COMBINATORICA 1(4) (1981) 319--325

ROTH'S ESTIMATE OF THE DISCREPANCY OF INTEGER SEQUENCES IS NEARLY SHARP

József BECK

Mathematical Institute of the
Hungarian Academy of Sciences
Budapest, Hungary H-1053

Received 29 April 1981

Let g be a coloring of the set $\{1, \ldots, N\}=[1, N]$ in red and blue. For each arithmetic progression A in $[1, N]$, consider the absolute value of the difference of the numbers of red and of blue members of A. Let $R(g)$ be the maximum of this number over all arithmetic progression (the *discrepancy* of g). Set $R(N)=\min_g R(g)$ over all two-colorings g. A remarkable result of K. F. Roth gives* $R(N) \gg N^{1/4}$. On the other hand, Roth observed that $R(N) \ll N^{1/2+\varepsilon}$ and suggested that this bound was nearly sharp. A. Sárközy disproved this by proving $R(N) \ll N^{1/3+\varepsilon}$. We prove that $R(N)=N^{1/4+o(1)}$ thus showing that Roth's original lower bound was essentially best possible.

Our result is more general. We introduce the notion of *discrepancy of hypergraphs* and derive an upper bound from which the above result follows.

1. Introduction

The basic problem of combinatorial discrepancy theory is how to two-color a set as uniformly as possible with respect to a given family of subsets. What we want to achieve is that the coloring be nearly balanced in each of the subsets considered.

Perhaps the most popular problems of this kind are those concerned with the deviation from uniformity of colorings of the integers $[1, N]$ with respect to some families of arithmetic progressions.

The classical example is van der Waerden's theorem (cf. [3]) concerned with *monochromatic* arithmetic progressions. In this case, however, the *length* of the monochromatic arithmetic progressions is *extremely small*. For longer arithmetic progressions, it is interesting to have information about the discrepancy of the coloring, i.e. the difference of the numbers of blue and red points in each progression. A remarkable result of K. F. Roth [4] of this type is the following.

* Following the common usage among number theorists (e.g. [1]), we use the typographically more convenient notation $f(N) \ll g(N)$ to mean $f(N)=O(g(N))$, i.e. $|f(N)/g(N)|$ is bounded.

AMS subject classification (1980): 10 H 20, 10 K 35; 10 L 20, 05 C 65, 05 C 55

Theorem 1.1 (K. F. Roth). *Define* $R(N)=\min_{g}\max_{a,d}\left|\sum_{k} g(a+kd)\right|$, *where the maximum is taken over all arithmetic progressions in* $[1, N]$ *and the minimum is taken over all functions* g: $[1, N]\to\{+1, -1\}$. *Then* $R(N)\gg N^{1/4}$.

In fact, Roth proved that $\left|\sum_{k} g(a+kd)\right|^2$ is "large" on *average*, where the average is taken over all arithmetic progressions in $[1, N]$. Actually, Roth proved, employing the theory of complex variables, the following general result on the discrepancy of sequences with respect to arithmetic progressions.

For notational convenience let

$$M_{h,q}(m) = \{1 \leqq a \leqq m\colon a \equiv h \pmod q\},$$

that is, $M_{h,q}(m)$ denotes the intersection of the congruence hass $h \pmod q$ with the interval $[1, m]$.

Theorem 1.2 (K. F. Roth). *Let* N *be any integer,* $\mathscr{A}$ *a subset of* $[1, N]$. *For positive integers* h, q *and* m, *let*

$$D_{h,q}(m, \mathscr{A}) = D_{h,q}(m) = \left||\mathscr{A}\cap M_{h,q}(m)| - \eta\cdot|M_{h,q}(m)|\right|,$$

where $\eta=|\mathscr{A}|/N$ *denotes the density of* $\mathscr{A}$. *Set*

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

Then for any integer Q,

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

where the implicit constant is absolute.

Choosing $Q=\lfloor N^{1/2}\rfloor$ ($\lfloor x\rfloor$ stands for the greatest integer $\leqq x$), one can easily deduce Theorem 1.1 (details are left to the reader).

As Roth writes, Theorem 1.2 says that a sequence $\mathscr{A}$ cannot be "well-distributed simultaneously among and within all congruence classes".

