Discrepancy of Sums of Three Arithmetic Progressions

Aleš Přívětivý *

Department of Applied Mathematics of Charles University
Malostranské nám. 25, 11800 Praha, Czech Republic
privetivy@kam.mff.cuni.cz

Submitted: Jul 24, 2005; Accepted: Dec 5, 2005; Published: Jan 25, 2006
Mathematics Subject Classification: 11K38

Abstract

The set system of all arithmetic progressions on $[n]$ is known to have a discrepancy of order $n^{1/4}$. We investigate the discrepancy for the set system $\mathcal{S}_n^3$ formed by all sums of three arithmetic progressions on $[n]$ and show that the discrepancy of $\mathcal{S}_n^3$ is bounded below by $\Omega(n^{1/2})$. Thus $\mathcal{S}_n^3$ is one of the few explicit examples of systems with polynomially many sets and a discrepancy this high.

1 Introduction

Let $(X, \mathcal{F})$ be a set system on a finite set. The discrepancy problem is to color each point of X either red or blue, in such a way that any of the sets of $\mathcal{F}$ has roughly the same number of red points and blue points. The maximum deviation from an even splitting, over all sets of $\mathcal{F}$, is the discrepancy of $\mathcal{F}$, denoted by $\mathrm{disc}(\mathcal{F})$. Formally

$$\mathrm{disc}(\mathcal{F}) = \min_{\chi: X \to \{-1,1\}} \max_{S \in \mathcal{F}} \Big| \sum_{x \in S} \chi(x) \Big|.$$

For further information see Beck and Sós [BS95], Chazelle [Cha00], and Matoušek [Mat99].

Let n be a positive integer and let $[n]$ denote the set $\{0, 1, \ldots, n-1\}$. For any $a \in \mathbf{Z}$ and $d_1, n_1 \in \mathbf{N}$ we define the arithmetic progression $AP(a, d_1, n_1)$ as the set $\{a + id_1 : i \in [n_1]\}$. The set system formed by all arithmetic progressions on $[n]$ we denote by $([n], \mathcal{S}_n)$ where $\mathcal{S}_n = \{AP(a, d_1, n_1) \cap [n] : a, d_1, n_1 \in \mathbf{N}\}$.

The lower bound $\Omega(n^{1/4})$ on the discrepancy of arithmetic progressions $\mathcal{S}_n$ proved by Roth [Rot64] was one of the early results in combinatorial discrepancy. In 1974, Sárközy (see [ES74]) established an $O(n^{1/3+\epsilon})$ upper bound. This was improved by Beck [Bec81],

*Supported by Czech Science Foundation grant 201/05/H014.

who obtained the near-tight upper bound of $O(n^{1/4}\log^{5/2} n)$, inventing the powerful partial coloring method for that purpose. The asymptotically tight upper bound $O(n^{1/4})$ was finally proved by Matoušek and Spencer [MS96].

Discrepancies of related set systems were also studied. One possible extension of the original problem is to consider set systems formed by sums of arithmetic progressions, where a sum of k arithmetic progressions $AP_k(a, d_1, \ldots, d_k, n_1, \ldots, n_k)$ is defined for $a \in \mathbf{Z}$ and $d_1, \ldots, d_k, n_1, \ldots, n_k \in \mathbf{N}$ as the set $\{a + i_1d_1 + \ldots + i_kd_k : i_l \in [n_l], l = 1, \ldots, k\}$. The corresponding set system of all sums of k arithmetic progressions on $[n]$ is then $([n], \mathcal{S}_n^k)$, where $\mathcal{S}_n^k = \{AP_k(a, d_1, \ldots, d_k, n_1, \ldots, n_k) \cap [n] : a \in \mathbf{Z}; d_1, \ldots, d_k, n_1, \ldots, n_k \in \mathbf{N}\}$. Hebbinghaus [Heb04] proved that $\mathrm{disc}(\mathcal{S}_n^k) = \Omega(n^{\frac{k}{2k+2}})$. Here we show that for $k \geq 3$, $\mathrm{disc}(\mathcal{S}_n^k) = \Omega(n^{1/2})$. Thus $\mathcal{S}_n^3$ is one of the few explicit examples of systems with polynomially many sets and a discrepancy this high.

For a fixed $k \geq 3$, the lower bound on $\mathcal{S}_n^k$ is nearly tight since the random coloring lemma [AS92] provides the upper bound $O(n^{1/2}\log^{1/2} n)$. In the case $k = 2$, there is still a considerable gap, $\Omega(n^{1/3})$ versus $O(n^{1/2}\log^{1/2} n)$, and estimating the correct bound remains still open.

