DISCREPANCY OF ARITHMETIC PROGRESSIONS IN HIGHER DIMENSIONS

BENEDEK VALKÓ (BUDAPEST)

1. Introduction

Let $\mathcal{H}$ be a family of subsets of a finite set X. We say that a function $f : X \to \{-1, +1\}$ is a two-coloring of X and for every $Y \subseteq X$ we define $f(Y) = \sum_{x \in Y} f(x)$. The discrepancy of $\mathcal{H}$ is defined by $\operatorname{disc}(\mathcal{H}) = \min_f \max_{Y \in \mathcal{H}} |f(Y)|$ where the minimum is extended over all two-colorings of X.

In 1964 K. F. Roth [4] proved that if $\mathcal{H}$ is the family of all arithmetic progressions on $[1, N] = \{1, 2, \ldots, N\}$ then $\operatorname{disc}(\mathcal{H}) \geq cN^{\frac{1}{4}}$. Roth thought that his result is not sharp and instead $\operatorname{disc}(\mathcal{H}) = N^{\frac{1}{2} - o(1)}$ might be true. A. Sárközy disproved this conjecture [2] by showing that $\operatorname{disc}(\mathcal{H}) = O\left(N^{\frac{1}{3}+\varepsilon}\right)$. In 1981 J. Beck [1] proved that Roth's result is nearly sharp, that is $\operatorname{disc}(\mathcal{H}) \leq cN^{\frac{1}{4}} \ln^{\frac{5}{2}} N$. Using his methods J. Matoušek and J. Spencer [5] were able to prove that the theorem is indeed sharp.

Over the years Roth's paper inspired the study of several similar problems. In [3] P. Knieper generalized the problem in d dimensions: let $\mathcal{H}$ be the family of all sets on $[1, N]^d$ which are the Cartesian product of d arbitrary arithmetic progressions on $[1, N]$ ($d = 1$ gives back the original problem). She proved that $\operatorname{disc}(\mathcal{H}) \geq cN^{\frac{d}{4}}$ and showed that this result is sharp apart of logarithmic powers.

In this paper we consider another possible generalization in higher dimensions. Let $\mathcal{H}$ be the family of all arithmetic progressions contained in $[1, N]^d$, i.e.

$$\mathcal{H} = \left\{ \{\underline{a} + k \cdot \underline{b} : 0 \leq k \leq r\} \subset [1, N]^d \right\}$$

($d = 1$ also gives back the original problem). We show that $\operatorname{disc}(\mathcal{H}) \geq cN^{\frac{d}{2d+2}}$ and prove that this is nearly sharp, $\operatorname{disc}(\mathcal{H}) \leq cN^{\frac{d}{2d+2}} (\log N)^{\frac{5}{2}}$. The proof of the lower bound uses exponential sums it's the adaptation of Roth's method. For the upper bound we use a general estimate of Beck for discrepancy of hypergraphs. In the last section we use our results to give an upper estimate for a problem proposed by Knieper and we prove a theorem concerning the discrepancy of certain random hypergraphs.

2. Lower bound for the discrepancy

Throughout the paper underlined letters will denote d-dimensional vectors (in $\mathbb{R}^d$ or $\mathbb{Z}^d$) and we use the notation $e(a) = e^{2\pi i a}$.

The following theorem gives the lower bound for the discrepancy:

Theorem 2.1. *Let f be an arbitrary two-coloring of $[1,N]^d$. Then there exists an arithmetic progression $\underline{a}, \underline{a}+\underline{b}, \dots, \underline{a}+r\cdot\underline{b}$ on $[1,N]^d$ with $\left|\sum_{k=0}^{r} f(\underline{a}+k\cdot\underline{b})\right| \geq cN^{\frac{d}{2d+2}}$ (the constant c is absolute).*

We will prove that the inequality stated above is even true in a mean square sense regarding a large subset of the arithmetic progressions on $[1,N]^d$. For the proof we need the d-dimensional version of one of Roth's theorems:

Theorem 2.2. *Let $\left\{c_{\underline{a}}, \underline{a} \in [1,N]^d\right\}$ be a fixed set of complex numbers. We set $c_{\underline{a}} = 0$ if $\underline{a} \notin [1,N]^d$. Let Q, Q_1 be positive integers with $Q^d \geq 2Q_1$. For $\underline{a}, \underline{b} \in \mathbb{Z}^d$ we define $D(\underline{a},\underline{b}) = \sum_{k=0}^{Q_1-1} c_{\underline{a}+k\cdot\underline{b}}$. We use the notation*

$$\mathcal{A} = \{\underline{b} : \underline{b} = (b_1, b_2, \dots, b_d) \neq \underline{0}, |b_i| \leq Q \text{ for every } 1 \leq i \leq d\}$$

and

$$\mathcal{B}(\underline{b}) = \bigcup_{k=0}^{Q_1-1} \left([1,N]^d - k\cdot\underline{b}\right).$$

Then

$$\sum_{\underline{b}\in\mathcal{A}} \sum_{\underline{a}\in\mathcal{B}(\underline{b})} |D(\underline{a},\underline{b})|^2 \geq \left(\frac{2}{\pi}Q_1\right)^2 \sum_{\underline{a}\in[1,N]^d} \left|c_{\underline{a}}\right|^2.$$

For $\underline{\alpha} \in [0,1]^d$ we define $S(\underline{\alpha}) = \sum_{\underline{a}\in[1,N]^d} c_{\underline{a}} \cdot e(\langle \underline{a}, \underline{\alpha}\rangle)$ and for $x \in [0,1]$ we set $F(x) = \sum_{k=0}^{Q_1-1} e(kx)$.

