CHAPTER 26

Discrepancy Theory

József BECK

Rutgers University, Department of Mathematics, New Brunswick, NJ 08903, USA

Vera T. SÓS

Mathematical Research Institute of the Hungarian Academy of Sciences, Reáltanoda utca 13–15, Budapest 1364, Hungary

Contents

HANDBOOK OF COMBINATORICS
Edited by R. Graham, M. Grötschel and L. Lovász

1. Introduction

The concept of *uniformly distributed sequences* and *sets* plays a fundamental role in many branches of mathematics (measure theory, ergodic theory, diophantine approximation, mathematical statistics, discrete geometry, numerical integration, etc.) This chapter explores the combinatorial background of many of these results. See also the survey article of Sós (1983b), and the monograph by Beck and Chen (1987).

Measure theoretic discrepancy results are accumulated in two complementary chapters of number theory, called *uniform distribution* and *irregularities of distribution*. The object of these theories is to measure the uniformity (or non-uniformity) of sequences and point distributions. For instance: how uniformly can N points in the unit cube be distributed relative to a given family of "nice" sets (e.g., boxes with sides parallel to the coordinate axes, rotated boxes, balls, all convex sets, etc.). The theory was initiated by the following theorem of Aardenne-Ehrenfest (Van der Corput's conjecture): for every infinite sequence of reals in $[0, 1]$ and for every $k > 0$, there exists a beginning section $(x_1, \ldots, x_n)$ of the sequence and a subinterval (α, β) such that the number of elements of this beginning section in this subinterval differs from $n(\beta - \alpha)$ (the number one expects) by at least k. The best possible effective result on this problem is due to Schmidt; it is equivalent to the following basic result in the theory of uniform distribution.

Theorem 1.1 (Schmidt 1972). *Let P be an arbitrary set of N points in the unit square $[0, 1)^2$. Then there exists a rectangle $B \subset [0, 1)^2$ with sides parallel to the coordinate axes such that*

$$\Big| |P \cap B| - N \operatorname{area}(B) \Big| > c \log N$$

(*where c is an absolute constant*).

The left-hand side of this inequality measures the "discrepancy" (deviation from the uniform distribution) of P in B. As a fascinating fact, we mention that balls have much greater discrepancy than boxes with sides parallel to the axes. Now we have a good understanding of this phenomenon, as we shall see later.

The object of combinatorial discrepancy theory is to color a set with two or more colors so that each set in a given family be colored as uniformly as possible. As a beautiful example, we mention Roth's theorem on long arithmetic progressions.

Theorem 1.2 (Roth 1964). *For any partition of the integers* $1, 2, \ldots, N$ *into two sets* S_1 *and* S_2, *there exists an arithmetic progression* $P = \{a, a + d, \ldots, a + kd\} \subset \{1, 2, \ldots, N\}$ *such that*

$$\Big| |P \cap S_1| - |P \cap S_2| \Big| > \tfrac{1}{20} N^{1/4} .$$

It took more than a decade to realize the close relationship between these areas. We can now say that they represent the continuous and the discrete aspects of the very same coherent theory. A general form of these problems is the following: given a measure space, approximate the measure on a subfamily of the measurable sets by a measure where each point has measure 0 or 1. Nontrivial "transference theorems" help to transform combinatorial and measure theoretic results into each other.

Compare Roth's theorem also to the following fundamental results of Ramsey theory (see chapter 25).

Theorem 1.3 (Van der Waerden 1927). *For any integers k and r there exists an $W(k, r)$ such that if $N > W(k, r)$ then for every r-coloring of $\{1, 2, \dots, N\}$ there exists a monochromatic arithmetic progression of length k.*

Theorem 1.4 (Ramsey 1930). *For any integers t and r there exists an $R(t, r)$ such that if $n > R(t, r)$ and the edges of K_n are r-colored, then there must be a monochromatic K_t.*

These theorems have the same structure as Roth's: given an underlying set S and a family of subsets of this set, the claim is that the underlying set has no partition which splits each set contained in the given family "reasonably well" (only in this case any proper splitting is accepted).

Discarding the special structure of the system we can formulate the basic problem in combinatorial discrepancy theory. Let $S = \{x_1, \dots, x_n\}$ be a finite set and $\mathcal{H} = \{A_1, \dots, A_m\}$, a family of subsets of S. Our goal is to find a partition $S = S_1 \cap S_2$, $S_1 \cap S_2 = \emptyset$ that splits each set in the family $\mathcal{H}$ as equally as possible. In other words, we want to find the least integer D for which there exists a 2-coloring of the underlying set such that in each A_i, the difference between the numbers of red and blue elements is at most D.

Often we shall describe the partition by a function $f : S \to \{-1, 1\}$. Then the *discrepancy* of $\mathcal{H}$ is defined by

$$\mathcal{D}(\mathcal{H}) = \min_f \max_{1 \le j \le m} \left| \sum_{x_i \in A_j} f(x_i) \right| ,$$

where the minimum is taken over all functions $f : S \to \{-1, 1\}$.

Best and worst families. Although the systematic investigation of combinatorial discrepancy started just a few years ago, there is a fundamental old result which characterizes the "best" families, those for which $\mathcal{D}(\mathcal{H}) \le 1$, and this is inherited to subhypergraphs. These are the unimodular hypergraphs, whose theory was developed for its importance in integer programming (see chapter 30).

A hypergraph $\mathcal{H}$ is *unimodular*, if its incidence matrix A is totally unimodular (i.e., every square submatrix of A has determinant 0, +1 or −1). See chapters 7 and 30 for examples of such hypergraphs; here we mention hypergraphs whose edges are the vertex sets of directed paths in an arborescence. For $X \subseteq S$, the *restriction* $\mathcal{H}_X$ is defined as the family $\{A \cap X \mid A \in \mathcal{H}\}$.

Theorem 1.5 (Ghouila-Houri 1962). *$\mathcal{H}$ is unimodular iff $\mathcal{D}(\mathcal{H}_X) \leqslant 1$ for all restrictions $\mathcal{H}_X$ of $\mathcal{H}$.*

Unimodular hypergraphs have the following stronger property.

Theorem 1.6. *If $\mathcal{H} = (V, E)$ is unimodular then for any $p \in [-1, 1]^V$ there exist $\varepsilon \in \{-1, 1\}^V$ such that for every $A \in E$,*

$$\left| \sum_{i \in A} (\varepsilon_i - p_i) \right| \leqslant 1 .$$

Informally, an arbitrary weight distribution on S can be very well approximated with 0–1 weights.

Furthermore, we have the following.

Theorem 1.7. *If $\mathcal{H}$ is unimodular, then for every $r > 1$ there exists an r-equipartition $S = S_1 \cup \cdots \cup S_r$ so that for every $A \in \mathcal{H}$ and $1 \leqslant j \leqslant r$,*

$$\left\lfloor \frac{A}{r} \right\rfloor \leqslant |A \cap S_j| \leqslant \left\lceil \frac{A}{r} \right\rceil .$$

The "*worst*" families from the point of view of discrepancy are the "non-2-colorable families", i.e., families with chromatic number $\chi(\mathcal{H}) > 2$. (Recall from chapter 7 that a hypergraph is non-2-colorable iff for any partition $S = S_1 \cup S_2$ there exists an $A \in \mathcal{H}$ so that $A \subseteq S_1$ or $A \subseteq S_2$.) An r-uniform hypergraph is 2-colorable if and only if its discrepancy is less than r. (Note that this remark also shows that the computation of the discrepancy of a hypergraph is NP-hard.)

One of the most extensively studied field of combinatorics is Ramsey theory, which can be viewed as the theory of non-2-colorable families (see chapter 7). Many of the results and problems there are relevant to our subject.

Considering the results in Ramsey theory we must realize the white spots and gaps in discrepancy theory. A large variety of Ramsey-type results are available not only for graphs and hypergraphs but for different structures like vector spaces, combinatorial lines, parameter-sets, groups, euclidean spaces, topological spaces, sets of solutions of linear systems, etc. However, an analogous discrepancy theory is missing for most of these structures.

We can say that in the class of hypergraphs unimodular families are at one (at the "good") end and non-2-colorable families at the other ("bad") end. We conclude this section with an example of A.J. Hoffman showing that the union of two unimodular (so best!) families can be non-2-colorable (so worst!).

Example 1.8 (Hoffman 1987). Let T be an arbitrary arborescence rooted at r. Let $\mathcal{H}_1$ consist of the arc-sets of directed paths in T from r to a leaf. Let $\mathcal{H}_2$ consist of the sets $B(x)$, where $B(x)$ is the set of edges with their tails at node x, for each non-leaf node x. Obviously $\mathcal{H}_1$ and $\mathcal{H}_2$ are unimodular, but $\mathcal{H}_1 \cup \mathcal{H}_2$ is not even 2-colorable. (Note that we can choose the tree so that $\mathcal{H}_1 \cup \mathcal{H}_2$ is k-uniform for a given k.)

A very simple unimodular hypergraph is the hypergraph of all intervals in a permutation (a totally ordered set). How large can be the discrepancy of the union of such hypergraphs? For two permutations, the discrepancy is at most 2; but the following problem, due to Beck, has been open for quite a while.

Problem 1.9. Is it true that the hypergraph consisting of the intervals of three permutations of a set X has discrepancy O(1), independent of $|X|$?

Recently Bohus (1990) gave the upper bound $O(\log |X|)$ for this discrepancy, not only for three, but for any constant number of permutations.

2. Bounds on $\mathcal{D}(\mathcal{H})$

Many of the results in this section have applications in different fields. In fact, many of the problems originated in different branches of mathematics.

There is a trivial upper bound on the combinatorial discrepancy:

$$\mathcal{D}(\mathcal{H}) \leq \max_{A \in \mathcal{H}} |A| .$$

If $\mathcal{H}$ is k-uniform (i.e., $|A| = k$ for all $A \in \mathcal{H}$) then equality holds iff $\mathcal{H}$ is a not 2-colorable.

To bound the discrepancy in terms of the number of edges $m = |\mathcal{H}|$, observe that a pair of vertices contained in the same set of edges can be deleted without decreasing the discrepancy. Repeating this we end up with a hypergraph in which every edge has at most $2^m - 1$ elements and hence

$$\mathcal{D}(\mathcal{H}) \leq 2^m - 1 .$$

This upper bound can be easily improved. The first result in this direction was the theorem of Olson and Spencer (1978) where they proved the upper bound

$$\mathcal{D}(\mathcal{H}) \leq cm^{1/2} \log m .$$

The best possible result is the following.

Theorem 2.1 (Spencer 1985). *For every $\mathcal{H}$ with $|\mathcal{H}| = m$*

$$\mathcal{D}(\mathcal{H}) \leq 6m^{1/2} .$$

For a proof, which is an involved application of the probabilistic method, see chapter 33. This result is best possible (up to a constant): if an Hadamard matrix of order $m+1$ exists, then there exists a hypergraph $\mathscr{H}$ with $|\mathscr{H}|=m$ such that $\mathscr{D}(\mathscr{H}) \geq \frac{1}{2}m^{1/2}$ (see Corollary 2.11).

Spencer's theorem has interesting applications in Fourier analysis to "Rudin–Shapiro sequences" (see Spencer 1985), and to Littlewood's problem on "flat polynomials" (see Beck 1991b).

It is somewhat surprising that there is an upper bound on $\mathscr{D}(\mathscr{H})$ depending only on the maximum degree $\Delta(\mathscr{H}) = \max_{x\in S} |\{A \in \mathscr{H}: x \in A\}|$.

Theorem 2.2 (Beck and Fiala 1981). *Let $\mathscr{H}$ be a finite hypergraph. Then*

$$\mathscr{D}(\mathscr{H}) < 2\Delta(\mathscr{H}) .$$

In fact, we have the following more general result.

Theorem 2.2′. *Let us associate with every $i \in S$ a real number $p_i \in [-1, +1]$. Then there exist $\varepsilon_i \in \{-1, +1\}$ $(i \in S)$ such that*

$$\max_{A\in\mathscr{H}} \left|\sum_{i\in A} (\varepsilon_i - p_i)\right| < 2\Delta(\mathscr{H}) .$$

Proof. The key idea is to consider variables ε_i $(i \in S)$ lying anywhere in $[-1, +1]$. Initially $\varepsilon_i = p_i$; all sets then have zero "discrepancy". At the end each ε_i must be -1 or $+1$, providing the coloration in the theorem. We describe the procedure that is to be iterated to go from the initial trivial "coloration" to the final one.

Suppose we have some current assignment ε_i. Call *i fixed* if $\varepsilon_i = \pm 1$ and *floating* otherwise. Let $A = [a_{ij}]$ denote the incidence matrix of the family $\mathscr{H}$. Call row j *ignored* if $\sum' a_{ji} \leq \Delta(\mathscr{H})$ (the sum over the floating i) and *active* otherwise. As each column sum is at most $\Delta(\mathscr{H})$, there are fewer active rows than floating columns. Find y_i, for each floating i, with $\sum a_{ji} y_i = 0$ for each active row j. As this system is undetermined, there is a nonzero solution. Now replace ε_i by $\varepsilon_i + \lambda y_i$ where λ is chosen so that all ε_i remain in $[-1, +1]$ and some floating ε_i becomes ± 1 (i.e., fixed).

Iterate the above procedure until all $\varepsilon_i = \pm 1$. To see that the values obtained satisfy the requirement of the theorem, observe that a given row has zero "discrepancy" (i.e., $\sum a_{ji}(\varepsilon_i - p_i) = 0$) until it becomes ignored. After that, each ε_i still floating changes by at most 2 and hence the sum $\sum a_{ji}(\varepsilon_i - p_i)$ changes by less than $2\Delta(\mathscr{H})$. □

Theorem 2.2 was motivated by the following "integer making lemma" (and in fact is a generalization of it).

Lemma 2.3 (Baranyai 1974). *Let $A = (a_{ij})$ be a matrix of real elements. Then there* *exist an integer matrix* $A^* = (a^*_{ij})$ *such that*

$$|a_{ij} - a^*_{ij}| < 1 \qquad \textit{for all } i, j\,,$$

$$\Big|\sum_i a_{ij} - \sum_i a^*_{ij}\Big| < 1 \quad \textit{for all } j\,,$$

$$\Big|\sum_j a_{ij} - \sum_j a^*_{ij}\Big| < 1 \quad \textit{for all } i\,,$$

and

$$\Big|\sum_i \sum_j a_{ij} - \sum_i \sum_j a^*_{ij}\Big| < 1\,.$$

This lemma was the basic tool in Baranyai's theorem on the factorization of the complete uniform hypergraph (see chapters 7 and 14). The lemma can also be proved using the integrality theorem of flow theory (see chapter 2).