We start in Section 2 with recalling the eigenvalue bound method and then we show how it can be used for wrapped set systems. In Section 3 we discuss how to construct suitable wrapped set systems and illustrate this approach on the system of arithmetic progressions on $[n]$ (this version of proof is attributed to Lovász). Then we construct a wrapped set system for our main result.

2 Preliminaries

In this section we recall some basic facts. We start with some definitions from discrepancy theory; for more definitions see [Mat99].

Let $(X, \mathcal{F})$ be a set system on a finite set. Let us enumerate the elements of X as $x_1, x_2, \ldots, x_n$ and the sets of $\mathcal{F}$ as $S_1, S_2, \ldots, S_m$ in some arbitrary order. The incidence matrix of $(X, \mathcal{F})$ is the $m \times n$ matrix A, with columns corresponding to points of X and rows corresponding to sets of $\mathcal{F}$, whose element a_{ij} is given by

$$a_{ij} = \begin{cases} 1 & \text{if } j \in S_i \\ 0 & \text{otherwise.} \end{cases}$$

As we will see, it is useful to reformulate the definition of the discrepancy of $\mathcal{F}$ in terms of the incidence matrix. Now let us regard a coloring $\chi : X \to \{-1, +1\}$ as the column vector $(\chi(x_1), \chi(x_2), \ldots, \chi(x_n))^T \in \mathbf{R}^n$. Then the product $A\chi$ is the row vector $(\chi(S_1), \chi(S_2), \ldots, \chi(S_n)) \in \mathbf{R}^m$, where we extend the coloring χ for sets as $\chi(S) = \sum_{x \in S} \chi(x)$. Therefore, the definition of the discrepancy of $\mathcal{F}$ can be written as

$$\mathrm{disc}(\mathcal{F}) = \min_{x \in \{-1,1\}^n} \|Ax\|_\infty .$$

For many lower bound techniques, it is easier to consider the L_2-discrepancy instead of the worst-case discrepancy. In our case, this means replacing the max-norm $\|.\|_\infty$ by the usual Euclidean norm $\|.\|$. Namely, we have

$$\operatorname{disc}(\mathcal{F}) \geq \operatorname{disc}_2(\mathcal{F}) = \min_\chi \left(\frac{1}{m} \sum_{i=1}^{m} \chi(S_i)^2 \right)^{1/2} = \frac{1}{\sqrt{m}} \cdot \min_{x \in \{-1,1\}^n} \|Ax\|.$$

To obtain a lower bound on the L_2-discrepancy for a set system, we can use the following eigenvalue lower bound:

Theorem 2.1 (Eigenvalue bound, see [BS95]) *Let $(X, \mathcal{F})$ be a system of m sets on an n-point set, and let A denote its incidence matrix. Then we have*

$$\operatorname{disc}(\mathcal{F}) \geq \operatorname{disc}_2(\mathcal{F}) \geq \sqrt{\frac{n}{m} \cdot \lambda_{\min}},$$

where $\lambda_{\min}$ denotes the smallest eigenvalue of the $n \times n$ matrix $A^T A$.

The computation of eigenvalues becomes much easier when the matrix $A^T A$ is a circulant matrix. A *circulant* matrix is an $n \times n$ matrix whose rows are composed of cyclically shifted copies of the first row. Namely, for an n-dimensional vector $(a_0, a_1, \ldots, a_{n-1})$ we define the $n \times n$ circulant matrix $C(a_0, a_1, \ldots, a_{n-1})$ by putting $c_{ij} = a_{(j-i) \bmod n}$, i.e.

$$C(a_0, a_1, \ldots, a_{n-1}) = \begin{pmatrix} a_0 & a_1 & a_2 & \ldots & a_{n-1} \\ a_1 & a_2 & a_3 & \ldots & a_0 \\ a_2 & a_3 & a_4 & \ldots & a_1 \\ . & . & . & . & . \\ a_{n-1} & a_0 & a_1 & \ldots & a_{n-2} \end{pmatrix}.$$

Let $\zeta_0, \zeta_1, \ldots, \zeta_{n-1}$ denote the *n-th roots of the unity*, which are defined as roots of the cyclotomic equation $x^n = 1$. All the roots lie on the unit circle and we can order them according to the sequence of visiting them if we go around the unit circle counterclockwise starting at 0, namely we put $\zeta_k = e^{\frac{2\pi i}{n} k}$. This simplifies the following operations:

- $\zeta_j \zeta_k = \zeta_{(j+k) \bmod n}$
- $\zeta_j^k = \zeta_{(jk) \bmod n}$

For convenience, we will consider all operations $+, .$ on indices reduced modulo n and thus we will later omit the $\bmod n$ suffix.