Proof. The main idea of the proof is the estimation of the following integral:

$$J = \int_{[0,1]^d} |S(\underline{\alpha})|^2 \sum_{\underline{b}\in\mathcal{A}} |F(\langle \underline{b}, \underline{\alpha}\rangle)|^2 \, d\underline{\alpha}.$$

Let $\underline{b} \in \mathcal{A}$ be a fixed vector and consider $\int_{[0,1]^d} |S(\underline{\alpha})|^2 |F(\langle \underline{b}, \underline{\alpha}\rangle)|^2 \, d\underline{\alpha}$.

$$\begin{aligned}
\int_{[0,1]^d} |S(\underline{\alpha})|^2 |F(\langle \underline{b}, \underline{\alpha}\rangle)|^2 \, d\underline{\alpha} &= \int_{[0,1]^d} \left| \left(\sum_{\underline{a}\in[1,N]^d} c_{\underline{a}} \cdot e(\langle \underline{a}, \underline{\alpha}\rangle) \right) \left(\sum_{k=0}^{Q_1-1} e(k\cdot\langle \underline{b}, \underline{\alpha}\rangle) \right) \right|^2 d\underline{\alpha} \\
&= \int_{[0,1]^d} \left| \sum_{\underline{a}\in[1,N]^d} c_{\underline{a}} \cdot \sum_{k=0}^{Q_1-1} e(\langle \underline{a}+k\cdot\underline{b}, \underline{\alpha}\rangle) \right|^2 d\underline{\alpha}
\end{aligned}$$

An easy meditation shows that

$$\sum_{\underline{a}\in[1,N]^d} c_{\underline{a}} \cdot \sum_{k=0}^{Q_1-1} e(\langle \underline{a}+k\cdot\underline{b}, \underline{\alpha}\rangle) = \sum_{\underline{a}\in\mathcal{B}(\underline{b})} e(\langle \underline{a}, \underline{\alpha}\rangle) \left(\sum_{k=0}^{Q_1-1} c_{\underline{a}+k\cdot\underline{b}} \right).$$

From the d-dimensional version of Parseval's formula

$$\int\limits_{[0,1]^d} \left| \sum_{\underline{a}\in\mathcal{B}(\underline{b})} e\left(\langle \underline{a}, \underline{\alpha}\rangle\right) \left(\sum_{k=0}^{Q_1-1} c_{\underline{a}+k\cdot\underline{b}} \right) \right|^2 d\underline{\alpha} = \sum_{\underline{a}\in\mathcal{B}(\underline{b})} \left| \sum_{k=0}^{Q_1-1} c_{\underline{a}+k\cdot\underline{b}} \right|^2 = \sum_{\underline{a}\in\mathcal{B}(\underline{b})} \left| D\left(\underline{a}, \underline{b}\right)\right|^2$$

and therefore

$$J = \sum_{\underline{b}\in\mathcal{A}} \sum_{\underline{a}\in\mathcal{B}(\underline{b})} \left| D\left(\underline{a}, \underline{b}\right)\right|^2 .$$

For the proof of Theorem 2.2 we need a lower estimation for J. In Lemma 2.3 we shall prove that for every $\underline{\alpha} \in [0,1]^d$

$$\sum_{\underline{b}\in\mathcal{A}} \left| F\left(\langle \underline{b}, \underline{\alpha}\rangle\right)\right|^2 \geq \left(\frac{2}{\pi} Q_1\right)^2 .$$

From this the theorem follows, since

$$\begin{aligned} J &\geq \min_{\underline{\alpha}\in[0,1]^d} \sum_{\underline{b}\in\mathcal{A}} \left| F\left(\langle \underline{b}, \underline{\alpha}\rangle\right)\right|^2 \int\limits_{[0,1]^d} \left| S\left(\underline{\alpha}\right)\right|^2 d\underline{\alpha} \\ &= \min_{\underline{\alpha}\in[0,1]^d} \sum_{\underline{b}\in\mathcal{A}} \left| F\left(\langle \underline{b}, \underline{\alpha}\rangle\right)\right|^2 \sum_{\underline{a}\in[1,N]^d} \left| c_{\underline{a}}\right|^2 \\ &\geq \left(\frac{2}{\pi} Q_1\right)^2 \sum_{\underline{a}\in[1,N]^d} \left| c_{\underline{a}}\right|^2 \end{aligned}$$

□

Lemma 2.3.