We suspect that Theorem 2.2 can be essentially improved. The following conjecture would also generalize Spencer's theorem 2.1.

Conjecture 2.4 (Beck–Fiala).

$$\mathcal{D}(\mathcal{H}) \leqslant c(\Delta(\mathcal{H}))^{1/2}\,.$$

If true then it is best possible apart from the constant factor c. Corollary 2.6 below justifies the weaker conjecture $\mathcal{D}(\mathcal{H}) < (\Delta(\mathcal{H}))^{1/2+\varepsilon}$ when both $|S|$ and $|\mathcal{H}|$ are "subexponential" functions of the maximum degree. For later application, we state first a more general result.

Theorem 2.5 (Beck 1981b). *Let* $\mathcal{H}$ *be a finite hypergraph with* $\bigcup \mathcal{H} = S$. *Let* M *and* K *be natural numbers such that*

$$\Delta(\{A \in \mathcal{H}\colon |A| \geqslant M\}) \leqslant K\,.$$

Then

$$\mathcal{D}(\mathcal{H}) < c(M + K \cdot \log K)^{1/2} \cdot (\log|\mathcal{H}|)^{1/2} \cdot \log|S|\,.$$

Choosing $M = 1$ and $K = \Delta(H)$, we obtain the following.

Corollary 2.6. *For any finite hypergraph with* $\Delta = \Delta(\mathcal{H})$, *we have*

$$\mathcal{D}(\mathcal{H}) < c \cdot \Delta^{1/2} \cdot \log|\mathcal{H}| \cdot \log|S|\,.$$

The following somewhat technical theorem, which is useful in applications, is a generalization of Corollary 2.6.

Theorem 2.7 (Beck 1988). *Let $\mathcal{H}$ be a finite hypergraph with $\bigcup \mathcal{H} = S$. Suppose that there is a second family $\mathcal{G}$ of subsets of S such that*

(i) $\Delta(\mathcal{G}) \leq D$; *and*

(ii) *every $A \in \mathcal{H}$ can be represented as the disjoint union of at most K elements of $\mathcal{G}$. Then*

$$\mathcal{D}(\mathcal{H}) < c \cdot ((K \cdot D \cdot \log D \cdot \log|\mathcal{H}|)^{1/2} \cdot \log|S| .$$

Note that if $\mathcal{G} = \mathcal{H}$ then we obtain Corollary 2.6.

We have to remark that there are very few general *lower bounds* on $\mathcal{D}(\mathcal{H})$. The following one is based on linear algebra. To state it in its natural generality, define the ℓ_2-discrepancy of a hypergraph $\mathcal{H}$ by

$$\mathcal{D}_2(\mathcal{H}) = \min_{\varepsilon \in \{-1,1\}^S} \left(\sum_{A \in \mathcal{H}} \left(\sum_{i \in A} \varepsilon_i \right)^2 \right)^{1/2} .$$

Clearly $\mathcal{D}(\mathcal{H})m^{-1/2} \leq D(\mathcal{H}) \leq \mathcal{D}_2(\mathcal{H})$. We denote by $\lambda_{\min}(M)$ the least eigenvalue of the matrix M. We recall: $|\mathcal{H}| = m$ and $|S| = n$.

Theorem 2.8 (Lovász–T. Sós). *Let M be the incidence matrix of $\mathcal{H}$. Then*

(i) $\mathcal{D}_2(\mathcal{H}) \geq (n\lambda_{\min}(M^{\mathrm{T}}M))^{1/2}$,

(ii) *if for some diagonal matrix D, the matrix $M^{\mathrm{T}}M - D$ is positive semidefinite, then* $\mathcal{D}_2(\mathcal{H}) \geq (\mathrm{Tr}\, D)^{1/2}$. Note that T stands for transpose.

Proof. Let $f \in \{-1, 1\}^S$ attain the minimum in the definition of $\mathcal{D}_2(\mathcal{H})$. Then

$$\begin{aligned}\mathcal{D}_2(\mathcal{H})^2 &= \sum_{A \in H} \left(\sum_{i \in A} f_i \right)^2 = (Mf)^{\mathrm{T}}(Mf) = f^{\mathrm{T}}M^{\mathrm{T}}Mf \\ &\geq f^{\mathrm{T}}f\lambda_{\min}(M^{\mathrm{T}}M) = n\lambda_{\min}(M^{\mathrm{T}}M) .\end{aligned}$$

This proves (i); the proof of (ii) is similar. □

Corollary 2.9. *If $\mathcal{H}$ has constant pair-degree, i.e.,*

$$|\{A: i, j \in A \in \mathcal{H}\}| = \lambda$$

for every i, $j \in S$, $i \neq j$, and d_i denotes the degree of $i \in S$, then

$$\mathcal{D}(\mathcal{H}) \geq n^{-1/2} \left(\sum_{i=1}^{n} (d_i - \lambda) \right)^{1/2} .$$

Corollary 2.10. *Let $\mathcal{H}$ be formed by the set of lines in a finite projective plane of order p. Then*

$$\mathcal{D}(\mathcal{H}) \geq \sqrt{p} .$$

Corollary 2.11. *Let H be an $n \times n$ Hadamard matrix, i.e., a ± 1 matrix whose column vectors are mutually orthogonal and has all 1s in the first row. Let $\mathcal{H}$ be the* *hypergraph whose incidence matrix is obtained from H by replacing the* -1*s by* **0***s. Then*

$$\mathcal{D}(\mathcal{H}) > \frac{\sqrt{n}}{2}.$$

This corollary proves that Theorem 2.1 is best possible apart from the constant factor.

The most important application of Theorem 2.8 is Roth's theorem (Theorem 1.2, see section 5).

3. Various concepts of discrepancy

Suppose we want to split the sets in $\mathcal{H}$ in ratio α, $1-\alpha$. In other words, we want to find a system of representatives of $\mathcal{H}$ so that the number of representatives in every set $A \in \mathcal{H}$ is as close to $\alpha|A|$ as possible. Then, setting $\lambda = 2\alpha - 1$,

$$\mathcal{D}(\mathcal{H}; \lambda) = \min_{\varepsilon \in \{-1,1\}^S} \max_{A \in \mathcal{H}} \left| \sum_{i \in A} (\varepsilon_i - \lambda) \right|$$

measures the corresponding discrepancy. Obviously

$$\mathcal{D}(\mathcal{H}; \tfrac{1}{2}) = \mathcal{D}(\mathcal{H}).$$

More generally, we may consider a weight-function $p: S \to [-1, 1]$ and the corresponding discrepancy

$$\mathcal{D}(\mathcal{H}; p) = \min_{\varepsilon \in \{-1,1\}^S} \max_{A \in \mathcal{H}} \left| \sum_{i \in A} (\varepsilon_i - p_i) \right|$$

(this value has come up in Theorem 2.2′). The *inhomogeneous discrepancy* of $\mathcal{H}$ is defined by

$$\mathcal{D}_{\mathrm{I}}(\mathcal{H}) = \max_p \mathcal{D}(\mathcal{H}, p)$$

and measures how well an arbitrary weight distribution on S can be approximated with 0–1 measures regarding the family $\mathcal{H}$. Considering the particular cases $p_1 = \cdots = p_n = \lambda$ we define the *diagonal discrepancy* by

$$\mathcal{D}_{\mathrm{D}}(\mathcal{H}) = \max_\lambda \mathcal{D}(\mathcal{H}; \lambda).$$

The *hereditary discrepancy* of $\mathcal{H}$ is defined by

$$\mathcal{D}_{\mathrm{H}}(\mathcal{H}) = \sup_{X \subseteq S} \mathcal{D}(\mathcal{H}_X).$$

Ghouila-Houri's theorem 1.5 asserts that a hypergraph is totally unimodular iff its hereditary discrepancy is at most 1.

Observe that adding new elements to some of the sets in $\mathcal{H}$ appropriately we can achieve that this enlarged hypergraph will have discrepancy 0. This means, that $\mathscr{D}(\mathscr{H})$ can be small by accident, while $\mathscr{D}_{\mathrm{I}}(\mathscr{H})$ and $\mathscr{D}_{\mathrm{H}}(\mathscr{H})$ depend on more intrinsic properties of $\mathscr{H}$. In fact, $\mathscr{D}(\mathscr{H})$ can be much smaller then $\mathscr{D}_{\mathrm{I}}(\mathscr{H})$ or $\mathscr{D}_{\mathrm{H}}(\mathscr{H})$. A simple example is the following. Let $S=\{1,\ldots,4n\}$ and

$$\mathscr{H}=\{A \mid A\subset S, |A\cap\{1,\ldots,2n\}|=|A|/2\}\,.$$

Then $\mathscr{D}(\mathscr{H})=0$ but $\mathscr{D}_{\mathrm{I}}(\mathscr{H})=n$ and $\mathscr{D}_{\mathrm{H}}(\mathscr{H})=n$.

We mention the trivial inequalities

$$\mathscr{D}(\mathscr{H})\leqslant\min\{\mathscr{D}_{\mathrm{I}}(\mathscr{H}),\mathscr{D}_{\mathrm{H}}(\mathscr{H})\}$$

and

$$\mathscr{D}(\mathscr{H},\lambda)\leqslant\mathscr{D}_{\mathrm{D}}(\mathscr{H})\leqslant\mathscr{D}_{\mathrm{I}}(\mathscr{H})\,.$$

The following nontrivial inequality was first explicitly formulated in Lovász et al. (1986). The proof is identical with that of Lemma 3 in Beck and Spencer (1984b).

Theorem 3.1. *For every hypergraph* $\mathscr{H}$,

$$\mathscr{D}_{\mathrm{I}}(\mathscr{H})\leqslant 2\mathscr{D}_{\mathrm{H}}(\mathscr{H})\,.$$

Proof. Let, for each $i\in S$, a weight $-1\leqslant p_i\leqslant 1$ be given. Let $\alpha_i=(1+p_i)/2\in[0,1]$. Assume first that all the α_i have finite binary expansion, i.e., there is a natural number n so that $2^n\cdot\alpha_i\in\mathbb{Z}$ for all $i\in S$. Let n be minimal with this property. Let $X\subset S$ be the set of points $i\in S$ such that α_i has 1 for its nth binary digit. As $\mathscr{D}(\mathscr{H})\leqslant\mathscr{D}_{\mathrm{H}}(\mathscr{H})$, there exist $\varepsilon_i=\pm 1$ for all $i\in X$ such that

$$\Big|\sum_{i\in A\cap X}\varepsilon_i\Big|\leqslant\mathscr{D}_{\mathrm{H}}(\mathscr{H})$$

for all $A\in\mathscr{H}$. Define approximations $\alpha_1^{(1)},\alpha_2^{(1)},\ldots,\alpha_N^{(1)}$ by

$$\alpha_i^{(1)}=\begin{cases}\alpha_i+\varepsilon_i\cdot 2^{-n} & \text{if } i\in X\,,\\ \alpha_i & \text{if } i\in S\setminus X\,.\end{cases}$$

For any $A\in\mathscr{H}$,

$$\Big|\sum_{i\in A}(\alpha_i^{(1)}-\alpha_i)\Big|=\Big|\sum_{i\in A\cap X}2^{-n}\cdot\varepsilon_i\Big|\leqslant 2^{-n}\cdot\mathscr{D}_{\mathrm{H}}(\mathscr{H})\,.$$

The values $\alpha_i^{(1)}$ have binary expansions of length at most $(n-1)$. We repeat this procedure (note that X will be a different set), getting $\alpha_i^{(2)}$ with

$$\Big|\sum_{i\in A}(\alpha_i^{(2)}-\alpha_i^{(1)})\Big|\leqslant 2^{-(n-1)}\mathscr{D}_{\mathrm{H}}(\mathscr{H})$$

for all $A\in\mathscr{H}$.

We apply this procedure n times, finally reaching $\alpha_i^{(n)}$ with binary expansions of length zero, i.e., $\alpha_i^{(n)} = 0$ or 1. Let $\varepsilon_i = 2\alpha_i^{(n)} - 1 \in \{-1, +1\}$. Then for all $A \in \mathcal{H}$,

$$\Big|\sum_{x_i \in A} (\varepsilon_i - p_i)\Big| = 2\Big|\sum_{i\in A} (\alpha_i^{(n)} - \alpha_i)\Big| \leq 2 \sum_{j=0}^{n-1} \Big|\sum_{i \in A} (\alpha_i^{(j+1)} - \alpha_i^{(j)})\Big|$$

$$\leq 2 \sum_{j=0}^{n-1} 2^{-(n-j)} \cdot \mathcal{D}_{\mathrm{H}}(\mathcal{H}) \leq 2\mathcal{D}_{\mathrm{H}}(\mathcal{H})$$

as required. Finally, a compactness argument implies the truth of Theorem 3.1 for arbitrary $p_1, \ldots, p_n \in [-1, +1]$. □

Observe that all the upper bounds in Theorems 2.1, 2.2, 2.6, 2.7 are valid in fact for the hereditary discrepancy.

The discrepancy of a matrix. The concept of discrepancy can be expressed in terms of the incidence matrix M of the hypergraph $\mathcal{H}$:

$$\mathcal{D}(\mathcal{H}) = \min_{\varepsilon \in \{-1,+1\}^S} \|M\varepsilon\|_\infty$$

and

$$\mathcal{D}_{\mathrm{I}}(\mathcal{H}) = \max_{p \in [-1,+1]^S} \min_{\varepsilon \in \{-1,+1\}^S} \|M(\varepsilon - p)\|_\infty .$$

Note that these definitions are meaningful for any matrix M. Therefore, following Lovász et al. (1986), we can use the notation $\mathcal{D}(M)$ and $\mathcal{D}_{\mathrm{I}}(M)$ for an arbitrary matrix M. We can also generalize the hereditary version by letting $\mathcal{D}_{\mathrm{H}}(M)$ be the maximum of $\mathcal{D}(M')$ over all submatrices M' of M.

Almost all of the previous results, most notably Theorems 2.2 and 2.8, extend to matrices in a natural way. The following slight generalization of Theorem 2.2 also follows by the same argument.