We define the complex argument as usual by $\arg(x + iy) = \arctan(\frac{y}{x})$ and restrict its range to the interval $(-\pi, +\pi]$. The complex argument of the n-th root of unity is then as follows

$$\arg(\zeta_k) = \begin{cases} \frac{2\pi k}{n} & \text{if } 0 \leq k \leq \frac{n}{2} \\ \frac{2\pi(k-n)}{n} & \text{if } \frac{n}{2} < k < n. \end{cases}$$

Let B be a circulant matrix $C(a_0, a_1, \dots, a_{n-1})$. It can be easily verified that $z_i = (1, \zeta_i^1, \zeta_i^2, \dots, \zeta_i^{n-1})^T$ is an eigenvector of B and thus the eigenvalues $\lambda_0, \lambda_1, \dots, \lambda_{n-1}$ of B are

$$\lambda_i = a_0 + a_1\zeta_i + a_2\zeta_i^2 + \ldots + a_{n-1}\zeta_i^{n-1}.$$

Let A be an incidence matrix for the set system $(X, \mathcal{F})$ and let B denote $A^T A$. Then the element b_{ij} counts the number of sets $S_i \in \mathcal{F}$ containing both elements x_i and x_j. Moreover, if the matrix B is a circulant matrix $C(a_0, a_1, \dots, a_{n-1})$, we can derive a more useful expression for the eigenvalues of B:

$$\begin{aligned} n\lambda_k &= n\sum_{i=0}^{n-1} a_i\zeta_k^i = \sum_{i=0}^{n-1}\sum_{j=0}^{n-1} a_{(i-j) \bmod n}\zeta_k^{(i-j) \bmod n} = \sum_{i=0}^{n-1}\sum_{j=0}^{n-1} b_{ij}\zeta_k^{(i-j)} = \\ &= \sum_{S\in\mathcal{F}}\sum_{x_i\in S}\sum_{x_j\in S}\zeta_k^{(i-j)} = \sum_{S\in\mathcal{F}}\Big|\sum_{x_i\in S}\zeta_k^i\Big|^2. \end{aligned}$$

And thus

$$\lambda_k = \frac{1}{n}\sum_{S\in\mathcal{F}}\Big|\sum_{x_i\in S}\zeta_k^i\Big|^2.$$

Let $(X, \mathcal{F})$ be a set system, where $X = [n]$ and $\mathcal{F}$ contains exactly mn sets enumerated as $\mathcal{F} = \{S_0, S_1, \dots, S_{mn-1}\}$. We say that a set system $(X, \mathcal{F})$ is *wrapped* if for every $i \in [m]$ and $j \in [n]$ the set S_{in+j} is the set S_{in} cyclically translated by j, i.e.

$$S_{in+j} = \{(k + j) \bmod n : k \in S_i\}.$$

The incidence matrix A of a wrapped set system $(X, \mathcal{F})$ is composed of m square $n\times n$ circulant matrices $A_0, A_1, \dots, A_{m-1}$ stacked up vertically, one on top of the other:

$$A = \begin{pmatrix} A_0 \\ A_1 \\ \vdots \\ A_{m-1} \end{pmatrix}.$$

By the definition of a wrapped set system every A_i is a circulant and thus every $A_i^T A_i$ is a circulant too. Note that although A is not a circulant itself, the matrix $B = A^T A$ is equal to $\sum_{i=0}^{m-1} A_i^T A_i$ and therefore B is a circulant.

Alternatively, we can observe that the (i, j) entry of $A^T A$ is the number of sets from $\mathcal{F}$ that contain both elements i and j. Since the sets forming $\mathcal{F}$ are invariant under cyclic shifts, the entries (i, j) and $(i + k, j + k)$ of $A^T A$ are the same for an arbitrary shift by k and thus $A^T A$ is a circulant.