$$\sum_{\underline{b}\in\mathcal{A}} \left| F\left(\langle \underline{b}, \underline{\alpha}\rangle\right)\right|^2 \geq \left(\frac{2}{\pi} Q_1\right)^2$$

Proof. It is easy to see that $\left|F\left(x\right)\right|^2 = \frac{\sin^2(\pi Q_1 x)}{\sin^2(\pi x)}$ and

$$\text{if } \|x\| \leq \frac{1}{2Q_1} \text{ then } \left|F\left(x\right)\right|^2 \geq \left(\frac{2}{\pi} Q_1\right)^2$$

($\|x\|$ denotes the distance of x from the nearest integer). Using Dirichlet's Theorem on simultaneous approximation it is clear that for every $\underline{\alpha} \in [0,1]^d$ there exists a vector $\underline{b}^* \in \mathcal{A}$ with $\|\langle \underline{b}^*, \underline{\alpha}\rangle\| \leq \frac{1}{Q^d} \leq \frac{1}{2Q_1}$. From this the lemma follows:

$$\sum_{\underline{b}\in\mathcal{A}} \left| F\left(\langle \underline{b}, \underline{\alpha}\rangle\right)\right|^2 \geq \left| F\left(\langle \underline{b}^*, \underline{\alpha}\rangle\right)\right|^2 \geq \left(\frac{2}{\pi} Q_1\right)^2$$

□

Now we are ready for our main theorem.

Proof of Theorem 2.1. We use Theorem 2.2 with $c_{\underline{a}} = f(\underline{a})$ ($\underline{a} \in [1,N]^d$), and $Q = \left\lfloor 2N^{\frac{1}{d+1}} \right\rfloor$, $Q_1 = \left\lfloor \frac{Q^d}{2} \right\rfloor$(clearly $Q^d \geq 2Q_1$). Then as the theorem states

$$\sum_{\underline{b}\in\mathcal{A}} \sum_{\underline{a}\in\mathcal{B}(\underline{b})} \left|D\left(\underline{a},\underline{b}\right)\right|^2 \geq \left(\frac{2}{\pi}Q_1\right)^2 \sum_{\underline{a}\in[1,N]^d} \left|f\left(\underline{a}\right)\right|^2 = \left(\frac{2}{\pi}Q_1\right)^2 N^d.$$

Let $M = \max_{\underline{b}\in\mathcal{A},\underline{a}\in\mathcal{B}(\underline{b})} \left|D\left(\underline{a},\underline{b}\right)\right|$. From the previous inequality we have

$$M^2 \sum_{\underline{b}\in\mathcal{A}} \left|\mathcal{B}\left(\underline{b}\right)\right| \geq \left(\frac{2}{\pi}Q_1\right)^2 N^d.$$

Let $\underline{b} = (b_1, b_2, \dots, b_d) \in \mathcal{A}$ a fixed vector. Then

$$\begin{aligned}
\mathcal{B}\left(\underline{b}\right) &= \bigcup_{k=0}^{Q_1-1} \left([1,N]^d - k\cdot\underline{b}\right) \\
&= \left(\bigcup_{k=0}^{Q_1-2} \left([1,N]^d - k\cdot\underline{b}\right) \setminus \left([1,N]^d - (k+1)\cdot\underline{b}\right)\right) \bigcup \left([1,N]^d - (Q_1-1)\cdot\underline{b}\right)
\end{aligned}$$

where now all Q_1 sets are disjunct. Clearly

$$\begin{aligned}
\left|\left([1,N]^d - k\cdot\underline{b}\right) \setminus \left([1,N]^d - (k+1)\cdot\underline{b}\right)\right| &= \left|\left([1,N]^d\right) \setminus \left([1,N]^d - \underline{b}\right)\right| \\
&= N^d - \prod_{i=1}^{d} \left(N - |b_i|\right),
\end{aligned}$$

therefore

$$\left|\mathcal{B}\left(\underline{b}\right)\right| = (Q_1-1)\left(N^d - \prod_{i=1}^{d}\left(N-|b_i|\right)\right) + N^d = Q_1N^d - (Q_1-1)\prod_{i=1}^{d}\left(N-|b_i|\right).$$

Thus

$$\begin{aligned}
\sum_{\underline{b}\in\mathcal{A}} \left|\mathcal{B}\left(\underline{b}\right)\right| &= \left(\sum_{-Q\leq b_1\leq Q}\ \sum_{-Q\leq b_2\leq Q} \cdots \sum_{-Q\leq b_d\leq Q} \left|\mathcal{B}\left(\underline{b}\right)\right|\right) - \left|\mathcal{B}\left(\underline{0}\right)\right| \\
&= \left(\sum_{-Q\leq b_1\leq Q}\ \sum_{-Q\leq b_2\leq Q} \cdots \sum_{-Q\leq b_d\leq Q} \left(Q_1N^d - (Q_1-1)\prod_{i=1}^{d}\left(N-|b_i|\right)\right)\right) - N^d \\
&= \left((2Q+1)^d Q_1 - 1\right)N^d - (Q_1-1)\prod_{i=1}^{d}\ \sum_{-Q\leq b_i\leq Q}\left(N-|b_i|\right) \\
&= \left((2Q+1)^d Q_1 - 1\right)N^d - (Q_1-1)\left((2Q+1)N - Q(Q+1)\right)^d.
\end{aligned}$$