Theorem 3.2. *Assume that every square submatrix of a matrix M has row with l_1-norm at most* 1. *Then* $\mathcal{D}(M) \leq 2$.

The above generalized versions of the notion of discrepancy may become easier to grasp from the following nice geometric interpretation. Consider the set

$$U_A = \{x \in R^S : \|Ax\|_\infty \leq 1\} ,$$

i.e., the "unit ball" of the norm $\|Ax\|_\infty$. So U_A is a convex polyhedron centrally symmetric with respect to the origin. For $t > 0$, consider the convex set $t \cdot U_A$ and let $U_1(t), U_2(t), \ldots$ be the copies of $t \cdot U_a$ obtained by translating its center by all ± 1-vectors. Then

- $\mathcal{D}(A)$ is the least number t for which some $U_j(t)$ contains the origin;
- $\mathcal{D}_I(A)$ is the least number t for which the sets $U_j(t)$ cover the cube $[-1, 1]^S$;

• $\mathscr{D}(A)$ is the least number t for which the center of each face F of the cube $[-1, 1]^S$ is contained in at least one of the sets $U_j(t)$ centered at the vertices of F.

Theorem 1.5 raises the question whether in general the discrepancy of a hypergraph (or of a matrix) is related to the determinants of the submatrices of the incidence matrix. In this direction there is a lower bound theorem from Lovász et al. (1986).

Theorem 3.3. *For any matrix A,*

$$\mathscr{D}(A) \geq \max_k \max_B |\det B|^{1/k},$$

where B ranges over all $k \times k$ submatrices of A.

Let us think of the rows of matrix A as ordered by *importance* so that we may wish to make the discrepancy in early rows extremely small, perhaps at the expense of the later E_i. The following result states that there is an approximation which is extremely good with respect to the early rows and is reasonably good with respect to all.

Theorem 3.4 (Beck and Spencer 1984b, Spencer 1985). *Let $M = (m_{ij}) \in \mathbb{R}^{m \times n}$ be a matrix with $|m_{ij}| \leq 1$. Let $p_1, \ldots, p_N \in [-1, +1]$.*

(i) *There exist $\varepsilon_1, \ldots, \varepsilon_n \in \{-1, +1\}$ so that*

$$\left| \sum_{j=1}^{n} m_{ij}(p_i - \varepsilon_i) \right| < ci^{1/2},$$

(ii) *If the upper bound is relaxed to $2i$ then such ε_j are polynomial time computable.*

Note that (i) of Theorem 3.4 is best possible apart from constant factor (this again follows by considering Hadamard matrices). Part (ii) follows by applying Theorem 3.3 (whose proof, just like the proof of Theorem 2.2, can be followed by a polynomial time algorithm) to the matrix (m_{ij}/i).

In the particular case $m_{ij} \in \{0, 1\}$ and $p_i = 0$ we obtain the following.

Corollary 3.5. *Let $Y_1, Y_2, Y_3, \ldots, Y_M$ be a sequence of subsets of a finite set X.*

(i) *There exist a 2-coloring $f: X \to \{-1, +1\}$ so that*

$$\left| \sum_{x \in Y_i} f(x) \right| < c \cdot i^{1/2}, \quad 1 \leq i \leq M.$$

(ii) *One can find in polynomial time a 2-coloring $f: X \to \{-1, +1\}$ so that*

$$\left| \sum_{x \in Y_i} f(x) \right| < 2i, \quad 1 \leq i \leq M.$$

Theorem 3.4 has some nice applications in a matrix balancing problem (see

Beck and Spencer 1983, 1989). Let an arbitrary matrix $A=(a_{ij})$, $1\leq i, j\leq n$, be given with all $a_{ij}\in\{-1,+1\}$. By a row shift we mean the act of replacing, for a particular i, all coefficients a_{ij} in the ith row by their negatives $(-a_{ij})$. The column shift is defined similarly. A line shift means either a row or a column shift. Consider the following solitaire game. The player applies a succession of line shifts to the matrix A. His object is to make the absolute value of the sum of all the coefficients of A as small as possible. Let $\|A\|$ denote this minimum value. Komlós and Sulyok (1970), resolving a conjecture of L. Moser, showed that if n is sufficiently large then $\|A\|\leq 2$ may be achieved ($\|A\|\leq 1$ if n is odd). As an illustration, we shall derive this result from (ii) of Theorem 3.4 in the case of even n.

Theorem 3.6. *Let $n\geq 2$ be an even integer. Given any $n\times n$ matrix $A=(a_{ij})$ with all $a_{ij}\in\{-1,+1\}$, there exist $\delta_1,\ldots,\delta_n$, $\varepsilon_1,\ldots,\varepsilon_n\in\{-1,+1\}$ so that*

$$\|A\|=\left|\sum_{i=1}^{n}\sum_{j=1}^{n}\delta_i\varepsilon_j a_{ij}\right|\leq 2\,.$$

Proof. It follows from (ii) of Theorem 3.4 that there exist column shifts ε_j so that the new row sums r_i satisfy $|r_i|<2i$, $1\leq i\leq K$. For simplicity of notation let us then apply row shifts so that all row sums are nonnegative. Since all r_i are even integers we have $r_1=0$, and, in general, $0\leq r_i\leq 2i-2$.

We now describe a simple technique that will give the final row shifts. Let $s_1,\ldots,s_K$ be nonnegative integers and let T be a positive integer such that $s_1\leq T$ and for $1\leq i\leq n-1$,

$$s_{i+1}\leq s_1+\cdots+s_i+T\,.$$

Then there exist $\delta_i,\ldots,\delta_n=\pm 1$, so that

$$|\delta_1 s_1+\cdots+\delta_n s_n|\leq T\,.$$

We can find such δ_i by reverse induction. Set $\delta_n=+1$. Having found δ_n, $\delta_{n-1},\ldots,\delta_{i+1}$ we choose $\delta_i=\pm 1$ so as to minimize the absolute value of the partial sum $\delta_n s_n+\cdots+\delta_{i+1}s_{i+1}+\delta_i s_i$. We shall call this method the *greedy technique* for the remainder of the proof.

We may not immediately apply the greedy technique because we may have too many $r_i=0$ and thereby T large. Reorder the rows in increasing order of row sums. We then still have $0\leq r_i\leq 2i-2$. Suppose the first u rows have sum zero and the next v rows have sum two. If $u=1$ we may simply apply the greedy technique so we shall assume $u>1$. Let r_i' be the new absolute value of ith row sum after a single column is shifted. For the first u rows $r_i'=2$ regardless of which column is shifted. For the next v rows $r_i'=0$ for $(n/2)+1$ of the possible column shifts, these being the cases when an entry $+1$ switched to -1, and $r_i'=4$ for the remaining $(n/2)-1$ column shifts. Thus the average value of r_i', taken over all n possible column shifts, is $2-(4/n)$. Now we conclude that the average value of $r_{u+1}'+\cdots+r_{u+v}'$ is $v(2-(4/n))$. If $v\geq n/2$ then the greedy technique trivially works and hence we may assume $v < n/2$. Thus $v(2-(4/n)) > 2v-2$. Since this is the average, there must be one specific column change so that

(1) $r'_{u+1} + \cdots + r'_{u+v} \geq 2v$. We also have

(2) $r'_1 = \cdots = r'_u = 2$, and

(3) $0 \leq r'_i \leq 2i$ for $i > u+v$.

We observe that $r'_1 + \cdots + r'_{u+v} \geq 2(u+v)$ and $r'_i \geq 2$ for $i > u+v$ since $r_i \geq 4$. Hence

$$r'_1 + \cdots + r'_i + 2 \geq 2i + 2 \geq r'_{i+1}$$

for all $i \geq u+v$.

Trivially

$$r'_1 + \cdots + r'_i + 2 \geq 4 \geq r'_{i+1} ,$$

when $1 \leq i < u+v$. Thus we may apply the greedy technique to the row sums $r'_1, \ldots, r'_k$, completing the proof. □

Applying the stronger relation (i) of Theorem 3.3, one can prove the following general result (see Beck and Spencer 1989).

Theorem 3.7. *There exists a constant $c > 0$ such that for every $m \times n$ matrix $A = (a_{ij})$ with all $|a_{ij}| \leq 1$ there exist $\delta \in \{-1,1\}^m$ and $\varepsilon \in \{-1,1\}^n$ such that*

$$\left|\sum_i \sum_j \delta_i \varepsilon_j a_{ij}\right| < c .$$

4. Vector-sums

We have seen a geometric interpretation of discrepancy problems in the row space of the corresponding matrix. Now we consider the space of the column vectors, which leads to several new and interesting questions. In fact the investigation of value-distributions of *vector-sums* developed earlier and independently of hypergraph coloring problems or of discrepancy theory.

Let $M = (v_1, \ldots, v_n)$, $v_i \in \mathbb{R}^m$ for $1 \leq i \leq n$. Let further $\|\cdot\|$ and $\|\cdot\|'$ denote two arbitrary norms in $\mathbb{R}^m$.

We define the *discrepancy* (relative to the two norms) by

$$\mathcal{D}(M; \|\cdot\|, \|\cdot\|') = \frac{\min_{\varepsilon \in \{-1,1\}^n} \|\sum_{i=1}^n \varepsilon_i v_i\|}{\max_{1 \leq i \leq n} \|v_i\|'}$$

and

$$\mathcal{D}(\|\cdot\|, \|\cdot\|') = \max_M \mathcal{D}(M; \|\cdot\|, \|\cdot\|') .$$

Note that for any matrix M and norm $\|\cdot\|'$,

$$\mathcal{D}(M) = \mathcal{D}(M; l_\infty, \|\cdot\|') \cdot \max_{1 \le i \le n} \|v_i\|' .$$

The case when $\|\cdot\|$ was the l_2 norm also came up briefly in Theorem 2.8.

Already in 1963 it was asked by Dworetzky what $\mathcal{D}(\|\cdot\|, \|\cdot\|)$ equals for a given norm. The more general question (where the two norms are not necessarily the same) was formulated first in Bárány and Grinberg (1981), who gave the following general upper bound for Dworetzky's problem.

Theorem 4.1 (Bárány and Grinberg 1981). *For an arbitrary norm $\|\cdot\|$ in $\mathbb{R}^m$,*

$$\mathcal{D}(\|\cdot\|, \|\cdot\|) \le m .$$

This is sharp when $\|\cdot\|$ is the l_1 norm.

Now let us consider the special cases when $\|\cdot\|$ and $\|\cdot\|^*$ are one of the three most important norms: the l_∞ norm, the l_2 norm or the l_1 norm. Theorem 2.1 has the following generalization in this setting.

Theorem 4.2 (Spencer 1985). $\mathcal{D}(l_\infty, l_\infty) \le 6\sqrt{m}$.

(Observe that the upper bounds in Theorems 4.1 and 4.2 depend only on the dimension!) Theorem 2.2 is also valid in this more general form.

Theorem 4.3 (Beck and Fiala 1981). $\mathcal{D}(l_\infty, l_1) \le 2$.

Grinberg observed, that for any M in $\mathbb{R}^m$,

$$\mathcal{D}(l_2, l_2) \le \sqrt{m} .$$

This is sharp. Indeed, consider m pairwise orthogonal unit vectors $e_1, \ldots, e_m$ in $\mathbb{R}^m$. Then $\|\sum_{i=1}^m \varepsilon_i e_i\|_2 = m^{1/2}$ for any choice of $\varepsilon \in \{-1, 1\}^m$.

All but one of the remaining cases are trivial or easy consequences of the above ones. The only nontrivial case is when $\|\cdot\| = l_\infty$ and $\|\cdot\|' = l_2$. In that case nothing nontrivial is known. The conjecture of Komlós refers to this case.

Conjecture 4.4 (Komlós). There exists an absolute constant c such that

$$\mathcal{D}(l_\infty, l_2) \le c .$$

The Komlós conjecture implies the Beck–Fiala conjecture 2.4 for set-systems.

Partial sums. The problems we considered in the preceding paragraphs are of *static character*. The *dynamic* version is when we color the points one by one and we would like to have a "good" coloring at *each stage*. This formulation also allows us to study problems in which the underlying set S is infinite. The following theorems are of this "dynamic" character.

Theorem 4.5 (Bárány and Grinberg 1981). *Let $v_1, v_2, \ldots, v_n$ be n vectors in $\mathbb{R}^m$ with $\|v_i\| \leq 1$, where $\|\cdot\|$ is any norm in $\mathbb{R}^m$. Then there exist a sequence $\varepsilon_1, \ldots, \varepsilon_n$, $\varepsilon_i \in \{-1, +1\}$ so that*

$$\left\|\sum_{i=1}^{t} \varepsilon_i v_i\right\| \leq 2m\,, \quad \text{for } t = 1, 2, \ldots, n\,.$$

It is conjectured that if $\|\cdot\| = l_2$ or l_∞, then in this theorem, $2m$ can be replaced by $K\sqrt{m}$. For l_∞ norm and if $m = n$, Spencer proved this conjecture.

Theorem 4.6 (Spencer 1986). *For any sequence $v_1, \ldots, v_n$ of vectors in $\mathbb{R}^m$ with $\|v_i\|_\infty \leq 1$, there exists a sequence $\varepsilon_1, \ldots, \varepsilon_n$, $\varepsilon_i \in \{+1, -1\}$ so that*

$$\left\|\sum_{i=1}^{t} \varepsilon_i v_i\right\|_\infty \leq K\sqrt{m} \quad \text{for } t = 1, \ldots, n\,.$$

An infinite-dimensional version of Theorem 4.5 is the following.

Theorem 4.7 (Beck 1990). *Let $v_1, v_2, v_3, \ldots$ be infinite-dimensional vectors satisfying $\|v_i\|_\infty \leq 1$. Then there exist $\varepsilon_1, \varepsilon_2, \varepsilon_3, \ldots$; $\varepsilon_i \in \{-1, +1\}$ so that*

$$\left|\left(\sum_{i=1}^{t} \varepsilon_i v_i\right)_j\right| \leq j^{4+o(1)}$$

for all j and t. Here v_j stands for the jth coordinate of the vector v.

Permutation of vectors. Instead of flipping the sign of vectors, we may achieve that all partial sums be small just by rearranging them. In fact, the two kinds of problems are strongly related as the following "transference lemma" of Chobayan shows.