Lemma 2.2 *Let $(X, \mathcal{F})$ be a wrapped set system, where $|X| = n$ and $|\mathcal{F}| = mn$, and let A be its incidence matrix. Then the $n \times n$ matrix $B = A^T A$ is a circulant and its eigenvalues are*

$$\lambda_k = \sum_{i=0}^{m-1} \Big| \sum_{j \in S_{in}} \zeta_k^j \Big|^2.$$

Proof. Since for each set S_{in}, we have its $n-1$ translates in $\mathcal{F}$ that give the same contribution, we may just count n-times the contribution of the set S_{in} and thus

$$\lambda_j = \frac{1}{n} \sum_{S \in \mathcal{F}} \Big| \sum_{k \in S} \zeta_j^k \Big|^2 = \sum_{i=0}^{m-1} \Big| \sum_{k \in S_{in}} \zeta_j^k \Big|^2.$$

□

3 Lower bounds

In this section we will prove the lower bound for the sums of three arithmetic progressions. For this purpose we will use following lemma:

Lemma 3.1 *Let $([n], \mathcal{F})$ be a wrapped set system, where $|\mathcal{F}| = mn$, and let $\zeta_0, \zeta_1, \ldots, \zeta_{n-1}$ be the n-th roots of unity. If there are real constants $c, \alpha > 0$ such that for each $j \in [n]$ there is $S_{in} \in \mathcal{F}$ such that*

$$\Big| \sum_{k \in S_{in}} \zeta_j^k \Big| \geq cn^\alpha$$

holds, then $\mathrm{disc}(\mathcal{F}) \geq \frac{cn^\alpha}{\sqrt{m}}$.

Proof. To invoke the eigenvalue bound for an L_2-discrepancy we need to lowerbound the value of smallest eigenvalue $\lambda_{\min}$. Since our set system is wrapped, we know that all eigenvalues are given by the expression

$$\lambda_j = \sum_{i=0}^{m-1} \Big| \sum_{k \in S_{in}} \zeta_j^k \Big|^2.$$

We know that for each j there is a set S_{in} that makes the eigenvalue 'large' and hence for every eigenvalue we know that

$$\lambda_j = \sum_{i=0}^{m-1} \Big| \sum_{k \in S_{in}} \zeta_j^k \Big|^2 \geq \Big| \sum_{k \in S_{in}} \zeta_j^k \Big|^2 \geq c^2 n^{2\alpha}.$$

Thus

$$\mathrm{disc}(\mathcal{F}) \geq \mathrm{disc}_2(\mathcal{F}) \geq \sqrt{\frac{n}{mn} c^2 n^{2\alpha}} = \frac{cn^\alpha}{\sqrt{m}}.$$

□

If we want to obtain a good lower bound from Lemma 3.1, the number of sets forming $\mathcal{F}$ has to be small and $\mathcal{F}$ has to contain for each $j \in [n]$ a set B_j, such that $\left|\sum_{k\in B_j} \zeta_j^k\right|$ is large. Our goal is to ensure that for each $j \in [n]$ there is a $B_j \in \mathcal{F}$ such that all ζ_j^k for $k \in B_j$ are concentrated in one part of the unit circle. Namely, if all $k \in B_j$ satisfy

$$-\frac{\pi}{3} \leq \arg\ \zeta_j^k\ \leq \frac{\pi}{3},$$

then Re $\zeta_j^k \geq \frac{1}{2}$ for all $k \in B_j$, and the value of $\left|\sum_{k\in B_j} \zeta_j^k\right|$ will be at least $|B_j|/2$.

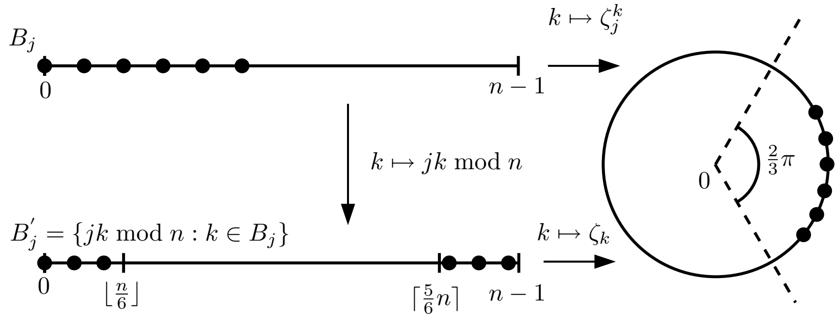

Figure 1: The relation of the set $B_j^{'}$ and the sum $\sum_{k\in B_j} \zeta_j^k$

For convenience, we define for every $B_j \subseteq [n]$ a set $B_j^{'}$ as the set $\{jk \mod n : k \in B_j\}$. The set $B_j^{'}$ is actually the set of indices i of $\zeta_i = \zeta_j^k$ that participate in the sum $\sum_{k\in B_j} \zeta_j^k$ (see figure 1). The condition $|\arg\ \zeta_k| \leq \frac{\pi}{3}$ for all $k \in B_j$ is thus equivalent to the condition

$$B_j^{'} \subseteq \left\{0, \dots, \left\lfloor \frac{1}{6} n \right\rfloor\right\} \cup \left\{\left\lceil \frac{5}{6} n \right\rceil, \dots, n-1\right\}.$$

Moreover, if n is a prime and $0 < j < n$, the mapping $k \mapsto jk \bmod n$ is a bijection and the cardinalities of B_j and $B_j^{'}$ are the same.