If $x \geq y \geq 0$ then

$$dx^{d-1}y \geq y\sum_{j=0}^{d-1} x^{d-1-j}(x-y)^j = x^d - (x-y)^d$$

thus

$$(x-y)^d \geq x^d - dx^{d-1}y.$$

Using this with $x = (2Q+1)\,N$ and $y = Q\,(Q+1)$ we have

$$\begin{aligned}\sum_{\underline{b}\in\mathcal{A}} |\mathcal{B}(\underline{b})| &\le \left((2Q+1)^d Q_1 - 1\right) N^d - (Q_1-1)\left((2Q+1)^d N^d - dQ\,(Q+1)\,(2Q+1)^{d-1} N^{d-1}\right) \\ &= \left((2Q+1)^d - 1\right) N^d + d\,(Q_1-1)\,Q\,(Q+1)\,(2Q+1)^{d-1} N^{d-1} \\ &\le 3^d Q^d N^d + d\, 3^d Q_1 Q^{d+1} N^{d-1} \\ &\le c_1(d)\cdot Q_1 N^{d-1}(N+QQ_1).\end{aligned}$$

Comparing this with

$$M^2 \sum_{\underline{b}\in\mathcal{A}} |\mathcal{B}(\underline{b})| \ge \left(\frac{2}{\pi}Q_1\right)^2 N^d$$

we have

$$M \ge \sqrt{c_2(d)\,\frac{Q_1^2 N^d}{Q_1 N^{d-1}(N+QQ_1)}} \ge c(d)\cdot N^{\frac{d}{2d+2}}$$

and that is what we had to prove. □

3. Upper bound for the discrepancy

Theorem 3.1.

$$\operatorname{disc}(\mathcal{H}) \le cN^{\frac{d}{2d+2}}(\log N)^{\frac{5}{2}}$$

(with an absolute constant c).

For the upper bound we apply a theorem of Beck on the discrepancy of general hypergraphs which he used in his proof about the discrepancy of arithmetic progressions on $[1,N]$. First we introduce a couple of notations. If $\mathcal{H}$ is a hypergraph then let

$$\begin{aligned} S(\mathcal{H}) &= \bigcup_{A\in\mathcal{H}} A && \text{(the vertex-set of } \mathcal{H}) \\ \deg(\mathcal{H},x) &= |\{A\in\mathcal{H} : x\in A\}| && \text{(the degree of } x \text{ in } \mathcal{H}) \\ \deg(\mathcal{H}) &= \max_x \deg(\mathcal{H},x) && \text{(the degree of } \mathcal{H}).\end{aligned}$$

Theorem 3.2 (Beck)**.** *Let $\mathcal{H}$ be a hypergraph and assume that there exists a real number t such that*

$$deg(\{A\in\mathcal{H} : |A|\ge t\}) \le t.$$

Then

$$disc(\mathcal{H}) \le c_0\sqrt{t}\sqrt{(\log|\mathcal{H}|)}\,\log|S(\mathcal{H})|,$$

where c_0 is an absolute constant.

Now we are ready to prove Theorem 3.1.

Proof of Theorem 3.1. For $i\le j$ let $\mathrm{AP}(\underline{a},\underline{b},i,j)$ denote the arithmetic progression with difference $\underline{b}$ starting from $\underline{a}+i\underline{b}$ and terminating at $\underline{a}+j\underline{b}$. We say that an arithmetic progression is *elementary* if its length is a power of 2 (for example 2^s, $s\ge 0$), it has a difference $\underline{b}\ne\underline{0}$ and starts from $\underline{a}+(i2^s)\,\underline{b}$ where $i\ge 0$ and $\underline{a}\in[1,N]^d\setminus\left([1,N]^d-\underline{b}\right)$. Formally an arithmetic progression is elementary if it is of type $\mathrm{AP}(\underline{a},\underline{b},i2^s,(i+1)\,2^s-1)$ where i, s, $\underline{a}$, $\underline{b}$ meet the previous conditions. Let

$\mathcal{H}_N$ denote the family of elementary arithmetic progressions contained in $[1,N]^d$. We will give an estimate for $\deg(\{A\in\mathcal{H}_N : |A|\geq k+1\})$ where k is a fixed positive integer. From the definitions we have

$$\deg\left(\{A\in\mathcal{H}_N : |A|\geq k+1\}\right)=\max_{\underline{m}}\left|\left\{\underline{m}\in \mathrm{AP}\left(\underline{a},\underline{b},i2^s,(i+1)\,2^s-1\right)\subseteq[1,N]^d : 2^s\geq k+1\right\}\right|$$

(where $\mathrm{AP}(\underline{a},\underline{b},i2^s,(i+1)\,2^s-1)$ is elementary).