Theorem 4.8. *Let $v_1, \ldots, v_n \in \mathbb{R}^m$ with $v_1 + v_2 + \cdots + v_n = 0$, and let $\|\cdot\|$ be an arbitrary norm in $\mathbb{R}^m$. Suppose that for every permutation $\pi = (i_1, i_2, \ldots, i_n)$ of $\{1, 2, \ldots, n\}$ there exist $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_n \in \{-1, +1\}$ (depending on π) such that*

$$\max_{1 \leq t \leq n} \left\|\sum_{j=1}^{t} \varepsilon_j v_{i_j}\right\| \leq A\,.$$

Then there is a permutation $\pi^* = (l_1, l_2, \ldots, l_n)$ of $\{1, 2, \ldots, n\}$ such that

$$\max_{1 \leq t \leq n} \left\|\sum_{j=1}^{t} v_{l_j}\right\| \leq A\,.$$

Proof. Let

$$B = \min_{\pi=(i_1,\ldots,i_n)} \max_{1\leq t\leq n} \left\| \sum_{j=1}^{t} v_{i_j} \right\| .$$

We have to show that $B \leq A$. Let $\pi^* = (l_1, l_2, \ldots, l_n)$ denote the permutation where the minimum is attained. By the hypothesis of the theorem, there exist $\varepsilon_1^*, \ldots, \varepsilon_n^* \in \{-1, +1\}$ such that

$$\left\| \sum_{j=1}^{t} \varepsilon_j^* v_{l_j} \right\| \leq A \quad \text{for all } 1 \leq t \leq n .$$

Let

$$M^+ = \{1 \leq j \leq n : \varepsilon_j^* = +1\} , \qquad M^- = \{1 \leq j \leq n : \varepsilon_j^* = -1\} .$$

We have

$$\sum_{j=1}^{t} v_{l_j} + \sum_{j=1}^{t} \varepsilon_j^* v_{l_j} = 2 \sum_{\substack{j\in M^+ \\ 1\leq j\leq t}} v_{l_i} ,$$

and

$$\sum_{j=1}^{t} v_{l_j} - \sum_{j=1}^{t} \varepsilon_j^* v_{l_j} = 2 \sum_{\substack{j\in M^- \\ 1\leq j\leq t}} v_{l_j} .$$

Hence

$$\left\| \sum_{\substack{j\in M^+ \\ 1\leq j\leq t}} v_{l_j} \right\| \leq \frac{A+B}{2} ,$$

and

$$\left\| \sum_{\substack{j\in M^- \\ 1\leq j\leq t}} v_{l_j} \right\| \leq \frac{A+B}{2} .$$

Setting $M^+ = \{p_1 < p_2 < \cdots < p_r\}$ and $M^- = \{q_1 < q_2 < \cdots < q_s\}$, we define the permutation

$$\pi^{**} = (p_1, p_2, \ldots, p_r, q_s, q_{s-1}, \ldots, q_2, q_1) ,$$

which we also denote by $(h_1, \ldots, h_n)$. It follows from the assumption $v_1 + v_2 + \cdots + v_n = 0$ that

$$\max_{1\leq t\leq n} \left\| \sum_{j=1}^{t} v_{h_j} \right\| \leq \frac{A+B}{2} .$$

Since B was the minimum, we must have $B \leqslant (A+B)/2$, and the desired inequality $B \leqslant A$ follows. $\square$

Combining Theorems 4.5 and 4.7 with Chobanyan's transference lemma, we get the following result.

Corollary 4.9 (Bárány and Grinberg 1981). *Let $v_1, \ldots, v_n$ be n vectors in $\mathbb{R}^m$ with $\|v_i\| \leqslant 1$ where $\|\cdot\|$ is any norm in $\mathbb{R}^m$. Assume that $v_1 + v_2 + \cdots + v_n = 0$. Then there exists a permutation $v_{i_1}, v_{i_2}, \ldots, v_{i_n}$ of the vectors v_i such that*

$$\max_{1 \leqslant t \leqslant n} \left\| \sum_{j=1}^{t} v_{i_j} \right\| \leqslant 2m .$$

Corollary 4.10. *Let $v_1, \ldots, v_n$ be infinite-dimensional vectors satisfying $\|v_i\|_\infty \leqslant 1$ $(1 \leqslant i \leqslant n)$ and $v_1 + v_2 + \cdots + v_n = 0$. Then there exists a permutation v_{i_1}, $v_{i_2}, \ldots, v_{i_n}$ of the vectors v_i such that*

$$\left| \max_{1 \leqslant t \leqslant n} \left(\sum_{j=1}^{t} v_{i_j} \right)_l \right| \leqslant l^{4+o(1)}$$

for all $l \geqslant 1$.

5. Arithmetic progressions

A structure whose discrepancy properties have been extensively investigated is the family of arithmetic progressions. We have seen Roth's theorem 1.2 and Van der Waerden's theorem 1.3, showing the two sides of (qualitatively) the same phenomenon: If we focus on the short arithmetic progressions, we get a monochromatic one; if we focus on longer arithmetic progressions, a weaker preponderance phenomenon (large discrepancy) can be asserted.

Van der Waerden's theorem and related results on arithmetic progressions are discussed in chapter 25. Here we treat the ramifications of Roth's theorem 1.2. Let us reformulate it in the language introduced above. Let $\mathscr{H}_n$ denote the hypergraph formed by the arithmetic progressions in $\{1, \ldots, n\}$. Then

Theorem 5.1. $\mathscr{D}(\mathscr{H}_n) > cn^{1/4}$.

Proof. Let $k = \lfloor \sqrt{n/6} \rfloor$. We show that the arithmetic progression can be chosen of length k and of difference at most $6k$. Let us allow, however, also "wrapped" arithmetic progressions, i.e., subsets of $\{1, \ldots, n\}$ that arise from an arithmetic progression of length k and difference at most $6k$ by reduction modulo n. By the choice of k, every "wrapped" progression is the union of two "proper" arithmetic progressions, and hence it suffices to prove that if $\mathscr{H}$ is the hypergraph formed by "wrapped" arithmetic progressions, then $\mathscr{H}$ has discrepancy at least $\frac{1}{10}n^{1/4}$. Note that $m = |\mathscr{H}| = 6kn$.

Let M be the incidence matrix of $\mathscr{H}$. By Theorem 2.8(i), it suffices estimate $\lambda_{\min}(M^{\mathrm{T}}M)$ from below.

Now the matrix $M^{\mathrm{T}}M$ is a circulant (this is where wrapping is needed!), and hence we know that its eigenvectors are $(1, \epsilon, \epsilon^2, \ldots, \epsilon^{n-1})^{\mathrm{T}}$, where ϵ is an nth root of unity. The corresponding eigenvalues are

$$\lambda(\epsilon) = \frac{1}{n} \sum_{A \in \mathscr{H}} \left| \sum_{j \in A} \epsilon^j \right|^2 .$$

Note that for each arithmetic progression A, there are $n-1$ others (its translates) that give the same contribution. So we may just select arithmetic progressions starting at 0:

$$\lambda(\epsilon) = \sum_{d=1}^{6k} \left| \sum_{t=0}^{k-1} \epsilon^{td} \right|^2 .$$

By the pigeon hole principle we can find a d_0, $1 \leqslant d_0 \leqslant k$ such that

$$-\pi/(3k) \leqslant \arg(\epsilon^{d_0}) \leqslant \pi/(3k) .$$

Then $\operatorname{Re} \epsilon^{td_0} \geqslant \frac{1}{2}$ for $1 \leqslant t \leqslant k-1$, and hence

$$\lambda(\epsilon) \geqslant \left| \sum_{t=0}^{k-1} \epsilon^{td_0} \right|^2 \geqslant \left(\operatorname{Re} \sum_{t=0}^{k-1} \epsilon^{td} \right)^2 \geqslant \frac{k^2}{4} .$$

Thus

$$\mathscr{D}(\mathscr{H}) \geqslant \frac{1}{\sqrt{m}} \mathscr{D}_2(\mathscr{H}) \geqslant \left(\frac{n}{m} \lambda_{\min} \right)^{1/2} \geqslant \left(\frac{k}{24} \right)^{1/2} > \tfrac{1}{10} n^{1/4} . \qquad \square$$

Note that we have actually proved a stronger, l_2 norm version. This gives the following information about the difference d of the arithmetic progressions of large discrepancy.

Corollary 5.2 (Roth). *Given any 2-coloring $f: \mathbb{N} \to \{-1, +1\}$ of the natural numbers, for infinitely many values of d, there is an arithmetic progression $P = P(d)$ of difference d such that*

$$\left| \sum_{k \in P(d)} f(k) \right| > c\sqrt{d} .$$

Roth conjectured that the exponent $\frac{1}{4}$ of N in Theorem 1.2 can be improved to $\frac{1}{2}$ (which corresponds to the random 2-coloring). This was disproved by Sárközy (1973). Beck (1981b) proved that Roths's lower bound is nearly sharp, by a combinatorial argument based on Theorem 2.5.

Theorem 5.3.* $\mathscr{D}(\mathscr{H}_n) < c \cdot n^{1/4} \cdot (\log n)^3$.

Proof. For integers satisfying $i \leqslant j$, let

$$\mathrm{AP}(a, d, i, j) = \{a + k \cdot d : i \leqslant k \leqslant j\} ,$$

i.e., $\mathrm{AP}(a, d, i, j)$ denotes the arithmetic progression with difference d, starting from $(a + i \cdot d)$ and terminating at $(a + j \cdot d)$. We shall say that an arithmetic progression is special if it is of the type

$$\mathrm{AP}(b, d, i \cdot 2^s, (i+1) \cdot 2^s - 1) ,$$

where $d \geqslant 1$, $1 \leqslant b \leqslant d$, $i \geqslant 0$ and $s \geqslant 0$. Let $\mathscr{H}_n^*$ denote the family of special arithmetic progressions contained in $\{1, 2, \ldots, n\}$. By definition,

$$\begin{aligned} \Delta(\{A \in \mathscr{H}_n^* : |A| \geqslant M\}) &= \max_{1 \leqslant k \leqslant n} |\{A \in \mathscr{H}_n^* : |A| \geqslant M \text{ and } k \in A\}| \\ &\leqslant \max_{1 \leqslant k \leqslant n} \sum_{1 \leqslant d \leqslant \frac{n-1}{M-1}} \sum_{\substack{1 < b < d \\ b \equiv k \pmod d}} \sum_{\substack{s \\ 2^s \geqslant M \\ b + (2^s - 1)d \leqslant n}} 1 . \end{aligned}$$

Simple calculation shows that the innermost sum is at most $c \cdot \log(n/(d \cdot M))$. It follows that

$$\begin{aligned} \Delta(\{A \in \mathscr{H}_n^* : |A| \geqslant M\}) &\leqslant c \cdot \max_{1 \leqslant k \leqslant n} \sum_{1 \leqslant d \leqslant \frac{n-1}{M-1}} \sum_{\substack{1 \leqslant b \leqslant d \\ b \equiv k \pmod d}} \log\left(\frac{n}{d \cdot M}\right) \\ &= c \cdot \sum_{1 \leqslant d \leqslant \frac{n-1}{M-1}} \log\left(\frac{n}{d \cdot M}\right) \leqslant c_1 \cdot \frac{n}{M} . \end{aligned}$$

Now we apply Theorem 2.5 to $\mathscr{H}_n^*$ with $M = D = \lceil (c_1 n)^{1/2} \rceil$. Then we obtain

$$\mathscr{D}(\mathscr{H}_n^*) < c_2 \cdot n^{1/4} \cdot (\log n)^2 .$$

We claim that

$$\mathscr{D}(\mathscr{H}_n) \leqslant (2 \log_2 n) \cdot \mathscr{D}(\mathscr{H}_n^*) .$$

To see this, first observe that any arithmetic progression $a, a + d, \ldots, a + l \cdot d$ in $[1, n]$ is representable in the form

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

where $a = b + (p_2 + 1)d$, $1 \leqslant b \leqslant d$ and $p_1 = p_2 + 1 + l$. Moreover, both $\mathrm{AP}(b, d, 0, p_i)$ $(i = 1, 2)$ are disjoint unions of not more than $\log_2 n$ special

* Very recently Matousek and Spencer (1994) cancelled the factor $(\log n)^3$. The new idea is a clever application of a lemma of Haussler. See also Matousek (1994).

arithmetic progressions, i.e., elements of $\mathcal{H}_n^*$. Hence the "best" 2-coloring of $\mathcal{H}_n^*$ gives a 2-coloring of $\mathcal{H}_n$ with discrepancy at most $(2\log_2 n)$ times as large. □

The following result is a sort of converse of Corollary 5.2.

Theorem 5.4 (Beck and Spencer 1984a). *Let n be a positive integer. Then there exists a 2-coloring $f: \mathbb{N} \to \{-1, +1\}$ of the natural numbers such that for any arithmetic progression $P = P(d) = \{a, a+d, a+2d, \ldots\}$ of difference $d \leq n$ and of arbitrary length,*

$$\left|\sum_{k\in P(d)} f(k)\right| < c \cdot \sqrt{d} \cdot (\log n)^{3.5} \quad (1 \leq d \leq n) .$$

Unfortunately, we cannot prove that Theorem 5.4 is true with the right-hand side replaced by $d^{(1/2)+o(1)}$. As an upper bound depending only on the difference d of the progression, the weaker estimate $d^{8+o(1)}$ immediately follows from Theorem 4.7.

There is still no answer to the following old conjecture of P. Erdős (worth of $\geq \$500$).

Conjecture 5.5. For any $f: \mathbb{N} \to \{-1, +1\}$ and for every constant C there are a d and n so that

$$\left|\sum_{k=1}^{n} f(k \cdot d)\right| > C .$$

In other words, the family of arithmetic progressions with first term 0 has unbounded discrepancy.

6. Measure theoretic discrepancy

We find the roots of discrepancy theory in number theory, in the theory of uniformly distributed sequences, and we give a brief introduction to this theory. (For the general theory of uniformly distributed sequences see the book of Kuipers and Niederreiter 1974.)