Let us return to the order of magnitude of $R(N)$. In the other direction, Roth observed that the "probabilistic method" immediately gives $R(N)\ll \ll N^{1/2}\cdot(\log N)^{1/2}$ and suspected that for every $\varepsilon>0$, $R(N)\gg N^{1/2-\varepsilon}$. P. Erdős (cf. [2], § 8) showed that $R(N)\ll N^{1/2}$. J. Spencer [5] subsequently improved this to $R(N)=o(N^{1/2})$, more precisely $R(N)\ll N^{1/2}\dfrac{\log\log N}{\log N}$. A. Sárközy (cf. [2], § 8) unexpectedly reduced the upper bound to $R(N)\ll N^{1/3+\varepsilon}$, disproving the conjecture of Roth. The objective of this paper is to prove $R(N)\ll N^{1/4+\varepsilon}$. This shows that Roth's lower bound is essentially best possible.

Theorem 1.3. $R(N)\ll N^{1/4}\cdot(\log N)^{5/2}$.

2. Discrepancy of hypergraphs

We introduce some notation. $|H|$ denotes the number of elements of the set H. By a hypergraph we mean a finite family of finite sets. Given a hypergraph $\mathscr{H}$, let

$$S(\mathscr{H}) = \text{vertex-set of } \mathscr{H} = \bigcup_{A\in\mathscr{H}} A,$$

$$\mathrm{Deg}(\mathscr{H}, x) = \text{degree of } x \text{ in } \mathscr{H} = |\{A\in\mathscr{H}\colon x\in A\}|,$$

$$\mathrm{Deg}(\mathscr{H}) = \text{degree of } \mathscr{H} = \max_x \mathrm{Deg}(\mathscr{H}, x),$$

$$\mathrm{Disc}(\mathscr{H}) = \text{discrepancy of } \mathscr{H} = \min_g \max_{A\in\mathscr{H}} \Big|\sum_{x\in A} g(x)\Big|,$$

where the minimum is extended over all functions $g\colon S(\mathscr{H})\to\{+1, -1\}$.

In order to prove Theorem 1.3, we state a general upper bound on the discrepancy of hypergraphs.

Theorem 2.1. *Let $\mathscr{H}$ be a hypergraph and assume that one can find a real number t such that*

$$\mathrm{Deg}(\{A\in\mathscr{H}\colon |A|\geqq t\})\leqq t.$$

Then

$$\mathrm{Disc}(\mathscr{H})\leqq c_0\cdot t^{1/2}\cdot(\log|\mathscr{H}|)^{1/2}\cdot\log|S(\mathscr{H})|,$$

where c_0 is a universal constant.

First we deduce Theorem 1.3 from Theorem 2.1. For notational convenience let $\mathrm{AP}(a, d, i, j)$, $i\leqq j$, denote the arithmetic progression with difference d, starting from $a+id$ and terminating at $a+jd$, i.e.

$$\mathrm{AP}(a, d, i, j) = \{a+kd\colon i\leqq k\leqq j\}.$$

We call an arithmetic progression *elementary* if its length is a power of 2, say 2^s, $s\geqq 0$, it has difference $d\geqq 1$ and starts from $b+(i2^s)d$, where $1\leqq b\leqq d$ and $i\geqq 0$, or more formally, if it is of type $\mathrm{AP}(b, d, i2^s, (i+1)2^s-1)$, where $1\leqq b\leqq d$, $d\geqq 1$, $i\geqq 0$ and $s\geqq 0$.

Let $\mathscr{H}_N$ denote the family of elementary arithmetic progressions contained in $[1, N]$, i.e.

$$\mathscr{H}_N = \{\mathrm{AP}(b, d, i2^s, (i+1)2^s-1)\subseteqq[1, N]\colon 1\leqq b\leqq d,\ d\geqq 1,\ i\geqq 0,\ s\geqq 0\}.$$

By definition

$$\mathrm{Deg}(\{A\in\mathscr{H}_N\colon |A|\geqq k\}) = \max_m \big|m\in\mathrm{AP}(b, d, i2^s, (i+1)2^s-1)\subseteqq$$

$$\subseteqq[1, N]\colon 2^s\geqq k\}\big| = \max_m \sum_{1\leqq d\leqq n/k}\ \sum_{\substack{1\leqq b\leqq d\\ b\equiv m(\mathrm{mod}\,d)}}\ \sum_s{}' 1,$$

where the summation $\sum'$ is taken over all s for which $2^s\geqq k$ and $b+(2^s-1)d\leqq N$.