First we establish some simple relations between the parameters. If there is an arithmetic progression contained in $[1,N]^d$ with a difference of $\underline{b}$ and a length of at least $k+1$ then for every $1\leq j\leq d$ the following inequality must stand:

$$-\frac{N}{k}\leq b_j\leq\frac{N}{k},$$

(where $\underline{b}=(b_1,\dots,b_d)$). For every $\underline{b}$ and $\underline{m}$ in $[1,N]^d$ there is exactly one vector $\underline{a}$ in $[1,N]^d\setminus\left([1,N]^d-\underline{b}\right)$ from which one can reach $\underline{m}$ with an arithmetic progression with a difference of $\underline{b}$. If $\underline{a},\underline{b}\in[1,N]^d$ and $s\geq 0$ is fixed, and there exists an elementary arithmetic progression $\mathrm{AP}(\underline{a},\underline{b},i2^s,(i+1)\,2^s-1)\subseteq[1,N]^d$ (with $i\geq 0$) then $\underline{a}+(2^s-1)\,\underline{b}\in[1,N]^d$ must hold. (Of course if the previous condition holds then there is at most one $i\geq 0$ for which $\underline{m}\in\mathrm{AP}(\underline{a},\underline{b},i2^s,(i+1)\,2^s-1)$.) It is also easy to see that if $\underline{a},\underline{b}\in[1,N]^d$ are fixed then there are at most $\log_2\left(\frac{N}{k\max\limits_{1\leq j\leq d}|b_j|}\right)$ possible values of s with $2^s\geq k+1$ and $\underline{a}+(2^s-1)\,\underline{b}\in[1,N]^d$. Using the notation $\|b\|_d=\max\limits_{1\leq j\leq d}|b_j|$ our results can be summarized in the following inequality:

$$\deg\left(\{A\in\mathcal{H}_N : |A|\geq k+1\}\right)\leq\sum_{\|b\|_d\leq\frac{N}{k}}\log_2\left(\frac{N}{k\,\|b\|_d}\right).$$

If $z\geq 1$ is a fixed integer then

$$\left|\left\{\|\underline{m}\|_d=z:\underline{m}\in\mathbb{Z}^d\right\}\right|=\left|[-z,z]^d\setminus[-(z-1),z-1]^d\right|=(2z+1)^d-(2z-1)^d,$$

where $[-x,x]=\{-x\leq n\leq x : n\in mathbbZ\}$. Thus

$$\sum_{\|b\|_d\leq\frac{N}{k}}\log_2\left(\frac{N}{k\,\|b\|_d}\right)=\sum_{1\leq z\leq\frac{N}{k}}\left((2z+1)^d-(2z-1)^d\right)\log_2\left(\frac{N}{kz}\right).$$

With the notation $f(z)=(2z-1)^d$ we have

$$\begin{aligned}\sum_{1\leq z\leq\frac{N}{k}}\left((2z+1)^d-(2z-1)^d\right)\log_2\left(\frac{N}{kz}\right) &= \int_1^{\left\lfloor\frac{N}{k}\right\rfloor+1}\log_2\left(\frac{N}{k\lfloor z\rfloor}\right)df(z)\\ &= \left(3^d-1\right)\log_2\left(\frac{N}{k}\right)+\int_2^{\left\lfloor\frac{N}{k}\right\rfloor+1}\log_2\left(\frac{N}{k\lfloor z\rfloor}\right)df(z).\end{aligned}$$

The function $f(z)$ is increasing and $\log_2\left(\frac{N}{k\lfloor z\rfloor}\right)\leq\log_2\left(\frac{N}{k(z-1)}\right)$ if $z>1$ therefore

$$\left(3^d-1\right)\log_2\left(\frac{N}{k}\right)+\int_2^{\left\lfloor\frac{N}{k}\right\rfloor+1}\log_2\left(\frac{N}{k\lfloor z\rfloor}\right)df(z)\leq\left(3^d-1\right)\log_2\left(\frac{N}{k}\right)+\int_1^{\left\lfloor\frac{N}{k}\right\rfloor}\log_2\left(\frac{N}{kz}\right)df(z).$$

Using

$$\int \log_2\left(\frac{u}{z}\right) df\left(z\right) = z^d\left(\log_2\left(\frac{u}{z}\right) + \frac{1}{d\log 2}\right),$$

one can easily show that there is a constant c_1 (with a value depending only on d) with

$$\deg\left(\{A \in \mathcal{H}_N : |A| \geq k+1\}\right) \leq \sum_{1 \leq z \leq \frac{N}{k}} \left((2z+1)^d - (2z-1)^d\right)\log_2\left(\frac{N}{kz}\right) \leq c_1\left(\frac{N}{k+1}\right)^d.$$

Thus if we set $t = (c_1 N)^{\frac{d}{d+1}}$ we can apply Theorem 3.2 to $\mathcal{H}_N$:

$$\operatorname{disc}\left(\mathcal{H}_N\right) \leq c_0\sqrt{t}\sqrt{\left(\log|\mathcal{H}_N|\right)\log|S\left(\mathcal{H}_N\right)|}.$$