Now let us apply this method to prove the $\Omega(n^{1/4})$ lower bound for the set system of arithmetic progressions on $[n]$. For this purpose we construct a small auxiliary wrapped set system $\mathcal{F}$ that is suitable for Lemma 3.1 and disc$(\mathcal{S}_n)$ is asymptotically bounded below by disc$(\mathcal{F})$.

We will show, that for each $j \in [n]$ we can find a positive integer $d_j = O(\sqrt{n})$, such that $|\arg\ \zeta_j^{d_j}| = O(n^{-1/2})$. Let us take as B_j an arithmetic progression with difference d_j having $\Omega(\sqrt{n})$ elements, such that $|\arg\ \zeta_j^k| \leq \frac{\pi}{3}$ for all $k \in B_j$. For such a B_j, we get $\left|\sum_{k\in B_j} \zeta_j^k\right| = \Omega(\sqrt{n})$. Since there are only $O(\sqrt{n})$ possible choices of d_j, it suffices us to put only $O(\sqrt{n})$ different sets B_j into $\mathcal{F}$. With each inserted B_j, we also have to put into $\mathcal{F}$ its $n-1$ wrapped translates, and thus $\mathcal{F}$ has size $O(n^{3/2})$. The following theorem summarizes our discussion. This version of the proof of the lower bound for $\mathcal{S}_n$ was first suggested by Lovász and can be found in [BS95].

Theorem 3.2 *For any $n \in \mathbf{N}$ we put $k = \lfloor \sqrt{n/6} \rfloor$ and $m = 6k$. Let us consider the following set system $([n], \mathcal{F})$, where $\mathcal{F} = \{S_0, S_1, \ldots, S_{mn-1}\}$ and the sets S_{dn+j} for $d \in [m]$ and $j \in [n]$ are given as*

$$S_{dn+j} = \{(di + j) \bmod n : i \in [k]\}.$$

Then

$$\operatorname{disc}(\mathcal{F}) \geq cn^{1/4}.$$

Proof. For a fixed $j \in [n]$, there is by the Pigeonhole Principle a positive integer c_0, $1 \leq c_0 \leq m$ such that

$$-\frac{2\pi}{m} \leq \arg(\zeta_j^{c_0}) \leq \frac{2\pi}{m}.$$

Then $\operatorname{Re} \zeta_j^{ic_0} \geq 1/2$ for $0 \leq i \leq k-1$, and hence

$$\Big| \sum_{i \in S_{c_0 n}} \zeta_j^i \Big| \geq \Big(\operatorname{Re} \sum_{i \in S_{c_0 n}} \zeta_j^i \Big) \geq k/2.$$

From this and Lemma 3.1 it immediately follows that

$$\operatorname{disc}(\mathcal{F}) > \frac{1}{10} n^{1/4}.$$

□

Since every $S \in \mathcal{F}$ from theorem 3.2 is a disjoint union of two arithmetic progressions, we get the following corollary.

Corollary 3.3 *For $n \in \mathbf{N}$, let $([n], \mathcal{S}_n)$ be a set system formed by all arithmetic progressions on $[n]$. Then $\operatorname{disc}(\mathcal{S}_n) = \Omega(n^{1/4})$.*

For the set system $([n], \mathcal{S}_n)$ is the $\Omega(n^{1/4})$ lower bound tight. We would like to show that the set systems $([n], \mathcal{S}_n^k)$ for $k \geq 2$ have their discrepancy bounded below by $\Omega(n^{1/2})$. Unfortunately, we are able to prove this only for $k \geq 3$, while for $k = 2$ the currently known best lower bound is $\Omega(n^{1/3})$; see [Heb04].

As we have seen in the proof of Theorem 3.2, for each $j \in \{1, \ldots, n-1\}$ we can find two positive integers $0 < c_1 \leq \sqrt{n}$ and $0 < d_1 \leq \sqrt{n}$, such that $|\arg \zeta_j^{c_1}| = \frac{2\pi d_1}{n}$. Without loss of generality, let us assume that $\arg \zeta_j^{c_1}$ is positive and thus $d_1 = c_1 j \bmod n$, the other case can be handled in the same way. Let A_j be the set $\{ic_1 : i \in [n_1]\}$. If $n_1 \leq \min\{\frac{n}{c_1}, \frac{n}{6d_1}\}$, then A_j is an arithmetic progression on $[n]$ and $A_j^{'}$ is an arithmetic progression on $[\lfloor n/6 \rfloor]$ (see figure 2). Although is n_1 is at least $\Omega(\sqrt{n})$, we cannot generally expect a greater value.