The field originated with the celebrated paper of Weyl (1916), which was intended to furnish a deeper understanding of the results in diophantine approximation and to generalize some basic results in this field. At the beginning of this century, due to the work of Ostrowski, Hecke, Hardy, Littlewood, and others, it became clear that the approximability properties of an irrational α by rationals depends on the partial quotients (the "digits" a_k) in its continued fraction expansion

$$\alpha = \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cdots}} .$$

It became also clear that the approximability property of α is closely related to the distribution of the sequence $(\{n\alpha\})$ in $[0, 1)$. ($\{x\}$ stands for the fractional part of the real number x.)

For every irrational α, the sequence $(\{n\alpha\})$ is everywhere dense in $[0, 1)$. The fact that it is *uniformly distributed* expresses a stronger property. Let us give the definition for arbitrary dimension.

Let $\omega = (u_n)$, $n \in \mathbb{N}$ be a sequence in the k-dimensional unit cube $[0, 1)^k$. Let $B(a, b) = \prod_{i=1}^{k} [a_i, b_i)$ be an aligned box in $[0, 1)^k$, and $\mathcal{B}$, the family of all such boxes. $Z(B; N)$ will denote the number of v with $u_v \in B$, $1 \leqslant v \leqslant N$. Let $R([0, 1]^k)$ denote the set of Riemann-integrable functions on $[0, 1]^k$.

Definition 6.1. The sequence $\omega = (u_n)$, $n \in \mathbb{N}$ is said to be uniformly distributed in $[0, 1)^k$ if for every aligned box $B \subset [0, 1)^k$

$$\lim_{N\to\infty} \frac{1}{N} Z(B; N) = \mu(B)$$

(here μ stands for the usual k-dimensional Lebesgue measure). Note that it would suffice to consider only boxes $B(b) = B(0, b)$, since the characteristic function of every other box can be obtained by adding and subtracting the characteristic functions of at most 2^k of these special boxes.

Equivalent definitions are given by the following.

Theorem 6.2. *For a sequence* (u_n) *in* $[0, 1)^k$, *the following are equivalent*:

(i) (u_n) *is uniformly distributed in* $[0, 1)^k$.

(ii) *For every* $f \in R([0, 1]^k)$,

$$\lim_{N\to\infty} \frac{1}{N} \sum_{n=1}^{N} f(u_n) = \int_{[0,1]^k} f(x)\, \mathrm{d}x .$$

(iii) (Weyl's criterion) *For every integer point* $z \in \mathbb{Z}^k \setminus \{0\}$,

$$\lim_{N\to\infty} \frac{1}{N} \sum_{n=1}^{N} \mathrm{e}^{2\pi \mathrm{i} z^{\mathrm{T}} u_n} = 0 .$$

Condition (ii) indicates why uniformly distributed sequences are important in the theory of numerical integration. Observe that we obtain an equivalent condition if we assume that (ii) holds for a dense subset of $R([0, 1]^k)$, and Weyl's criterion is obtained by postulating (ii) for the functions $\mathrm{e}^{2\pi \mathrm{i} z^{\mathrm{T}} x}$ (and consequently for all linear combinations of these). (This also suggests how the concept of uniformly distribution sequences can be generalized to topological groups.)

As an illustration, we derive from Weyl's criterion the following improvement on the classical Kronecker theorem.

Corollary 6.3 (Weyl 1916). *Suppose that* $\alpha_1, \ldots, \alpha_k$ *are real numbers such that* 1,

$\alpha_1, \ldots, \alpha_k$ are linearly independent over the rationals. Then the sequence

$$u_n = (\{n\alpha_1\}, \ldots, \{n\alpha_k\}), \quad n \in \mathbb{N}$$

is uniformly distributed in $[0,1)^k$.

Proof. Let $m = (m_1, \ldots, m_k) \in \mathbb{Z}^k \setminus \{0\}$. Then

$$\sum_{n=1}^{N} e^{2\pi i m^{\mathrm{T}} u_n} = \sum_{n=1}^{N} e^{2\pi i n y},$$

where $y = m_1\alpha_1 + m_1\alpha_2 + \cdots + m_k\alpha_k$. Observe that y is irrational by the hypothesis, and hence $e^{2\pi i y} \neq 1$. Therefore,

$$\left|\sum_{n=1}^{N} e^{2\pi i n y}\right| = \left|e^{2\pi i y} \cdot \frac{1 - e^{2\pi i N y}}{1 - e^{2\pi i y}}\right| \leqslant \frac{2}{|1 - e^{2\pi i y}|} = O(1).$$

Thus Weyl's criterion is satisfied. □

It is easy to see that the sequence $\omega = (u_n)$, $n \in \mathbb{N}$ is uniformly distributed in $[0,1)^k$ iff

$$\sup_{\substack{B \subset [0,1)^k \\ \text{aligned box}}} |Z(B, N) - N \cdot \mu(B)| = o(N).$$

But how small can $o(N)$ be? To handle this question, put

$$\mathscr{D}_N(B) = Z(N; B) - N|B|,$$
$$\mathscr{D}_N = \sup_{\substack{B \subset [0,1]^k \\ \text{aligned box}}} |\mathscr{D}_N(B)|;$$

and

$$\mathscr{D}_N^p = \left(\int_{[0,1]^k} |\mathscr{D}_N(B(0,x))|^p \, dx\right)^{1/p}.$$

(Warning: this is *not* the pth power of $\mathscr{D}_N$.)

$\mathscr{D}_N$ and $\mathscr{D}_N^p$ measure (in different norms) the discrepancy of the sequence $u_1, \ldots, u_N$, and their behavior for $N \to \infty$ measures the irregularity of the distribution of the infinite sequence (u_N). In the quantitative theory of uniform distribution, a central problem is the investigation of the order of magnitude of the discrepancy functions $\mathscr{D}_N^p$ and $\mathscr{D}_N$.

The quantitative theory started with the conjecture of Van der Corput (1935a), asserting that for an arbitrary sequence in $[0,1)$, $\sup_N \mathscr{D}_N = \infty$. This was proved by Van Aardenne-Ehrenfest (1945) who showed that for an arbitrary sequence (u_n)

for infinitely many N,

$$\mathscr{D}_N > c(\log\log N)(\log\log\log N)^{-1}.$$

Roth (1954) strengthened this result.

Theorem 6.4. (i) *For an arbitrary infinite sequence* (u_n) *in* $[0,1]^k$ *and for every* $N > N_0$,

$$\max_{1\leq n\leq N} \mathscr{D}_n^2 > c_k(\log N)^{k/2}.$$

(ii) *For* N *arbitrary points* $u_1, \ldots, u_N$ *in* $[0,1]^k$,

$$\mathscr{D}_N^2 > c'_k(\log N)^{(k-1)/2}.$$

(Here c_k, c'_k are positive constants depending only on k.)

For $k=2$ (Davenport 1956) and for $k \geq 3$ (Roth 1979, 1980) it is proved that (apart from a multiplicative constant) these results are sharp.

The problem of finding bounds for the discrepancy in the supremum norm is more difficult. Since $\mathscr{D}_N \geq \mathscr{D}_N^2$, the preceding results give some lower bounds on $\mathscr{D}_N$. For infinite sequences sharp results are known only for $k=1$, for finite sequences for $k=2$; the latter is a reformulation of Theorem 1.1.

Theorem 6.5 (Schmidt 1972). (i) *For an arbitrary infinite sequence* (u_n) *in* $(0,1)$ *and for every* $N \geq 2$,

$$\max_{1\leq n\leq N} \mathscr{D}_N > c\log N.$$

(ii) *For arbitrary* N *points* $U = \{u_1, \ldots, u_N\} \subseteq [0,1)^2$,

$$\mathscr{D}_N > c''\log N.$$

(Here c, c' are positive absolute constants.)

This result is best possible apart from the multiplicative constant. If $u_n = \{n\alpha\}$ where α is an irrational number of bounded partial quotients ($a_k \leq K$, $k = 1, 2, \ldots$), then for every N, $\mathscr{D}_N < c_K \log N$. Similarly, for the N points $u_n = \{\{n\alpha\}, n/N\}$ $(1 \leq n \leq N)$ in $[0,1]^2$, $\mathscr{D}_N < c_K \log N$.

There is a "transference principle" between *sequences* in $[0,1)^k$ and *sets* in $[0,1)^{k+1}$ (showing that parts (i) and (ii) in both Theorems 6.4 and 6.5 are equivalent). This is given by the following construction.

(1) For a finite sequence $u_1, \ldots, u_N$ in $[0,1)^k$, take the set

$$\left\{\left(u_n, \frac{n-1}{N}\right) \in [0,1)^{k+1} : 1 \leq n \leq N\right\}.$$

(2) Let $v_n \in [0,1)^{k+1}$, $1 \leq n \leq N$ be N points. Write $v_n = (u_n, y_n)$ where $u_n \in [0,1)^k$ and $y_n \in [0,1)$. Arrange the last coordinates y_n, $1 \leq n \leq N$ in increasing order $y_{i_1} \leq y_{i_2} \leq \cdots \leq y_{i_N}$. Take the sequence $u_{i_1}, \ldots, u_{i_N}$ in $[0,1)^k$.

In both cases the discrepancies are the same up to a universal constant factor.

All known proofs of the fundamental Theorem 6.5 are rather hard. We sketch here a proof due to Halász (1981).

Proof of Theorem 6.5. We prove (ii). Given any $x = (x_1, x_2) \in [0, 1]^2$, let

$$\mathscr{Z}(x) = |U \cap B(x)| ,$$

and

$$\mathscr{D}(x) = \mathscr{Z}(x) - Nx_1x_2 .$$

We shall construct an auxiliary function $F(x)$ such that

$$\left|\int_{[0,1]^2} F(x)\mathscr{D}(x)\,\mathrm{d}x\right| > c_1 \log N , \tag{6.6}$$

and

$$\int_{[0,1]^2} |F(x)|\,\mathrm{d}x \leqslant 2 . \tag{6.7}$$

These yield

$$\mathscr{D}_N \geqslant \max_x |\mathscr{D}(x)| \geqslant \tfrac{1}{2}c_1 \log n ,$$

and Theorem 6.5 follows.

Any $x \in [0, 1]$ can be written uniquely in the binary form

$$x = \sum_{j=0}^{\infty} \beta_j(x)2^{-j-1} ,$$

where $\beta_j(x) = 0$ or 1 and the sequence $\beta_j(x)$ does not end with $1, 1, 1, \ldots$. For $m = 0, 1, 2, \ldots$ let

$$R_m(x) = (-1)^{\beta_m(x)}$$

(Rademacher function). Let $m = (m_1, m_2)$ be a pair of nonnegative integers. Let $\|m\| = m_1 + m_2$ and writing $x = (x_1, x_2)$, let

$$R_m(x) = R_{m_1}(x_1) \cdot R_{m_2}(x_2) .$$

By an m-box we mean a set of the form

$$[n_1 \cdot 2^{-m_1}, (n_1 + 1) \cdot 2^{-m_1}] \times [n_2 \cdot 2^{-m_2}, (n_2 + 1)2^{-m_2}] .$$

For any m-box A let

$$f_m(x) = \begin{cases} R_m(x) , & \text{if } A \cap U = \emptyset , \\ 0 , & \text{otherwise} . \end{cases}$$

Let $2N \leq 2^n < 4N$, n integer. Let $\alpha = 2^{-6}$, and write

$$F(x) = \prod_{m:\ \|m\|=n} (1 + \alpha f_m(x)) - 1 .$$

Using the orthogonality of the modified Rademacher functions $f_m(x)$, we have

$$\int_{[0,1)^2} |F(x)|\,\mathrm{d}x \leq \int_{[0,1]^2} \Big(\prod_{\|m\|=n} (1 + \alpha f_m(x)) + 1 \Big)\,\mathrm{d}x$$

$$= \int_{[0,1)^2} \prod_{\|m\|=n} (1 + \alpha f_m(x))\,\mathrm{d}x + 1 = 1 + 1 = 2 .$$

Note that

$$F(x) = \alpha F_1(x) + \sum_{j=2}^{n+1} \alpha^j F_j(x) ,$$

where

$$F_1(x) = \sum_{\|m\|=n} f_m(x) ,$$

and for $j = 2, \ldots, n+1$

$$F_j(x) = \sum_{\substack{\|m_1\| = \cdots = \|m_j\| = n \\ m_k \neq m_l \text{ if } k \neq l}} f_{m_1}(x) \cdots f_{m_j}(x) .$$

It is not hard to prove that for every m satisfying $\|m\| = n$, we have

$$\int_{[0,1]^2} f_m(x) \mathscr{L}(x)\,\mathrm{d}x = 0 , \tag{6.8}$$

$$\int_{[0,1]^2} f_m(x) x_1 x_2\,\mathrm{d}x_1\,\mathrm{d}x_2 \geq (2^n - N) 2^{-2n-4} , \tag{6.9}$$

and

$$\left| \int_{[0,1]^2} F_j(x) \mathscr{D}(x)\,\mathrm{d}x \right| \leq \sum_{k=0}^{n-j+1} \sum_{l=1}^{n-k} 2^{-n-l-4} \cdot N \cdot \binom{l-1}{j-2} . \tag{6.10}$$

The proof of relations (6.8)–(6.10) is straightforward calculation.

Now we are able to complete the proof. By (6.10), we have

$$\left| \sum_{j=2}^{n+1} \alpha^j \int_{[0,1]^2} F_j(x) \mathscr{D}(x)\,\mathrm{d}x) \right| \leq \sum_{j=2}^{n+1} \sum_{k=0}^{n-j+1} \sum_{l=1}^{n-k} \alpha^j \cdot 2^{-n-l-4} \cdot N \cdot \binom{l-1}{j-2}$$

$$= N\alpha^2 \sum_{k=0}^{n-1} \sum_{l=1}^{n-k} \sum_{j=2}^{n+1} 2^{-n-l-4} \cdot \binom{l-1}{j-2} \alpha^{j-2}$$

$$\leq N \cdot \alpha^2 \sum_{k=0}^{n-1} \sum_{l=1}^{\infty} 2^{-n-l-4} (1 + \alpha)^l$$

$$\leqslant N \cdot n \cdot \alpha^2 \cdot 2^{-n-4} \sum_{l=1}^{\infty} \left(\frac{1+\alpha}{2}\right)^l$$
$$\leqslant N \cdot n \cdot \alpha^2 \cdot 2^{-n-3} .$$

Combining this with (6.8) and (6.9), we obtain

$$\left|\iint F(x)\mathscr{D}(x)\,\mathrm{d}x\right| \geqslant \left|\iint F_1(x)\mathscr{L}(x)\,\mathrm{d}x_1\,\mathrm{d}x_2\right| - \left|\sum_{j=2}^{n+1} \int_{[0,1]^2} F_j(x)\mathscr{D}(x)\,\mathrm{d}x\right|$$
$$\geqslant \alpha(n+1)N(2^n - N)\cdot 2^{-2n-4} - N\cdot n\cdot \alpha^2 \cdot 2^{-n-3}$$
$$> 2^{-15}\cdot n = c\log N ,$$

as required. □

As to the discrepancy in supremum norm, the following is a very difficult old problem.