If $\mathrm{AP}(\underline{a}, \underline{b}, i2^s, (i+1)\,2^s - 1) \subseteq [1, N]^d$ is elementary then for every $1 \leq j \leq d$ we have $b_j = 0$ or $\mathrm{AP}(a_j, b_j, i2^s, (i+1)\,2^s - 1) \subseteq [1, N]$ is an elementary arithmetic progression in one dimension. An easy meditation shows that the number of such arithmetic progressions is at most $2N^2$ thus

$$|\mathcal{H}_N| \leq c_2 N^{2d}$$

with a suitable constant c_2. Since $|S\left(\mathcal{H}_N\right)| = N^d$ therefore combining the previous inequalities we get

$$\operatorname{disc}\left(\mathcal{H}_N\right) \leq cN^{\frac{d}{2d+2}}\left(\log N\right)^{\frac{3}{2}}$$

where the constant only depends on d.
Clearly any arithmetic progression contained in $[1, N]^d$ is representable in the form of

$$\mathrm{AP}\left(\underline{a}, \underline{b}, 0, p_1\right) \setminus \mathrm{AP}\left(\underline{a}, \underline{b}, 0, p_1\right)$$

where $\underline{a} \in [1, N]^d \setminus \left([1, N]^d - \underline{b}\right)$ and both arithmetic progressions are contained in $[1, N]^d$. If the binary representation of $p_i + 1$ is

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

then

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

and $l_i \leq \log_2\left(p_i + 1\right) \leq \log_2 N$. Thus both $\mathrm{AP}(b, d, 0, p_i)$, $i = 1, 2$, are unions of at most $\log_2 N$ disjoint elementary arithmetic progressions, i.e. disjoint members of $\mathcal{H}_N$. By the previous arguments it is clear that

$$\operatorname{disc}\left(\mathcal{H}\right) \leq \left(2\log_2 N\right)\ \operatorname{disc}\left(\mathcal{H}_N\right)$$

and from this Theorem 3.1 follows. $\square$

4. Discrepancy of random hypergraphs

In [3] Knieper examined the discrepancy of all lines on the lattice points of $[1, N]^2$. Now our hypergraph is

$$\mathcal{H}_L = \left\{ \mathrm{AP}\left(\underline{a}, \underline{b}, 0, k\right) \subseteq [1, N]^2 : \underline{b} = (b_1, b_2) \neq \underline{0} \text{ and } \gcd\left(b_1, b_2\right) = 1 \right\},$$

and we need to estimate disc$(\mathcal{H}_L)$. Knieper proved that

$$\operatorname{disc}\left(\mathcal{H}_L\right) \leq c\sqrt{N \log N}$$

and she gives the result

$$\operatorname{disc}\left(\mathcal{H}_L\right) \geq c_1 \sqrt[4]{N}$$

without proof. It is easy to see that from Theorem 3.1 we get a stronger upper bound for disc$(\mathcal{H}_L)$. Since $\mathcal{H}_L \subseteq \mathcal{H}$ where $\mathcal{H}$ is the family of all arithmetic progressions on $[1, N]^2$ we have

$$\operatorname{disc}\left(\mathcal{H}_L\right) \leq \operatorname{disc}\left(\mathcal{H}\right).$$

Theorem 3.1 gives the inequality

$$\operatorname{disc}\left(\mathcal{H}\right) \leq c\sqrt[3]{N}\left(\log N\right)^{\frac{5}{2}}$$

and this also provides an upper bound for disc$(\mathcal{H}_L)$. The truth may be "around" $\sqrt[3]{N}$ and our next theorem will give some reason why this conjecture might be valid. It is known that the set $\{(b_1, b_2) : \gcd(b_1, b_2) = 1\}$ has an asymptotically uniform distribution with density $\frac{6}{\pi^2}$. Thus $\mathcal{H}_L$ is the set of all arithmetic progressions contained in $[1, N]^2$ with the possible differences taken from a subset of $\mathbb{Z}^2$ with "uniform" density.

The following theorem shows that if we consider a random subset of the family of arithmetic progressions in a way that we choose the possible differences independently with uniform probability then this random hypergraph has "almost" the same discrepancy as the original one with probability close to 1.

Theorem 4.1. *Let $d \geq 1$ and $0 < p < 1$ be fixed. Denote $\mathcal{A}_0 = \{-N, \ldots, N\}^d \setminus \{\underline{0}\}$ and for every $\underline{b} \in \mathcal{A}_0$ let $Z_{\underline{b}}$ be an independent random variable with*

$$\mathbf{P}\left(Z_{\underline{b}} = 1\right) = 1 - \mathbf{P}\left(Z_{\underline{b}} = 0\right) = p.$$

Consider the random set $\mathcal{A}_p = \left\{\underline{b} \in \mathcal{A}_0 : Z_{\underline{b}} = 1\right\}$ and let $\mathcal{H}_p$ be the family of all arithmetic progressions contained in $[1, N]^d$ with difference belonging to $\mathcal{A}_p$. Then there exists a constant $c_{d,\varepsilon}$ for every $\varepsilon > 0$ with

$$\mathbf{P}\left(\mathit{disc}\left(\mathcal{H}_p\right) \geq c_{d,\varepsilon} \frac{N^{\frac{d}{2d+2}}}{\log N} \right) \geq 1 - \frac{1}{\left(2N\right)^{\varepsilon}}.$$

Some elements of the proof are similar to that of Theorem 2.1 thus some details will be left to the reader. First we need the following lemma.