Simple calculation shows that

$$\sum_s{}' 1\leqq\log_2(N/(dk)),$$

($\log_2 x$ stands for base 2 logarithms.) Thus we obtain

$$\mathrm{Deg}\,(\{A\in\mathscr{H}_N\colon |A|\geqq k\}) \leqq \max_m \sum_{1\leqq d\leqq N/k} \sum_{\substack{1\leqq b\leqq d\\ b\equiv m(\mathrm{mod}\,d)}} \log_2(N/dk) =$$

$$= \sum_{1\leqq d\leqq N/k} \log_2(N/dk) \leqq c_1 N/k$$

with a suitable constant c_1.

Set $t=(c_1N)^{1/2}$. Applying Theorem 2.1 to $\mathscr{H}_N$ we conclude that

$$\mathrm{Disc}\,(\mathscr{H}_N) \leqq c_0 t^{1/2}(\log|\mathscr{H}_N|)^{1/2}\log|S(\mathscr{H}_N)| \ll N^{1/4}(\log N)^{3/2}, \tag{1}$$

since clearly $|\mathscr{H}_N|\leqq N^2$ and $S(\mathscr{H}_N)=[1, N]$.

We claim

$$R(N) \leqq 2\log_2 N\,\mathrm{Disc}\,(\mathscr{H}_N). \tag{2}$$

First observe that any arithmetic progression $\{a, a+d, \ldots, a+md\}\subseteqq[1, N]$ is representable in the form

$$\mathrm{AP}\,(b, d, 0, p_1)\setminus\mathrm{AP}\,(b, d, 0, p_2),$$

where $a=b+p_2d$, $1\leqq b\leqq d$, and $p_1=m+p_2$. Moreover, both $\mathrm{AP}\,(b, d, 0, p_i)$, $i=1, 2$, are unions of not more than $\log_2 N$ disjoint elementary intervals, that is, disjoint members of $\mathscr{H}_N$. More formally,

$$\mathrm{AP}\,(b, d, 0, p_i) = \bigcup_{r=1}^{l_i} \mathrm{AP}\left(b, d, \sum_{j=1}^{r-1} 2^{s(i,j)}, \sum_{j=1}^{r} 2^{s(i,j)} - 1\right),$$

where

$$p_i+1 = \sum_{j=1}^{l_i} 2^{s(i,j)},\ s(i, 1) > s(i, 2) > \ldots > s(i, l_i).$$

Since $l_i\leqq\log_2(p_i+1)\leqq\log_2 N$, then (2) follows.

By (1) and (2) we obtain

$$R(N) \leqq 2\log_2 N\,\mathrm{Disc}\,(\mathscr{H}_N) \ll N^{1/4}(\log N)^{5/2}.$$

completing the deduction of Theorem 1.3 from Theorem 2.1. ∎

3. The basic lemma

The proof of Theorem 2.1 will consist of a repeated application of the following result.

Lemma 3.1. *Under the hypothesis of Theorem* 2.1 *there exists a function* $f\colon S(\mathscr{H})\to\{0, +1, -1\}$ *such that*

$$\left|\sum_{x\in A} f(x)\right| \leqq c_2 t^{1/2}(\log|\mathscr{H}|)^{1/2} \quad \textit{for every} \quad A\in\mathscr{H}, \tag{3}$$

and

$$|\{x\in S(\mathscr{H}): f(x)=0\}| \leqq \frac{9}{10}|S(\mathscr{H})|, \tag{4}$$

where c_2 is a universal constant.

Proof. Set $\mathscr{H}^*=\{A\in\mathscr{H}: |A|\geqq t\}$. Let $|S(\mathscr{H})|=N$ and $|\mathscr{H}^*|=K$. Let G denote the set of 2^N functions $g: S(\mathscr{H})\to\{+1,-1\}$. Using the well-known asymptotic properties of the binomial coefficients (cf. Chernoff [1]) we obtain for every fixed $A\in\mathscr{H}$

$$\left|\left\{g\in G: \left|\sum_{x\in A} g(x)\right| > 2\mu|A|^{1/2}\right\}\right| = 2^{N-|A|}\sum_{|i-|A|/2|>\mu|A|^{1/2}}\binom{|A|}{i} \leqq 2^N e^{-\mu^2/2}.$$

From this it follows that for a sufficiently large constant c_3 the cardinality of the set

$$G_1=\left\{g\in G: \left|\sum_{x\in A} g(x)\right| \leqq c_3(|A|\log|\mathscr{H}|)^{1/2} \quad \text{for every} \quad A\in\mathscr{H}\right\}$$

is greater than 2^{N-1}.