Conjecture 6.11. For all $k \geqslant 2$ and for N arbitrary points in $[0, 1]^k$,

$$\mathscr{D}_N > c(k)(\log N)^{k-1} .$$

This would mean that the exponent $(k-1)/2$ implied by Theorem 6.4 (using $\mathscr{D}_N \geqslant \mathscr{D}_N^2$) is only half the truth. Note that the case $k=2$ is settled by Theorem 6.5. If true, Conjecture 6.6 is best possible by the Van der Corput–Halton–Hammersley sequence, see, e.g., Beck and Chen (1987). Recently Beck (1989a) improved on the old result of Roth by proving a 2-dimensional version of the Aardenne-Ehrenfest theorem, but Conjecture 6.11 appears still very difficult.

Approximation of measures. One interpretation of Theorem 6.5 is that it is impossible to approximate the Lebesgue measure on the system of rectangles "too well" with a measure of finite support. There is a more general phenomenon in the background, as proved by Chen: the same is true for arbitrary measures.

Theorem 6.12 (Chen 1984). *Let g be a Lebesgue-integrable function in E^2, and assume that $g(x) \neq 0$ on a subset $S \subseteq E^2$ with $\mu(s) > 0$. Then there exists a constant $c(g) > 0$ such that for every set U of N points in E^2 and for every function $\lambda: U \to \mathbb{R}$,*

$$\sup_{x\in E^2} \left| \sum_{u\in B(x)\cap U} \lambda(u) - N\int_{B(x)} g(x)\,\mathrm{d}\mu \right| > c(g)\log N .$$

Rectangles in the $N \times N$ lattice. It is easy to see that Schmidt's theorem 6.5 has the following corollary. Let the hypergraph $\mathscr{L}_N$ be defined on the underlying set

$S = \{0, 1, \ldots, N\}^2$ by

$$\mathscr{L}_N = \{S \cap B(a, b) \mid 0 \leq a \leq N, 0 \leq b \leq N\} .$$

Obviously $\mathscr{D}(\mathscr{L}_N) = 1$. What can be said about $\mathscr{D}_{\mathrm{D}}(\mathscr{L}_N)$, $\mathscr{D}_{\mathrm{I}}(\mathscr{L}_N)$ or $\mathscr{D}_{\mathrm{H}}(\mathscr{L}_N)$? It follows easily from Theorem 6.5 that with a positive constant $c > 0$

$$\mathscr{D}_{\mathrm{D}}(\mathscr{L}_N) > c \log N .$$

Hence by Theorem 3.1,

$$\mathscr{D}_{\mathrm{H}}(\mathscr{L}_N) \geq \tfrac{1}{2}\mathscr{D}_{\mathrm{I}}(\mathscr{L}_N) \geq \tfrac{1}{2}\mathscr{D}_{\mathrm{D}}(\mathscr{L}_N) > c \log n .$$

A related problem concerning balanced 2-colorings of finite sets in the plane was formulated by G. Tusnády. Let $\mathscr{P}$ be an N-element point set on the plane. Let $T = T(\mathscr{P})$ be the least integer t such that one can assign ± 1s to the points of P so that the sum of these values in any rectangle with sides parallel to the coordinate axes has absolute value at most T. Now Tusnády's problem is to determine

$$T_N = \max_{|\mathscr{P}| = N} T(\mathscr{P}) .$$

The following theorem gives the best known bounds; the lower bound is due to Beck (1981a), the upper is a recent result of Bohus (1990), improving a result of Beck.

Theorem 6.13. *For* $N \geq 2$,

$$c_1 \cdot \log N < T_N < c_2 \cdot (\log N)^3 .$$

Proof. We give the proof of Beck's upper bound of $(\log N)^4$ as an application of Theorem 2.2. It suffices to prove the following. Let $A = (a_{ij})$, where $a_{ij} = 0$ or 1, be a matrix of size $N \times N$. Then there exist "signs" $\varepsilon_{ij} \in \{-1, +1\}$ such that

$$\left| \sum_{i=1}^{n} \sum_{j=1}^{m} \varepsilon_{ij} a_{ij} \right| < c(\log N)^4 \tag{6.14}$$

for all $1 \leq n$, $m \leq N$.

We now prove (6.14). Adding a few 0-rows and 0-columns if necessary, we may assume that $N = 2^l$ where l is an integer. For every pair (p, q) of integers satisfying $0 \leq p, q \leq l$, we partition A into 2^{p+q} submatrices, splitting the horizontal side of the matrix into 2^p equal pieces and the vertical side of the matrix into 2^q equal pieces. There are $(l+1)^2 \approx (\log N)^2$ partitions. Let us call a submatrix of A special if it occurs in one of these partitions. Let $S = \{(i, j)\colon a_{ij} = 1\}$, and let us associate with every submatrix B the subset

$$Y_B = \{(i, j)\colon a_{ij} \text{ belongs to } B, a_{ij} = 1\} .$$

Let

$$\mathcal{H} = \{Y_B\colon B \text{ is a special submatrix of } A\}\ .$$

Since the maximum degree $\Delta(\mathcal{H}) \le (l+1)^2$, by Theorem 2.2 there exists an assignment of ± 1s so that the absolute value of the sum of the signed entries in each of the special submatrices is less than $2\Delta(\mathcal{H}) \le 2(l+1)^2$. Note, however, that any submatrix of A containing the lower corner A is the union of at most l^2 disjoint special submatrices. Thus (6.14) follows.

The proof of the lower bound depends on Theorems 3.1 and 6.5. We may clearly assume that $N = n^2$, n integer. We need the following reformulation of Theorem 6.5:

Let P be an arbitrary finite set in the square $[0, y)^2$, $y > 1$. There exists an aligned rectangle $A \subset [0, y)^2$ such that

$$\big||P \cap A| - \mu(A)\big| > c \cdot \log y\ .$$

We shall use that for any convex set $A \subset [0, n)^2$, we have

$$|A \cap \mathbb{Z}^2| = \mu(A) + \mathrm{O}(n)\ .$$

Let $S = [0, n)^2 \cap \mathbb{Z}^2$, $\mathcal{H} = \{S \cap A\colon A \subset [0, n)^2 \text{ aligned rectangle}\}$ and $q = 1 - 2 \cdot n^{-1}$. Let $\varepsilon(s) \in \{-1, +1\}$ $(s \in S)$ be fixed such that

$$\mathcal{D}(\mathcal{H}; q) = \max_A \Big| \sum_{s \in S \cap A} (\varepsilon(s) - q) \Big|\ ,$$

and let $S^- = \{s \in S\colon \varepsilon(s) = -1\}$. Then we have

$$\begin{aligned}\mathcal{D}(\mathcal{H}; q) &= 2 \max_A \Big| |S^- \cap A| - \frac{1}{n} |A \cap \mathbb{Z}^2| \Big| \\ &\ge 2 \max_A \Big| |S^- \cap A| - \frac{1}{n} \mu(A) \Big| + \mathrm{O}(1)\ .\end{aligned}$$

Apply a contraction of linear ratio $n^{-1/2} : 1$, and apply the reformulation of Schmidt's theorem given above to the resulting set. We obtain that

$$\mathcal{D}(\mathcal{H}; q) \ge 2c \cdot \log(n^{1/2}) - \mathrm{O}(1) \ge c \log N\ .$$

Thus by Theorem 3.1,

$$\mathcal{D}_{\mathrm{H}}(\mathcal{H}) \ge \tfrac{1}{2} \mathcal{H}_{\mathrm{I}}(\mathcal{H}) \ge \tfrac{1}{2} \mathcal{D}(\mathcal{H}; q) \ge c_2 \cdot \log N\ .$$

In other words,

$$\mathcal{D}(\mathcal{H}_Z) \ge c_2 \cdot \log N$$

for some $Z \subset S$. Since $|Z| \le |S| = n^2 = N$, we have

$$T_N \ge T_{|Z|} \ge \mathcal{D}(\mathcal{H}_Z) \ge c_2 \cdot \log N\ . \qquad \square$$

Let $X = \{(i, j): a_{ij} = 1\}$, $\mathscr{H}$ be the family of submatrices of A containing the lower left corner of A, $\mathscr{G}$ be the family of special submatrices, $N = 2^l$, $D = (l + 1)^2$, $K = l^2$. Applying Theorem 2.7, we obtain the following modest improvement on (6.14):

$$\left|\sum_{i=1}^{n} \sum_{j=1}^{m} \varepsilon_{ij} a_{ij}\right| < c(\varepsilon) \cdot (\log N)^{(7/2)+\varepsilon}$$

for all $1 \leqslant n,\ m \leqslant N$.

In higher dimensions, however, the improvement given by Theorem 2.7 becomes significant. Repeating the proof of 6.13 in higher dimensions, we get the following result:

Let $A = (a_n)$ $(n \in \{1, \ldots, N\} \times \cdots \times \{1, \ldots, N\})$ be a k-dimensional matrix with entries $a_n = 0$ or 1. Then there exist "signs" $\varepsilon_n \in \{-1, +1\}$ such that

$$\left|\sum_{n:\, n \leqslant m} \varepsilon_n a_n\right| \leqslant c(k) \cdot (\log N)^{2k}$$

for all $m = (m_1, m_2, \ldots, m_k)$ satisfying $1 \leqslant m_1, \ldots, m_k \leqslant N$. Applying Theorem 2.7 we obtain, however, the following better bound:

$$\left|\sum_{n:\, n \leqslant m} \varepsilon_n a_n\right| < c(k, \varepsilon) \cdot (\log N)^{k+(3/2)+\varepsilon} ,$$

for all m as above. We have strong indications that the true order of magnitude is probably about $(\log N)^{k-1}$.

In contrast to the case of Theorem 2.2, when the proof gives a polynomially computable algorithm to construct the desired signs $\varepsilon_i = \pm 1$, the proofs of Theorems 2.5 and 2.7 imply only the *existence* of balanced 2-colorings.

7. Geometric structures

In this section we discuss a variety of questions where the underlying set S is either the k-dimensional unit cube $[0, 1]^k$ or (in the discrete version) the $N \times N \times \cdots \times N$ lattice.

We study generalizations of the classical problem considered in Theorem 1.1. We no longer restrict ourselves to the boxes: we allow rotation, and we also study more general shapes. Many problems of this type originated with the paper of Erdős (1964).

Let $\mathscr{A}$ be a family of simple geometric objects, as aligned or tilted rectangles, triangles, balls, etc., in R^k. Let $P \subseteq [0, 1]^k$ be a set of N points. Set

$$\mathscr{D}_N(\mathscr{A}) = \inf_{|P|=N} \sup_{A \in \mathscr{A}} \big||A \cap P| - N\mu(A \cap [0, 1]^k)\big| .$$

We consider first the case of aligned right triangles.

Theorem 7.1 (Schmidt 1969). *Let $P_1, \ldots, P_N$ be N points in the unit square $[0, 1]^2$. Then there exists a right triangle $T \subset [0, 1)^2$ with two sides parallel to the coordinate axes, and with*

$$||P \cap T| - N \cdot \mu(T)| > N^{(1/4)-\varepsilon} .$$

Beck (1984a, 1987a) slightly improved the lower bound and also proved that the lower bound is nearly sharp.

Theorem 7.1′. *Let $\mathcal{A}$ be the family of right triangles in the plane with two sides parallel to coordinate axes. Then*

$$c_1 N^{1/4} < \mathcal{D}_N(\mathcal{A}) < N^{1/4}\sqrt{\log N} .$$

This theorem exhibits a rather paradoxical phenomenon. Let T' be a right triangle. There is a unique right triangle T'' such that $T' \cup T''$ is an aligned rectangle A. We know that there exist N-element sets P with

$$||P \cap A| - N \cdot \mu(A)| < c \cdot \log N$$

for all aligned rectangles $A \subset [0, 1)^2$. This set contains almost the "right" number of points in $T' \cup T''$ but – by Theorem 7.1 – must be quite irregularly distributed in the two halves T' and T''.

Essentially the same proof gives the following 2-coloring result. Let f be a 2-coloring of the $N \times N$ square lattice. Then there exists an aligned right triangle T such that the difference between the number of red points and the number of blue points in T is at least $c \cdot N^{1/2}$. In other words, the corresponding hypergraph has discrepancy at least $c \cdot N^{1/2}$.

(Note that the analogous question for aligned rectangles is trivial. The chessboard type 2-coloring of $N \times N$ has deviation at most 1 for any aligned rectangle.)

Consider next the family of balls. Again we have a "large discrepancy" result (for the pioneering result, see Schmidt 1969).

Theorem 7.2 (Beck 1987a). *Let $\mathcal{A}$ be the family of balls contained in $[0, 1)^k$. Then*

$$\mathcal{D}_N(\mathcal{A}) > N^{1/2-1/2k-\varepsilon} .$$

The following result states, roughly speaking, that for rotation invariant families the discrepancy is always "large".

Theorem 7.3 (Beck 1987a). *Let $A \subset [0, 1)^k$ be a k-dimensional convex body, and let $\mathcal{A}$ be the family of convex sets obtained from A by a similarity transformation (rotation, translation, and homothetic transformation). Then*

$$\mathcal{D}_N(\mathcal{A}) > c(A, \varepsilon) \cdot N^{1/2-1/2k-\varepsilon} .$$

We remark that Theorems 7.2–7.3 are nearly best possible (see Beck 1984a).

The situation is more complicated if rotation is forbidden (as the difference between aligned right triangles and rectangles indicates). The discrepancy of the family of homothetic copies of a given convex shape A depends mainly on the smoothness of the boundary A. We have a fairly good understanding of this phenomenon (for more details, see Beck 1988 and Beck and Chen 1987).

For the discrepancy of congruent sets, see Beck (1987b). For the discrepancy of half-plances, see Beck (1983), Alexander (1990) and Matousek (1994).