Lemma 4.2. *Let $\mathcal{A}_p$ be the random set defined in Theorem 4.1 and Q, Q_1 be positive integers satisfying $Q^d \geq 2Q_1 K \log(2N)$ and $N \geq QQ_1$ where $K = \frac{d+\varepsilon}{-\log(1-p)} + 1$.*

Denote $\mathcal{A}^* = \{\underline{b} \in \mathcal{A}_p : \|\underline{b}\|_d \le Q\}$ *and* $\mathcal{B}(\underline{b}) = \bigcup_{k=0}^{Q_1-1} \left([1,N]^d - k \cdot \underline{b}\right)$. *Then*

$$\mathbf{P}\left(\sum_{\underline{b}\in\mathcal{A}^*}\sum_{\underline{a}\in\mathcal{B}(\underline{b})}\left|\sum_{k=0}^{Q_1-1} c_{\underline{a}+k\cdot\underline{b}}\right|^2 \ge \left(\frac{2}{\pi}Q_1\right)^2 \sum_{\underline{a}\in[1,N]^d}\left|c_{\underline{a}}\right|^2 \textit{ for every } \left\{c_{\underline{a}} : \underline{a}\in[1,N]^d\right\}\right) \ge 1 - \frac{1}{(2N)^{\varepsilon}}.$$

(Where $c_{\underline{a}} = 0$ *if* $\underline{a} \notin [1,N]^d$ *.)*

From this the proof of the theorem follows.

Proof of Theorem 4.1. Let f be an arbitrary coloring of $[1,N]^d$ and let $c_{\underline{a}} = f(\underline{a})$ (with $c_{\underline{a}} = 0$ if $\underline{a} \notin [1,N]^d$). If

$$\sum_{\underline{b}\in\mathcal{A}^*}\sum_{\underline{a}\in\mathcal{B}(\underline{b})}\left|\sum_{k=0}^{Q_1-1} c_{\underline{a}+k\cdot\underline{b}}\right|^2 \ge \left(\frac{2}{\pi}Q_1\right)^2 \sum_{\underline{a}\in[1,N]^d}\left|c_{\underline{a}}\right|^2 = \left(\frac{2}{\pi}Q_1\right)^2 N^d$$

then using the enumeration method seen in the proof of Theorem 2.1 we can prove that there exist vectors $\underline{a}, \underline{b}$ with

$$\left|\sum_{k=0}^{Q_1-1} c_{\underline{a}+k\cdot\underline{b}}\right| \ge c_1(d)\sqrt{\frac{Q_1^2 N^d}{Q^d N^d + Q_1 Q^{d+1} N^{d-1}}}.$$

With $Q = \left\lfloor N^{\frac{1}{d+1}} \right\rfloor$, $Q_1 = \left\lfloor \frac{Q^d}{2K\log(2N)} \right\rfloor$ and applying the lemma Theorem 4.1 follows for large enough N (from this we can get the theorem for every N easily). $\square$

Proof of Lemma 4.2. First let $\left\{c_{\underline{a}} : \underline{a}\in[1,N]^d\right\}$ be a fixed set (with $c_{\underline{a}} = 0$ if $\underline{a} \notin [1,N]^d$). For $\underline{\alpha} \in [0,1]^d$ denote $S(\underline{\alpha}) = \sum_{\underline{a}\in[1,N]^d} c_{\underline{a}} \cdot e(\langle\underline{a},\underline{\alpha}\rangle)$ and $F(x) = \sum_{k=0}^{Q_1-1} e(kx)$ for $x \in [0,1]$. Set $\mathcal{D}(N) = \left\{\frac{1}{2N}\cdot\underline{a} : \underline{a}\in[1,N]^d\right\}$ and

$$J = \frac{1}{(2N)^d}\sum_{\underline{\alpha}\in\mathcal{D}(N)} |S(\underline{\alpha})|^2 \sum_{\underline{b}\in\mathcal{A}^*} |F(\langle\underline{b},\underline{\alpha}\rangle)|^2 .$$

Using the discrete version of Parseval's formula we can show that

$$\frac{1}{(2N)^d}\sum_{\underline{\alpha}\in\mathcal{D}(N)} |S(\underline{\alpha})|^2 |F(\langle\underline{b},\underline{\alpha}\rangle)|^2 = \sum_{\underline{a}\in\mathcal{B}(\underline{b})}\left|\sum_{k=0}^{Q_1-1} c_{\underline{a}+k\cdot\underline{b}}\right|^2 .$$

