequences relative to arithmetic progressions, *Math. Ann.* **169** (1967), 1–25.

[23] K.F. Roth, Irregularities of sequences relative to arithmetic progressions, II, *Math. Ann.* **174** (1967), 41–52.

[24] K.F. Roth, Irregularities of sequences relative to arithmetic progressions, III, *J. Number Theory* **2** (1970), 125–142.

[25] K.F. Roth, Irregularities of sequences relative to arithmetic progressions, IV, *Period. Math. Hungar.* **2** (1972), 301–326.

[26] A. Sárközy, Some remarks concerning irregularities of distribution of sequences of integers in arithmetic progressions, I, *Coll. Math. Soc. J. Bolyai* **13** (1974), 287–303.

[27] A. Sárközy, Some remarks concerning irregularities of distribution of sequences of integers in arithmetic progressions, II, *Studia Sci. Math. Hungar.* **11** (1976), 79–103.

[28] A. Sárközy, Some remarks concerning irregularities of distribution of sequences of integers in arithmetic progressions, III, *Period. Math. Hungar.* **9** (1978), 127–144.

[29] A. Sárközy, Some remarks concerning irregularities of distribution of sequences of integers in arithmetic progressions, IV, *Acta Math. Acad. Sci. Hungar.* **30** (1977), 155–162.

[30] A. Sárközy and C.L. Stewart, On irregularities of distribution in shifts and dilations of integer sequences, I, *Math. Annalen* **276** (1987), 353–364.

[31] A.V. Sokolovskii, On a theorem of A. Sárközy (in Russian), *Acta Arith.* **41** (1982), 27–31.

[32] J.H. Spencer, A remark on coloring integers, *Canadian Math. Bull.* **15** (1972), 43–44.

[33] E. Szemerédi, On sets of integers containing no four elements in arithmetic progression, *Acta Math. Acad. Sci. Hungar.* **20** (1969), 89–104.

[34] E. Szemerédi, On sets of integers containing no k elements in arithmetic progression, *Acta Arith.* **27** (1975), 199–245.

[35] B. Valkó, On irregularities of sums of integers, *Acta Arith.* **92** (2000), 367–381.

[36] B. Valkó, Discrepancy of arithmetic progressions in higher dimensions, *J. Number Theory* **92** (2002), 117–130.

[37] B. Van der Waerden, Beweis einer Baudetschen Vermutung, *Nieuw Arch. Wisk.* **15** (1927), 212–216.

A. Sárközy
Eötvös Loránd University
Department of Algebra and Number Theory
H–1117 Budapest, Pázmány Péter sétány 1/C
Hungary
e-mail: sarkozy@cs.elte.hu

and

C.L. Stewart
Department of Pure Mathematics
University of Waterloo
Waterloo, Ontario
Canada N2L 3G1
e-mail: cstewart@uwaterloo.ca