It is worthwhile to mention here that all of these theorems are essentially independent of the shape of the underlying set – instead of the unit cube one can consider the unit ball, the regular simplex, any "reasonable" convex body, the surface of the unit sphere, etc.

An application in discrete geometry. For which set of N points on the unit sphere is the sum of all $\binom{N}{2}$ euclidean distances between these points maximal, and what is the maximum? Let S^k denote the surface of the unit sphere in $\mathbb{R}^{k+1}$. Let P be a set of N points on S^k. Let $|x|$ denote the usual euclidean length. We define

$$L(N, k, P) = \sum_{p,q \in P} |p - q|$$

and

$$L(N, K) = \max_{P} L(N, k, P) ,$$

where the maximum is taken over all $P \subset S^k$, $|P| = N$. The determination of $L(N, k)$ is a long-standing open problem in discrete geometry. For $k = 1$, the solution is given by the regular N-gon. It is also known that for $N = k + 2$, the regular simplex is optimal. For $N > k + 2$ and $k \geqslant 2$, the exact value of $L(N, k)$ is unknown. The reason for this is that if N is sufficiently large compared to k, then there are no "regular" configurations on the sphere, so the extremal point system(s) is (are), as expected, quite complicated and "ad hoc".

Since the determination of $L(N, k)$ seems to be hopeless, it is natural to compare the discrete sum $L(N, k, P)$ with the following integral (the solution of the "continuous relaxation" of the distance problem)

$$\frac{N^2}{2} \cdot \frac{1}{\sigma(S^k)} \int_{S^k} |p - p_0| \, \mathrm{d}\sigma(P) = c_0(k) \cdot N^2 ,$$

where σ denotes the surface area, $\mathrm{d}\sigma(P)$ represents an element of the surface area on S^k, $p_0 = (1, 0, 0, \dots, 0) \in \mathbb{R}^{k+1}$. The constants $c_0(k)$ can be calculated explicitly; e.g., $c_0(1) = 2/\pi$, $c_0(2) = \frac{2}{3}$). Stolarsky (1973) has discovered a beautiful identity saying, roughly speaking, that the discrete sum $L(N, k, P)$, plus a measure of how far the set P deviates from uniform distribution, is constant. Thus the sum of distance is maximized by a well-distributed set of points. Combining Stolarsky's identity with a result in "irregularities of distribution", one can obtain some nontrivial information on the order of magnitude of $L(N, k)$ (see Beck 1984b).

Theorem 7.4. $L(N, k) = c_0(k) \cdot N^2 + O(N^{1-(1/k)})$.

Finally, we mention the famous Heilbronn's triangle problem which is, in a broader sense, related to our topic (see Roth 1976 and Komlós et al. 1982).

8. Uniform distribution and ergodic theory

The most important class of uniformly distribution sequences in $[0, 1)$ is the class of sequences $(\{n\alpha\})$ for α irrational. These are the basic sequences in the theory of diophantine approximation. Further, these are the best "test-sequences": very often theorems which were found first for sequences $(\{n\alpha\})$ turned out to be true for more general ones. Finally we mention the relation of sequences $(\{n\alpha\})$ to topological transformations.

The discrepancy of $((n\alpha\})$ depends on the partial quotients a_k, $k = 1, 2, \ldots$ of α. For every N and $x \in [0, 1)$ there is an "explicit" formula for the discrepancy $\mathcal{D}_N([0, x))$ defined in section 6 (Sós 1974). This leads to the following bounds.

Theorem 8.1. *Let p_k/q_k be the kth convergent of α: $p_k/q_{jk} = [a_1, \ldots, a_{k-1}]$. If $q_k \leq N < q_{k+1}$ then*

$$c_1 \sum_{i=1}^{k} a_i < \max_{1 \leq n \leq N} \mathcal{D}_N < c_2 \sum_{i=1}^{k+1} a_i \, .$$

Consequently, if $a_i \leq K$, $i = 1, \ldots,$ then

$$\mathcal{D}_N < c \cdot K \cdot \log N \, .$$

Much is known about the finer properties of the distribution. Though

$$\max_{1 \leq n \leq N} \sup_{I} \mathcal{D}_n(I) > c \log N \, ,$$

there are intervals I in which the distribution is very good.

Theorem 8.2 (Hecke–Kesten). *For the sequence $(\{n\alpha\})$ and for a fixed interval I, the discrepancy $\mathcal{D}_N(I)$ remains bounded if and only if $\mu(I) = \{k\alpha\}$ for some integer k.*

The "if" part was proved by Hecke (1922) and the much deeper "only if" part by Kesten (1966). Very elegant proofs and generalizations of this theorem in the framework of ergodic theory are due to Fürstenberg et al. (1973), Halász (1976), Petersen (1973).

On the other hand it is remarkable that this theorem and further properties of $\mathcal{D}_N$ are relevant in ergodic theory (see, e.g., Herman 1976, Deligne 1975).

Schmidt investigated the analogous question for arbitrary sequences in $[0, 1)$.

Theorem 8.3 (Schmidt 1974). *For an arbitrary sequence (u_n) in $[0,1)$ the lengths of all intervals I for which $\mathscr{D}_N(I)$ remains bounded form a countable set.*

The ergodic theoretical generalization shows the essence of Kesten's theorem. Let $(\Omega, \mathscr{A}, \mu)$ be a probability space, $T:\Omega \to \Omega$ an ergodic transformation (a measure preserving transformation such that every T-invariant measurable set has measure 0 or 1). For $A \in \mathscr{A}$, $x \in \mathscr{A}$ let $Z_N^T(A;x)$ denote the number of points $T^n x \in A$, $1 \leqslant n \leqslant N$. Set

$$\mathscr{D}_N^T(A;x) = |Z_N^T(A;x) - N\mu(A)|\,.$$

By Birkhoff's ergodic theorem, for every fixed $A \in \mathscr{A}$, for almost all $x \in \Omega$,

$$\frac{1}{N}\mathscr{D}_N^T(A;x) \to 0 \quad \text{if } N \to \infty\,.$$

The uniformity or irregularity of the distribution of the orbit is measured by the sequence $\mathscr{D}_N^T(A;x)$. Fürstenberg et al. (1973), Petersen (1973), Halász (1976) proved the following very striking generalization of Kesten's theorem.

Theorem 8.4. *If for some $A \in \mathscr{A}$, $\mathscr{D}_N^T(A;x)$ is bounded on a set $X \subset \Omega$ of positive measure, then $\mathrm{e}^{2\pi \mathrm{i}\mu(A)}$ is an eigenvalue of T; that is, there exists a function $g \not\equiv 0$ such that*

$$g(Tx) = \mathrm{e}^{2\pi \mathrm{i}\mu(A)} g(x) \quad \textit{for } x \in \Omega\,.$$

Conversely, for every eigenvalue $e^{2\pi i \mu}$ there exists an $A \in \mathscr{A}$ such that $\mu(A) = \mu$ and $\mathscr{D}_N^T(A;x)$ remains bounded as $N \to \infty$ for almost all $x \in \Omega$.

Remark. Kesten's theorem follows from Theorem 8.4. To see this, let $\Omega = \mathbb{R}/\mathbb{Z}$. Let $R_\alpha : x \to x + \alpha \pmod 1$ be the rotation by $2\pi\alpha$). The eigenvalues of R_α are the numbers $\mathrm{e}^{2\pi \mathrm{i}\{k\alpha\}}$; hence Kesten's theorem follows.

We give another example of the relationship between uniform distribution and ergodic theory, illustrating how results on distribution of the sequences $(\{n\alpha\})$ imply general results on homeomorphisms of the circle.

Denjoy (1932) proved that for every homeomorphism $T: \mathbb{R}/\mathbb{Z} \to \mathbb{R}/\mathbb{Z}$ having no periodic point there exists an irrational $\alpha(T) \in (0,1)$ such that T is conjugate to the rotation R_α. By this result, the distribution of $T^n x$, $n = 1, 2,, \ldots,$ is determined by the distribution of the sequence $(\{n\alpha\})$. In particular,

(a) By Birkhoff's ergodic theorem the discrepancy $\mathscr{D}_N^T(I;x) = \mathrm{o}(N)$. By Denjoy's theorem we know much more: $\mathscr{D}_N^T(I;x)$ is the same as the corresponding discrepancy of the sequence $(\{n\alpha(T)\})$.

(b) The order of points $\{n\alpha\}$, $1 \leqslant n \leqslant N$ is very restricted: if π is the permutation determined by $\{\pi(1)\alpha\} < \cdots < \{\pi(N)\alpha\}$, then, for example, for every fixed α and N the difference $\pi(i) - \pi(i-1)$ takes at most three different values. Now, by Denjoy's theorem the same holds for an arbitrary homeomorphism T having no periodic point and every point x, if we define the permutation π by $T^{\pi(1)}(x) < T^{\pi(2)}(x) < \cdots < T^{\pi(N)}$. (See Sós 1957, Swierczkowski 1958.)

One of the most fascinating and deepest relationships between combinatorics and ergodic theory is given by Fürstenberg. Since there is a recent expository paper by Fürstenberg et al. (1982), and the book of Fürstenberg (1981), we do not go into the discussion of this. We mention only the fascinating recent result of Fürstenberg and Katznelson (1989) on the density version of the Hales–Jewitt theorem (see chapter 25).

9. More versions of discrepancy

Strong irregularity. In $[0, 1)$ the following "strong irregularity" phenomenon holds.

Theorem 9.1. (i) *For every $\varepsilon > 0$ there exists a $\delta > 0$ (depending only on ε) such that for an arbitrary sequence (u_n) in $(0, 1)$ and for every $N > 0$, $\mathscr{D}_n > \delta \log n$ for all but at most N^{ε} values of $n \leq N$.*

(ii) *For every $K > 0$ there exists an $M > 0$ (depending only on K) such that for an arbitrary sequence (u_n) in $(0, 1)$ and for every $N > 0$, $\mathscr{D}_n > K$ for all but at most $(\log N)^M$ values of $n \leq N$.*

(iii) *For an arbitrary sequence (u_n) in $(0, 1)$ the set of values of x for which $\mathscr{D}_N([0, x)) = o(\log N)$ holds, has Hausdorff dimension 0.*

This theorem was proved first only for $(\{n\alpha\})$ sequences (Sós 1979, 1983a), then for arbitrary sequences and in a more general form by Halász (1981) and Tijdeman and Wagner (1980).

One-sided irregularities. Measuring the irregularities with $\mathscr{D}_N$ or $\mathscr{D}_N^p$, we do not have any information on the sign of the discrepancy. Therefore we define

$$\mathscr{D}_N^+([0, \beta)) = \max\{\mathscr{D}_N([0, \beta)), 0\} ,$$

and

$$\mathscr{D}_N^+ = \sup_{\beta} \mathscr{D}_N^+([0, \beta)) .$$

$\mathscr{D}_N^-$ is defined analogously.

One-sided discrepancies show some new phenomena. Again, the first results on one-sided irregularities were found for $(\{n\alpha\})$ sequences. For example, there is *no* one-sided strong irregularity phenomenon. We mention just the simplest illustration of this. It is easy to see that

$$\sup_N \mathscr{D}_N^+ = \infty , \qquad \sup_N \mathscr{D}_N^- = \infty .$$

But no explicit lower bound can be given: for an arbitrary sequence $M_N \to \infty$ there exists an α such that $\mathscr{D}_N^+ < M_N$, and also there exists an α such that $\mathscr{D}_N^- < M_N$, if N is large enough.

Similarly, it is easy to see that the sequence of indices N with $\mathscr{D}_N^+ < K$ has density 0. However, for an arbitrary sequence $M_N = o(N)$, there exist an α and a K such that $\mathscr{D}_N^+ < K$ holds for at most M_N values of $n \leq N$, if N is large enough (Sós 1983a).

Concerning intervals of small discrepancy, first we remark that $\mathscr{D}_N^+([0, \beta))$ may be bounded even in the case when $\beta \neq \{k\alpha\}$, i.e. when $\mathscr{D}_N([0, \beta))$ is not.

In Dupain and Sós (1978) those intervals $[0, \beta)$ are investigated for which $\mathscr{D}_N^+([0, \beta))$ is bounded. Here we mention just one of the new phenomena: there exists an α for which the set $\{\beta\colon \sup_N \mathscr{D}_N^+([0, \beta)) < \infty\}$ has the cardinality continuum.

As an example in the opposite direction, the assertion in Theorem 8.2 remains true if instead of the boundedness of $\mathscr{D}_N(A)$ we assume only one-sided boundedness. Halász (1976) proved that if

$$\sup_N \mathscr{D}_N^+(A; x) < \infty$$

holds on a set $X \subset \Omega$ of positive measure, then $e^{2\pi i \mu(A)}$ must be an eigenvalue of T.

In contrast to aligned boxes, for balls even the simplest results: $\sup_N \mathscr{D}_N^+ = \infty$, $\sup_N \mathscr{D}_N^- = \infty$ are nontrivial. The proof of these, that is, a one-sided version of Theorem 7.2, can be found in Beck (1989b).

The following problem of Erdős, which was recently solved, is essentially a one-sided discrepancy problem.

Let $\xi_1, \xi_2, \xi_3, \ldots$ be an arbitrary infinite sequence of complex numbers on the unit circle $|z| = 1$. For every $n \in \mathbb{N}$ and complex z, let

$$P_n(z) = \prod_{j=1}^{n} (z - \xi_j) .$$

Further, let

$$A_n = A(\xi_1, \xi_2, \ldots, \xi_n) = \max_{|z|=1} |P_n(z)| .$$

Erdős conjectured that for every fixed sequence (ξ_n), $\limsup A_n = \infty$, and asked about the correct order of magnitude of

$$\max_{1 \leq n \leq N} A_n \quad \text{as } N \to \infty .$$

Observe that if the points $\xi_1, \ldots, \xi_n$ are just the nth roots of unity, then $P_n(z) = z^n - 1$, and so $A_n = 2$. This shows that the relation $\limsup A_n = \infty$ must be a consequence of the impossibility of getting every segment $\xi_1, \ldots, \xi_n$ close to uniform distribution. There seems, therefore, to be an intimate connection with the Van der Corput problem (see section 6).