(We only have to duplicate the corresponding steps of the proof of Theorem 2.1 and observe that because of the conditions $N \ge QQ_1$ and $c_{\underline{a}} = 0$ if $\underline{a} \notin [1,N]^d$ we indeed get the same result.) Thus

$$J = \sum_{\underline{b}\in\mathcal{A}^*}\sum_{\underline{a}\in\mathcal{B}(\underline{b})}\left|\sum_{k=0}^{Q_1-1} c_{\underline{a}+k\cdot\underline{b}}\right|^2 .$$

Clearly

$$J \ge \min_{\underline{\alpha}\in\mathcal{D}(N)} \sum_{\underline{b}\in\mathcal{A}^*} |F(\langle\underline{b},\underline{\alpha}\rangle)|^2 \frac{1}{(2N)^d}\sum_{\underline{\alpha}\in\mathcal{D}(N)} |S(\underline{\alpha})|^2 = \min_{\underline{\alpha}\in\mathcal{D}(N)} \sum_{\underline{b}\in\mathcal{A}^*} |F(\langle\underline{b},\underline{\alpha}\rangle)|^2 \sum_{\underline{a}\in[1,N]^d}\left|c_{\underline{a}}\right|^2 .$$

Therefore if we verify that

$$\mathbf{P}\left(\min_{\underline{\alpha}\in\mathcal{D}(N)}\sum_{\underline{b}\in\mathcal{A}^*}\left|F\left(\langle\underline{b},\underline{\alpha}\rangle\right)\right|^2 \geq \left(\frac{2}{\pi}Q_1\right)^2\right) \geq 1-\frac{1}{(2N)^{\varepsilon}}$$

then the lemma follows, too. We will show that for every $\underline{\alpha}\in\mathcal{D}(N)$

$$\mathbf{P}\left(\sum_{\underline{b}\in\mathcal{A}^*}\left|F\left(\langle\underline{b},\underline{\alpha}\rangle\right)\right|^2 \geq \left(\frac{2}{\pi}Q_1\right)^2\right) \geq 1-\frac{1}{(2N)^{d+\varepsilon}}$$

and because $|\mathcal{D}(N)|=(2N)^d$ this will prove the needed inequality.

Set $\mathcal{A}=\left\{\underline{b}\in\mathbb{Z}^d : 0<\|\underline{b}\|_d\leq Q\right\}$ and $E_{\underline{\alpha}}=\left\{\underline{b}\in\mathcal{A} : \|\langle\underline{b},\underline{\alpha}\rangle\|\leq\frac{1}{2Q_1}\right\}$. Using the proof of Dirichlet's Theorem on simultaneous approximation (or simply the pigeonhole-principle) one can show that

$$\left|E_{\underline{\alpha}}\right| \geq \left\lceil\frac{Q^d}{2Q_1}\right\rceil-1.$$

We have already seen that if $E_{\underline{\alpha}}$ is not empty then

$$\sum_{\underline{b}\in\mathcal{A}^*}\left|F\left(\langle\underline{b},\underline{\alpha}\rangle\right)\right|^2 \geq \left(\frac{2}{\pi}Q_1\right)^2,$$

hence

$$\mathbf{P}\left(\exists\underline{b}\in E_{\underline{\alpha}} \text{ with } Z_{\underline{b}}=1\right) \leq \mathbf{P}\left(\sum_{\underline{b}\in\mathcal{A}^*}\left|F\left(\langle\underline{b},\underline{\alpha}\rangle\right)\right|^2 \geq \left(\frac{2}{\pi}Q_1\right)^2\right).$$

Since the random variables $Z_{\underline{b}}$ are independent and $\mathbf{P}\left(Z_{\underline{b}}\neq 1\right)=1-p$ we have

$$\mathbf{P}\left(\exists\underline{b}\in E_{\underline{\alpha}} \text{ with } Z_{\underline{b}}=1\right)=1-(1-p)^{\left|E_{\underline{\alpha}}\right|} \geq 1-(1-p)^{\left\lceil\frac{Q^d}{2Q_1}\right\rceil-1}.$$

But

$$\left\lceil\frac{Q^d}{2Q_1}\right\rceil-1 \geq \log(2N)\,\frac{d+\varepsilon}{-\log(1-p)}$$

therefore

$$\mathbf{P}\left(\exists\underline{b}\in E_{\underline{\alpha}} \text{ with } Z_{\underline{b}}=1\right) \geq 1-\frac{1}{(2N)^{d+\varepsilon}}$$

and from that the lemma follows. □

References

1. J. Beck, *Roth's estimate of the discrepancy of integer sequences is nearly sharp*, Combinatorica **1** (1981), 319–325.
2. P. Erdős and A. Sárközy, *Some solved and unsolved problems in combinatorial number theory*, Math. Slovaca **28** (1978), 407–421.
3. P. Knieper, *Discrepancy of arithmetic progressions*, Ph.D. thesis, Institute für Informatic, Humboldt-Universität zu Berlin, 1997.
4. K. F. Roth, *Remark concerning integer sequences*, Acta Arithmetica **IX** (1964), 257–260.
5. J. Matoušek and J. Spencer, *Discrepancy in arithmetic progressions*, J. Amer. Math. Soc. **9** (1996), 195–204.

E-mail address: `valko@cs.elte.hu`