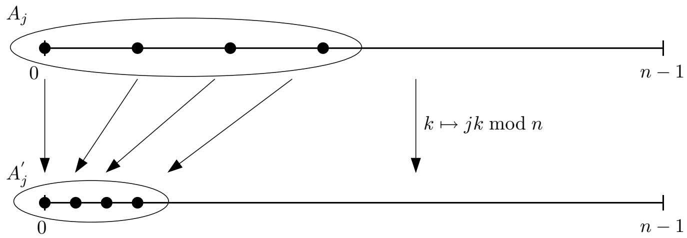

Figure 2: A_j with difference c_1 goes to A_j' with difference d_1

Our goal is to find a B_j such that B_j' covers a constant fraction of $\{0, \ldots, \lfloor \frac{1}{6}n \rfloor\} \cup \{\lceil \frac{5}{6}n \rceil, \ldots, n-1\}$. In next two steps we will schematically (and possibly misleadingly) show how to achieve this. In the first step we extend the arithmetic progression A_j' to a longer arithmetic progression B_j' with the same difference. This is done in such a way that B_j' consists of several copies of A_j' and thus B_j is taken as a sum of two arithmetic progressions (see figure 3). In this way we can have $\Omega(n/d_1)$ elements in B_j.

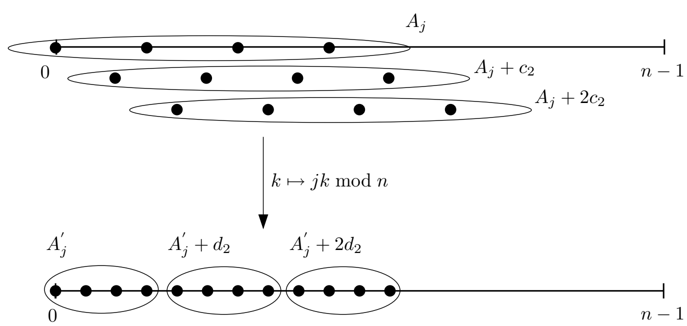

Figure 3: B_j (resp. B_j') composed from copies of A_j (resp. A_j')

In the last step we take a suitable sum of three arithmetic progressions for C_j such that C_j' is composed of $\Omega(d_1)$ interlaced copies of B_j' that are mutually disjoint (see figure 4), and thus C_j' has $\Omega(n)$ elements.

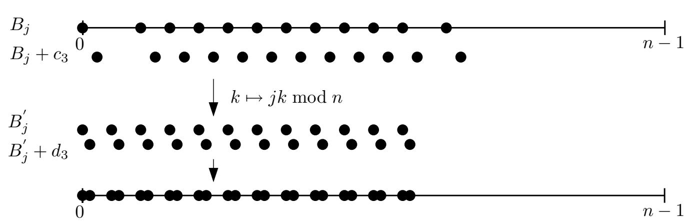

Figure 4: C_j' is composed from interlaced copies of B_j'

The following lemma provides, for each $j \in \{1, \ldots, n-1\}$, a precise and more careful construction of the set C_j. This construction requires n to be a prime.

Lemma 3.4 *Let n be a prime. For each $j \in \{1 \ldots n-1\}$ there exists a set C_j such that*

- *C_j is a sum of three arithmetic progressions on $[n]$*
- *$\operatorname{Re} \zeta_j^k \geq 1/2$ for every $k \in C_j$*
- *$|C_j| \geq \frac{1}{5000} n$.*

Proof. For a fixed j we find integer constants $c_1, c_2, c_3, d_1, d_2, d_3, n_1, n_2$ and n_3 as follows:

1. Let c_1 be the $k \in \{1 \ldots \lfloor \sqrt{n} \rfloor\}$ for which the value $\operatorname{Re} \zeta_j^k$ is maximum. We put $d_1 = \min\{jc_1 \mod n, -jc_1 \mod n\}$ and $n_1 = \lceil \frac{n}{12 \max\{c_1, d_1\}} \rceil$.
2. If $c_1 \leq 12 d_1$, then we put $c_2 = 1$, $d_2 = 1$ and $n_2 = 1$, otherwise we put $c_2 = n \mod c_1$, $d_2 = d_1 \lceil \frac{n}{c_1} \rceil$ and $n_2 = \lfloor \frac{c_1}{30 d_1} \rfloor$.
3. If $d_1 < 6$, then we put $c_3 = 1$, $d_3 = 1$ and $n_3 = 1$, otherwise we put c_3 to be the $k \in \{1 \ldots \lfloor \frac{2n}{d_1} \rfloor\}$ for which the value $\operatorname{Re} \zeta_j^k$ is maximum. We put $d_3 = \min\{jc_3 \mod n, -jc_3 \mod n\}$ and $n_3 = \lfloor \frac{d_1}{12} \rfloor$.
4. We put $C_j = \{i_1 c_1 + i_2 c_2 + i_3 c_3 : i_k \in [n_k], k = 1, 2, 3\}$.

We have chosen c_1 as the $k \in \{1 \ldots \lfloor \sqrt{n} \rfloor\}$ for which the value of $\operatorname{Re} \zeta_j^k$ is maximum, i.e. as the $k \in \{1 \ldots \lfloor \sqrt{n} \rfloor\}$ for which the value of $|\arg\ \zeta_j^k|$ is minimum. By the Pigeonhole Principle

$$-\frac{2\pi}{\lceil \sqrt{n} \rceil} \leq \arg\ \zeta_j^{c_1} \leq \frac{2\pi}{\lceil \sqrt{n} \rceil},$$

and since $|\arg \zeta_j^{c_1}| = \arg \zeta_{d_1} = \frac{2\pi d_1}{n}$, we conclude that $d_1 \leq \sqrt{n}$. Similarly we arrive at $c_3 \leq \frac{2n}{d_1}$ and $d_3 \leq \frac{d_1}{2}$.

Claim A: C_j is a sum of three arithmetic progressions on $[n]$.

By construction the set C_j is a sum of three arithmetic progressions. The largest element of C_j is bounded by

$$\begin{aligned} \max\ C_j &= c_1(n_1 - 1) + c_2(n_2 - 1) + c_3(n_3 - 1) \leq \\ &\leq \frac{n}{12} + \frac{n}{30} + \frac{n}{6} \leq \frac{n}{2}, \end{aligned}$$

and thus $C_j \subseteq [n]$.

Claim B: $\mathrm{Re}\,\zeta_j^k \geq 1/2$ for every $k \in C_j$.

We show that for every $k \in C_j$ the value of $|\arg\ \zeta_j^k|$ is less than $\pi/3$ and this already implies the claim.

$$\begin{aligned}
\max_{k\in C_j} |\arg\ \zeta_j^k| &= \max_{(i_1,i_2,i_3)\in[n_1]\times[n_2]\times[n_3]} |\arg\ \zeta_j^{c_1 i_1} + \arg\ \zeta_j^{c_2 i_2} + \arg\ \zeta_j^{c_3 i_3}| \leq \\
&\leq \max_{i_1\in[n_1]} |\arg\ \zeta_j^{c_1 i_1}| + \max_{i_2\in[n_2]} |\arg\ \zeta_j^{c_2 i_2}| + \max_{i_3\in[n_3]} |\arg\ \zeta_j^{c_3 i_3}| = \\
&= \frac{2\pi}{n}(d_1(n_1-1) + d_2(n_2-1) + d_3(n_3-1)).
\end{aligned}$$

In the case that $c_1 \leq 12 d_1$

$$\begin{aligned}
\max_{k\in C_j} |\arg\ \zeta_j^k| &= \frac{2\pi}{n}(d_1(n_1-1) + d_2(n_2-1) + d_3(n_3-1)) \leq \\
&\leq \frac{2\pi}{n}\left(d_1\frac{n}{12d_1} + d_2\cdot 0 + \frac{d_1}{2}\frac{d_1}{12}\right) \leq \frac{\pi}{3},
\end{aligned}$$

otherwise

$$\begin{aligned}
\max_{k\in C_j} |\arg\ \zeta_j^k| &= \frac{2\pi}{n}\left(d_1(n_1-1) + d_2(n_2-1) + d_3(n_3-1)\right) \leq \\
&\leq \frac{2\pi}{n}\left(d_1\frac{n}{144d_1} + d_1\left\lceil\frac{n}{c_1}\right\rceil\frac{c_1}{30d_1} + \frac{d_1}{2}\frac{d_1}{12}\right) \leq \frac{\pi}{3}.
\end{aligned}$$

Claim C: $|C_j| \geq \frac{1}{5000}n$.