By realizing this heuristics, Wagner (1980) proved the conjecture $\limsup A_n =$

∞. He developed a variation of Schmidt's original proof of Theorem 6.5, and actually proved the estimate

$$\max_{1\leq n\leq N} A_n > (\log N)^c .$$

Recently, Beck (1991a) managed to prove the best possible result

$$\max_{1\leq n\leq N} A_n > N^c ,$$

by developing a version of Halász's proof of Theorem 6.5.

10. Epilogue

As we mentioned already in the introduction, discrepancy theory has its roots, as well as its applications, in many different areas. Here we mention just a few recent applications of discrepancy and uniform distribution.

Squaring the circle. Tarski raised the following question, which is sometimes called "the problem of squaring the circle" (misusing the name of an ancient problem): is a disc equidecomposable to a square? In other words, can a disc be decomposed into finitely many parts, which can be arranged to obtain a partition of a square? The answer is in the negative under various restrictions, e.g., if the pieces are restricted to be Jordan domains.

Recently Laczkovich (1990) gave a striking and ingenious construction which answers Tarski's question in the affirmative. The proof is based on a sufficient condition for the equidecomposability of two bounded measurable sets in terms of the discrepancy of certain special sequences.

Computing the volume. Uniformly distributed sequences are used generally in applications of Monte Carlo methods. A recent success in this area is the computation of the volume of an n-dimensional convex body in polynomial time by Dyer et al. (1989). The basic tool is that a uniformly distributed point in the body can be generated efficiently (using random walk on a grid). It is a surprising fact that in this problem deterministic uniformly distributed sequences cannot give a good approximation in polynomial time (see Elekes 1986, Bárány and Füredi 1987).

Drawing segments on screen. Luby (1986) studied the question of drawing segments on a screen as paths in a grid. He showed that if certain natural assumptions are made, every scheme to assign a "connecting segment" to every pair of points will necessarily use "bent" segments. The amount of deviation from the straight line is determined by Schmidt's theorem 1.1.

"Gray" areas in photography. Rödl and Winkler (1990) studied the question of representing a gray area as a combination of black and white dots. Modelling the

"smoothness" of the resulting color as a discrepancy problem, he showed that the measure of this "smoothness" can be estimated by the theorem of Beck and its improvement by Bohus (Theorem 6.13).

References

Alexander, R.
[1990] Geometric methods in the study of irregularities of distribution, *Combinatorica* **10**, 115–136.

Alon, N., D.J. Kleitman, C. Pomerance, M. Saks and P. Seymour
[1987] The smallest n-uniform hypergraph with positive discrepancy, *Combinatorica* **7**, 151–160.

Bárány, I.
[1981] A vector-sum theorem and its application to improving flow shop guarantees, *Math. Oper. Res.* **6**(3), 445–452.

Bárány, I., and Z. Füredi
[1987] Computing the volume is difficult, *Discrete Comput. Geom.* **2**, 319–326.

Bárány, I., and V.S. Grinberg
[1981] On some combinatorial questions in finite dimensional spaces, *Linear Algebra Appl.* **41**, 1–9.
[1985] A vector-sum theorem in two-dimensional space, *Period. Math. Hung.* **16**(2), 135–138.

Baranyai, Zs.
[1974] On the factorization of the complete uniform hypergraph, in: *Infinite and Finite Sets,* eds. A. Hajnal, R. Rado and V.T. Sós, *Colloq. Math. Soc. János Bolyai* **10**, pp. 91–108.

Beck, J.
[1981a] Balanced two-colorings of finite sets in the square, *Combinatorica* **1**(4), 327–335.
[1981b] Roth's estimate of the discrepancy of integer sequences is nearly sharp, *Combinatorica* **1**(4), 319–325.
[1983] On a problem of K.F. Roth concerning irregularities of point distributions, *Invent. Math.* **74**, 477–487.
[1984a] Some upper bounds in the theory of irregularities of distribution, *Acta Arithm.* **43**, 115–130.
[1984b] Sums of distances between points on a sphere an application of the theory of irregularities of distribution to discrete geometry, *Mathematika* **31**, 33–41.
[1987a] Irregularities of Distribution I, *Acta Math.* **59**, 1–49.
[1987b] On a problem of Erdős in the theory of irregularities of distributions, *Math. Ann.* **277**, 233–247.
[1988] Irregularities of Distribution II, *Proc. London Math. Soc.* **56**(3), 1–50.
[1989a] A 2-dimensional van Aardenne-Ehrenfest theorem in irregularities of distribution, *Compos. Math.* **72**, 269–339.
[1989b] On a problem of W.M. Schmidt concerning one-sided irregularities of point distributions, *Math. Ann.* **285**, 29–55.
[1990] *On Sums of Infinite-Dimensional Vectors,* Manuscript, to appear in David Reimer's Ph.D. Thesis (Rutgers University, Piscataway, NJ).
[1991a] The modulus of polynomials with zeros on the unit circle – a problem of Erdős, *Ann. of Math.* **134**, 609–651.
[1991b] Flat polynomials on the unit circle – on a problem of Littlewood, *Bull. London Math. Soc.* **23**, 269–277.

Beck, J., and W. Chen
[1987] *Irregularities of Distribution* (Cambridge University Press, Cambridge).

Beck, J., and T. Fiala
[1981] "Integer-making" theorems, *Discrete Appl. Math.* **3**, 1–8.

Beck, J., and J. Spencer
[1983] Balancing matrices with line shifts, *Combinatorica* **3**(3–4), 299–304.
[1984a] Well-distributed 2-colorings of integers relative to long arithmetic progressions, *Acta Arithm.* **43**, 287–294.
[1984b] Integral approximation sequences, *Math. Programming* **30**, 88–98.

[1989] Balancing matrices with line shifts, II, in: *Irregularities of Partitions, Algorithms and Combinatorics,* Vol. 8 (Springer, Berlin) pp. 23–37.

Bohus, G.
[1990] On the discrepancy of 3 permutations, *Random Structures and Algorithms* **1**, 215–220.

Davenport, H.
[1956] Note on irregularities of distribution, *Mathematika* **3**, 131–135.

Deligne, P.
[1975] *Les Difféomorphismes du Cercle, Séminaire Bourbaki, Lecture Notes in Mathematics,* Vol. 477, 01 (Springer, Berlin).

Denjoy, A.
[1932] Sur les courbes définies par des équations differentielles à la surface du tore, *J. Math. Pures Appl.* **11**, 333–375.

Dupain, Y., and V.T. Sós
[1978] On the one-sided boundedness of discrepancy function of the sequence $(n\alpha)$, *Acta Arithm.* **37**, 363–374.

Dvoretzky, A.
[1961] Some results on convex bodies and Banach spaces, in: *Proc. Symp. on Linear Spaces, Jerusalem* (Pergamon Press, Oxford) pp. 123–160.

Dyer, M., A. Frieze and R. Kannan
[1989] A random polynomial time algorithm for approximating the volume of convex bodies, in: *Proc. 21st Annu. ACM Symp. on Theory of Computing* (ACM, New York) pp. 375–381.

Elekes, G.
[1986] A geometric inequality and the complexity of computing volume, *Discrete Comput. Geom.* **1**, 289–292.

Erdős, P.
[1964] Problems and results on diophantine approximations, *Comput. Math.* **16**, 52–65.

Erdős, P., and J. Spencer
[1972] Inbalances in k-colorations, *Network* **1**, 379–385.

Fürstenberg, H.
[1981] *Recurrence in Ergodic Theory and Combinatorial Number Theory* (Princeton University Press, Princeton, NJ).

Fürstenberg, H., and Y. Katznelson
[1989] Idempotents in compact semigroups and Ramsey theory, *Israel J. Math.* **68**, 257–270.

Fürstenberg, H., H. Keynes and L. Shapiro
[1973] Prime flows in topological dynamics, *Israel J. Math.* **14**(1), 26–38.

Fürstenberg, H., Y. Katznelson and D. Ornstein
[1982] The ergodic theoretical proof of Szemerédi's theorem, *Bull. Amer. Math. Soc.* **7**(3), 447–654.

Ghouila-Houri, A.
[1962] Caractérisation des matrices totalement unimodulaires, *C.R. Acad. Sci. Paris* **254**, 1192–1194.

Hajela, D.
[1988] On a conjecture of Komlós about signed sums of vectors inside the sphere, *European J. Combin.* **9**, 33–37.

Halász, G.
[1976] Remarks on the remainder in Birkhoff's ergodic theorem, *Acta Math. Hungar.* **27**, 389–396.
[1981] On Roth's method in the theory of irregularities of point-distributions, in: *Proc. Conf. on Analytic Number Theory, Durham,* Vol. 2 (Academic Press, London) pp. 79–94.

Hecke, E.
[1922] Über analytische Funktionen und die Verteilung von Zahlen mod Eins, *Abh. Math. Sem. Hamburg* **1**, 54–76.

Herman, M.R.
[1976] Conjugaison c^∞ des difféomorphismes du cercle dont le nombre de rotation satisfait a une condition arithmétique, *C.R. Acad. Sci. Paris* **282**.

Hoffman, A.
[1987] Oral communication.

Kesten, H.
[1966] On a conjecture of Erdős and Szüsz related to uniform distribution mod 1, *Acta Arithm.* **12**, 193–212.

Komlós, J., and M. Sulyok
[1970] On the sum of elements of ±1-matrices, in: *Combinatorial Theory and Its Applications, Proc. Colloq. Balatonfüred, Hungary* (North-Holland, Amsterdam) pp. 721–728.

Komlós, J., J. Pintz and E. Szemerédi
[1982] A lower bound for Heilbronn's problem, *J. London Math. Soc. (2)* **25**, 13–24.

Kuipers, L., and H. Niederreiter
[1974] *Uniform Distribution of Sequences, Pure and Applied Mathematics* (Wiley Interscience, New York).

Laczkovich, M.
[1990] Equidecomposability and discrepancy; a solution of Tarski's circle squaring problem, *J. Reine Angew. Math.* **404**, 77–117.

Lovász, L., J. Spencer and K. Vesztergombi
[1986] Discrepancy of set-systems and matrices, *European J. Combin.* **7**, 151–160.

Luby, M.
[1986] *Grid Geometries which Preserve Properties of Euclidean Geometry: A Study of Line Drawing Algorithms,* Technical Report 190/86 (University of Toronto, Computer Science Department).

Matousek, J.
[1994] *Tight upper Bounds for the Discrepancy of Half-planes,* Manuscript.

Matousek, J., and J. Spencer
[1994] *Discrepancy in Arithmetic Progressions,* Manuscript.

Olson, J.E., and J. Spencer
[1978] Balancing families of sets, *J. Combin. Theory A* **25**, 29–37.

Petersen, K.
[1973] On a series of cosecants to a problem in ergodic theory, *Comp. Math.* **26**(3), 313–317.

Ramsey, F.P.
[1930] On a problem of formal logic, *Proc. London Math. Soc. (2)* **30**, 264–285.

Rödl, V., and P. Winkler
[1990] Concerning a matrix approximation problem, *Crux Mathematicorum,* March, pp. 76–79.

Roth, K.F.
[1954] On irregularities of distributions, *Mathematika* **1**, 73–79.
[1964] Remark concerning integer sequences, *Acta Arithm.* **9**, 257–260.
[1976] Developments in Heilbronn's triangle problem, *Adv. in Math.* **22**, 364–385.
[1979] On irregularities of distribution III, *Acta Arithm.* **35**, 373–384.
[1980] On irregularities of distribution IV, *Acta Arithm.* **37**, 67–75.

Sárközy, A.
[1973] in: *Probabilistic Methods in Combinatorics,* eds. P. Erdős and J. Spencer (Akadémiai Kiadó, Budapest, 1974) section 8.

Schmidt, W.M.
[1969] Irregularities of distribution IV, *Invent. Math.* **7**, 55–82.
[1972] Irregularities of distribution VII, *Acta Arithm.* **21**, 45–50.
[1974] Irregularities of distribution VIII, *Trans. Amer. Math. Soc.* **198**, 1–22.

Sós, V.T.
[1957] On the theory of diophantine approximation I, *Acta Math. Acad. Sci. Hungar.* **8**, 461–472.
[1974] On the discrepancy of the sequence $(n\alpha)$, *Colloq. Math. Soc. János Bolyai* **13**, 359–367.
[1979] On strong irregularities of the distribution of $\{n\alpha\}$ sequences, *Tagungsber. Oberwolfach* **23**, 17–18.
[1983a] Strong irregularities of the distribution of $(n\alpha)$ sequences I, in: *Studies in Pure Mathematics* (Akadémiai Kiadó).
[1983b] Irregularities of partitions, in: *Surveys in Combinatorics 82, 9th British Combinatorial Conference, 1983,* ed. E.K. Lloyd (Cambridge University Press, Cambridge) pp. 201–245.

Spencer, J.
[1985] Six standard deviation suffice, *Trans. Amer. Math. Soc.* **289**, 679–706.
[1986] Balancing vectors in the max norm, *Combinatorica* **6**, 55–65.
Stolarsky, K.B.
[1973] Sums of distances between points on a sphere II, *Proc. Amer. Math. Soc.* 41, pp. 575–582.
Swierczkowski, S.
[1958] On successive settings of an arc on the circumference of a circle, *Fund. Math.* **46**, 187–189.
Tijdeman, R., and G. Wagner
[1980] A sequence has almost nowhere small discrepancy, *Monatsh. Math.* **90**, 315–329.
van Aardenne-Ehrenfest, T.
[1945] Proof of the impossibility of a just distribution of an infinite sequence of points over an interval, *Proc. Kon. Nederl. Akad. Wetensch.* **48**, 266–271.
[1949] On the impossibility of a just distribution, *Proc. Kon. Nederl. Akad. Wetensch.* **52**, 734–739.
Van der Corput, J.G.
[1935a] Verteilungsfunktionen I, *Proc. Kon. Nederl. Akad. Wetensch.* **38**, 813–821.
[1935b] Verteilungsfunktionen II, *Proc. Kon. Nederl. Akad. Wetensch.* **38**, 1058–1066.
van der Waerden, B.L.
[1927] Beweis einer Baudetschen Vermutung, *Nieuw Arch. Wisk.* **15**, 212–216.
Wagner, G.
[1980] On a problem of Erdős in diophantine approximation, *Bull. London Math. Soc.* **12**, 81–88.
Weyl, H.
[1916] Über die Gleichverteilung von Zahlen mod Eins, *Math. Ann.* **77**, 313–352.