Let $\mathscr{H}^*=\{A_1,\ldots,A_K\}$, and for each i, $1\leqq i\leqq K$, let us partition the interval

$$I_i=[-c_3(|A_i|\log|\mathscr{H}|)^{1/2},\ c_3(|A_i|\log|\mathscr{H}|)^{1/2}]$$

into $\lfloor(|A_i|/t)^{1/2}\rfloor$ equal segments,

$$I_i=\bigcup_{j=1}^{r_i} I_{i,j} \quad \text{with} \quad r_i=\lfloor(|A_i|/t^{1/2}\rfloor.$$

Let us now associate with every function $g\in G_1$ the K-dimensional vector $\vec{v}(g)$ as follows: if

$$\sum_{x\in A_i} g(x)\in I_{i,j_i}, \quad 1\leqq i\leqq K,$$

then let

$$\vec{v}(g)=(j_1,j_2,\ldots,j_K).$$

We are going to prove that there are at most $2^{3N/10}$ such vectors. By definition

$$|\{\vec{v}(g): g\in G_1\}| \leqq \prod_{i=1}^{K} r_i \leqq \left(\prod_{i=1}^{K}\frac{|A_i|}{t}\right)^{1/2} \leqq \exp\left\{\sum_{i=1}^{K}|A_i|/2et\right\} < \exp\left\{\sum_{i=1}^{K}|A_i|/5t\right\}.$$

Here we used the following well-known elementary inequality:

For any positive reals $b_1,\ldots,b_K$,

$$\prod_{i=1}^{K} b_i \leqq \exp\left(\sum_{i=1}^{K} b_i/e\right). \tag{5}$$

By the hypothesis of the lemma, $\mathrm{Deg}\,(\mathscr{H}^*)\leqq t$. Therefore

$$\sum_{i=1}^{K}|A_i| = \sum_{x\in S(\mathscr{H})}\mathrm{Deg}\,(\mathscr{H}^*,x) \leqq |S(\mathscr{H})|\,\mathrm{Deg}\,(\mathscr{H}^*) \leqq |S(\mathscr{H})|\,t.$$

Thus we have $\sum_{i=1}^{K} |A_i|/5t \leqq |S(\mathscr{H})|/5 = N/5$ and

$$|\{\vec{v}(g):\ g \in G_1\}| < \exp\left\{\sum_{i=1}^{K} |A_i|/5t\right\} < e^{N/5} < 2^{3N/10},$$

as stated.

By the pigeonhole principle we conclude that there is a subset $G_2 \subset G_1$ such that $|G_2| \geqq |G_1| 2^{-3N/10} \geqq 2^{7N/10-1}$ and $\vec{v}(g') = \vec{v}(g'')$ for all $g', g'' \in G_2$.

Choosing an element $g_0 \in G_2$, set

$$F_2 = \{(g_0 - g)/2:\ g \in G_2\}.$$

By definition F_2 is a set of functions $f\colon S(\mathscr{H}) \to \{0, +1, -1\}$ with the properties that

$$\left|\sum_{x \in A} f(x)\right| \leqq 2 \max_{g \in G_2} \left|\sum_{x \in A} g(x)\right| \leqq 2c_3(|A| \log |\mathscr{H}|)^{1/2} \leqq 2c_3(t \log |\mathscr{H}|)^{1/2},$$

for every $A \in \mathscr{H} \setminus \mathscr{H}^* = \{A \in \mathscr{H}:\ |A| < t\}$, and

$$\left|\sum_{x \in A} f(x)\right| \leqq \max_{i,j} \text{length } I_{i,j}$$

for every $A \in \mathscr{H}^*$. Since $I_{i,j}$ has length exactly

$$2c_3(|A_i| \log |\mathscr{H}|)^{1/2} / \lfloor (|A_i|/t)^{1/2} \rfloor = c_4 t^{1/2} (\log |\mathscr{H}|)^{1/2},$$

we conclude that every element of F_2 satisfies inequality (3) in the lemma. Therefore it remains to find an element of F_2 satisfying (4).