We put $D = \{i_1 d_1 + i_2 d_2 : i_1 \in [n_1], i_2 \in [n_2]\}$. From the fact that $d_2 = d_1\lceil\frac{n}{c_1}\rceil$ and $d_2 > n_1 d_1$ we deduce that D is a subset of an arithmetic progression with difference d_1 and $|D| = n_1 n_2$.

The set $E = \{i_1 d_1 + i_2 d_2 + i_3 d_3 : i_1 \in [n_1], i_2 \in [n_2], i_3 \in [n_3]\}$ is a union of n_3 shifted copies of D. Our goal is to show that those n_3 shifted copies of D are mutually disjoint. If there were two intersecting copies of D, then there has to exist a $k \in \{1, \ldots, n_3\}$, such that $d_1 | k d_3$. Let it be so and let k, l be the integers demonstrating this case, i.e. $l d_1 = k d_3$. Since $d_1 > d_3$, we have $l < k$. Thus $l < n_3 \leq n_1$ and the preimage of $l d_1$ under the mapping $f_j(k) = jk \bmod n$ is $f_j^{-1}(l d_1) = l c_1$ and similarly $f_j^{-1}(k d_3) = k c_3$. The mapping f_j is a bijection and therefore $l d_1 = k d_3$ implies $l c_1 = f_j^{-1}(l d_1) = f_j^{-1}(k d_3) = k c_3$. But since we also have $c_1 < c_3$, we arrive at the contradiction $l > k$. Thus all n_3 shifted copies of D are mutually disjoint and $|C_j| = |E| = n_1 n_2 n_3 \geq n/5000$.

□

Theorem 3.5 *For each prime n there exists a wrapped set system $([n], \mathcal{F}_n)$, where $\mathcal{F}_n = \{S_0, S_1, \ldots, S_{n^2-1}\}$ such that each $S_i \in \mathcal{F}_n$ is a union of two sums of three arithmetic progressions and*

$$\mathrm{disc}(\mathcal{F}_n) > \frac{1}{10000} n^{1/2}.$$

Proof. For a fixed n we construct $\mathcal{F}_n = \{S_0, S_1, \ldots, S_{n^2-1}\}$ as follows: For S_0 just take the set $\{0, 1, \ldots \lfloor n/5000 \rfloor\}$ and for $0 < j < n$ we put $S_{jn} = C_j$ as constructed in Lemma 3.4. Since for all $0 \leq j < n$ we know that

$$\Big|\sum_{k \in S_{jn}} \zeta_j^k\Big| \geq \sum_{k \in S_{jn}} \mathrm{Re}\ \zeta_j^k \geq \frac{1}{10000} n,$$

from lemma 3.1 it immediately follows that

$$\mathrm{disc}(\mathcal{S}) > \frac{1}{10000} n^{1/2}.$$

□

Corollary 3.6 *For* $n \in \mathbf{N}$*, let* $([n], \mathcal{S}_n)$ *be a set system formed by all sums of three arithmetic progressions on* $[n]$*. Then* $\mathrm{disc}(\mathcal{S}_n) = \Omega(n^{1/2})$.

Acknowledgements

I would like to thank Jiří Matoušek for introducing me into the area and for help with writing this paper, and Lisa Bailey for reading the paper and correcting grammatical errors.

References

[AS92] N. Alon and J. Spencer. *The Probabilistic Method*. J. Wiley and Sons, New York, NY, 1992.

[Bec81] J. Beck. Roth's Estimate of the Discrepancy of Integer Sequences is Nearly Sharp. *Combinatorica* 1(4):319-325, 1981.

[BS95] J. Beck and V. Sós. *Discrepancy Theory*. In Handbook of Combinatorics, pages 1405-1446. North-Holland, Amsterdam, 1995.

[Cha00] B. Chazelle. *The Discrepancy Method*. Cambridge University Press, 2000.

[ES74] P. Erdős and J. Spencer. *Probabilistic Methods in Combinatorics*. Academic Press, 1974.

[Heb04] N. Hebbinghaus. Discrepancy of Sums of Arithmetic Progressions. *In Electronic Notes in Discrete Mathematics 17C*, pages 185-189, 2004.

[Mat99] J. Matoušek. *Geometric Discrepancy*. Springer, 1999.

[MS96] J. Matoušek and J.Spencer. Discrepancy in Arithmetic Progressions. *Journal of the American Mathematic Society*, 9:195-204, 1996.

[Rot64] K. F. Roth. Remark Concerning Integer Sequences. *Acta Arithmetica* 9:257-260, 1964.