Let F^* denote the set of functions $f\colon S(\mathscr{H}) \to \{0, +1, -1\}$ such that

$$|\{x \in S(\mathscr{H}):\ f(x) = 0\}| \geqq \frac{9}{10} |S(\mathscr{H})| = \frac{9N}{10}.$$

Clearly

$$|F^*| = \sum_{i=0}^{\lfloor N/10 \rfloor} \binom{N}{i} 2^i \leqq 2 \binom{N}{\lfloor N/10 \rfloor} 2^{N/10} < 2^{7N/10-1} \leqq |F_2|,$$

so that the difference $F_2 \setminus F^*$ is non-empty. The lemma follows. ∎

4. Proof of Theorem 2.1

Lemma 3.1 yields the existence of a function $f_1\colon S(\mathscr{H}) \to \{0, +1, -1\}$ satisfying (3), (4). Let $\mathscr{H}_1$ be the restriction of $\mathscr{H}$ to

$$f_1^{-1}(0) = \{x \in S(\mathscr{H}):\ f_1(x) = 0\},$$

that is, let

$$\mathscr{H}_1 = \{A \cap f_1^{-1}(0):\ A \in \mathscr{H}\}.$$

Obviously $\deg(\{B \in \mathscr{H}_1:\ |B| \geqq t\}) \leqq \deg(\{A \in \mathscr{H}:\ |A| \geqq t\}) \leqq t$. Applying Lemma 3.1 to $\mathscr{H}_1$ we obtain the existence of a function $f_2\colon S(\mathscr{H}_1) \to \{0, +1, -1\}$ satisfying

(3), (4). Repeating this argument, at the i-th step we obtain a function f_i: $S(\mathscr{H}_{i-1}) \to \{0, +1, -1\}$ such that

$$\Big|\sum_{x \in B} f_i(x)\Big| \leqq c_2 t^{1/2}(\log |\mathscr{H}_{i-1}|)^{1/2} \quad \text{for every} \quad B \in \mathscr{H}_{i-1},$$

and

$$|\{x \in S(\mathscr{H}_{i-1}): f_i(x) = 0\}| \geqq \frac{9}{10}|S(\mathscr{H}_{i-1})|.$$

The procedure stops within

$$W = \lfloor \log |S(\mathscr{H})|/\log (10/9) \rfloor + 1$$

steps, since

$$|S(\mathscr{H}_i)| = |\{x \in S(\mathscr{H}_{i-1}): f_i(x) = 0\}| \geqq \frac{9}{10}|S(\mathscr{H}_{i-1})| \geqq \left(\frac{9}{10}\right)^i |S(\mathscr{H})|.$$

Set $g = \sum_{i \geqq 1} f_i$. Observe that g has only values ± 1. For $A \in \mathscr{H}$ let $A^{(i)}$ denote $A \cap S(\mathscr{H}_i)$ for $i \geqq 1$ and set $A^{(0)} = A$. Clearly $A^{(i)} \in S(\mathscr{H}_i)$. From the definition of the procedure above follows

$$\Big|\sum_{x \in A} g(x)\Big| = \Big|\sum_{i \geqq 1} \sum_{x \in A^{(i-1)}} f_i(x)\Big| \leqq \sum_{i \geqq 1} \Big|\sum_{x \in A^{(i-1)}} f_i(x)\Big| \leqq$$

$$\leqq \sum_{i \geqq 1} c_2 t^{1/2}(\log |\mathscr{H}_{i-1}|)^{1/2} \leqq c_2 t^{1/2}(\log |\mathscr{H}|)^{1/2} W,$$

for every $A \in \mathscr{H}$. Thus Theorem 2.1 is proved. ∎

References

[1] H. Chernoff, A measure of asymptotic efficiency of tests of a hypothesis based on the sum of observations, *Ann. Math. Stat.* **23** (1952), 493—509.

[2] P. Erdős and J. Spencer, *Probabilistic Methods in Combinatorics*, Akadémiai Kiadó, Budapest, 1974.

[3] R. L. Graham, B. L. Rothschild and J. Spencer, *Ramsey Theory*, John Wiley, New York, 1980.

[4] K. F. Roth, Remark concerning integer sequences, *Acta Arithmetica* **9** (1964), 257—260.

[5] J. Spencer, A remark on coloring integers, *Canad. Math. Bull.* **14** (1971), 45—47.