Discrepancy Theory

Geometric Analysis−Professor Brock Schmutzler

Daksh Aggarwal

December 20, 2019

1 Introduction

In this short article, we wish to give an introduction to the fascinating theory of discrepancy and entropy. While the concepts of discrepancy and entropy inherently belong to the field of probabilistic analysis, they have played a pivotal role in the recent resolution of problems from geometry, number theory, and combinatorics. Miklós Laczkovich's 1990 solution of Alfred Tarski's Circle−Squaring Problem makes heavy use of discrepancy. The advanced techniques in Terence Tao's 2016 solution of the classic Erdős Discrepancy Problem ultimately rely on entropy.

We think discrepancy theory is a topic worth studying because of its wide applicability in many mathematical fields, perhaps, because discrepancy in a certain sense makes rigorous the notion of how "unsymmetric" or "unbalanced" a system is. Although Tarski's and Erdős' problems are very classical in nature, their relatively recent solutions indicate that discrepancy is a concept that fundamentally extends the arsenal of techniques available to the mathematician. Moreover, discrepancy theory has ties to some very beautiful pieces of mathematics including, but in no way limited to, arithmetic geometry, harmonic analysis, and algebraic geometry. Here, however, we will limit our exposition to exploring basic applications of the theory.

There are two different approaches to the notion of discrepancy: combinatorial and geometric. But at the core, they capture the same notion of how much "imbalance" exists in a system. Since the combinatorial approach is very intuitive, we first introduce combinatorial discrepancy and show how the entropy method is applied to the Erdős Discrepancy Problem. Then we will see, at a high level, how ideas of geometric discrepancy are utilised in Laczkovich's solution of the Circle−Squaring Problem. Our goal, with this short article, is *not* to give a complete introduction to discrepancy theory, but rather to illustrate its intuitive nature and power as a mathematical tool.

2 Combinatorial Discrepancy

For a fixed positive integer n, let $[n] := \{1, 2, \ldots, n\}$ and consider a collection of sets $\mathcal{S} = \{S_1, \ldots, S_m\}$, with $S_i \subseteq [n]$ for $i = 1, \ldots, m$. A *colouring* of $[n]$ is a function $\chi : [n] \to \{-1, 1\}$. In other words, χ defines a way to colour each element of $[n]$ with either red or blue. A natural question we can ask is: what is a colouring of $[n]$ that will ensure in each S_i the number of red and blue elements is not too different? Discrepancy formalizes the intuition underneath this question.

Definition 2.1 (Combinatorial Discrepancy)**.** *Fix a positive integer n. Given a colouring χ of $[n]$ and a set system $\mathcal{S} \subseteq 2^{[n]}$, the discrepancy of a set $S_j \in \mathcal{S}$ is*

$$\chi(S_j) = \sum_{e \in S_j} \chi(e).$$

The discrepancy of $\mathcal{S}$ under χ is

$$\chi(\mathcal{S}) = \max_{1 \le j \le m} |\chi(S_j)| \, .$$

Further, the general discrepancy of $\mathcal{S}$ with respect to the $p-$norm is

$$D_p(\mathcal{S}) = \min_{\chi:[n] \to \{-1,1\}} \left(\sum_{j=1}^{m} \chi(S_j)^p \right)^{1/p} .$$

For instance,

$$D_\infty(\mathcal{S}) = \min_{\chi} \max_{1 \le j \le m} |\chi(S_j)| = \min_{\chi} \chi(\mathcal{S}),$$

recovers the most intuitive form of discrepancy while

$$D_2(\mathcal{S}) = \min_{\chi} \sqrt{\chi(S_1)^2 + \cdots + \chi(S_m)^2},$$

is a more tractable form for algebraic purposes. Using standard inequalities from probability theory, such as the Chernoff bound, it can be shown that the discrepancy for any pair $([n], \mathcal{S})$, with $|\mathcal{S}| = m$, never exceeds $\sqrt{2n \ln(2m)}$. In fact, with 1/2 probability, every random colouring achieves this bound, which turns out be the optimal upper bound when no additional restrictions are imposed upon $\mathcal{S}$ [see 1, Ch. 1].

2.1 The Entropy Method in Erdős Discrepancy Problem

An archetypal application of discrepancy methods is Terence Tao's solution of the Erdős Discrepancy Problem. The problem is rooted in the following fun puzzle. Suppose you are confined by an evil captor in a cave who has promised to set you free if you solve a puzzle. You are at the center of a cave and two paces to your left is a pit of venomous pythons and two paces to your right is a cliff. For a fixed positive integer n, your captor demands you to plan a sequence of n steps consisiting of only lefts and rights such that you stay alive, but with this cruel caveat: you only take the steps in your path which are at multiples of d, for any positive integer d chosen by your captor. So, can you construct such a sequence of n steps, for any n, which lets you stay alive? For instance, letting 1 denote a right and -1 a left step, $(1, -1, -1, 1, -1, 1, 1, -1, -1, 1)$ is such a sequence of steps for $n = 10$. However, it's easy to show that for $n = 12$, no such sequence of steps exists. But, what if we could choose the number of paces that the pythons and the cliff were at? Would it then be possible to construct an arbitrarily long suitable sequence of steps that avoids death? This is essentially the Erdős Discrepancy Problem:

Problem 2.1 (Erdős Discrepancy Problem)**.** *Let χ be a colouring of $\mathbb{N}$ and let S be a positive constant. Must there exist $n, d \in \mathbb{N}$ such that*

$$\left| \sum_{i=1}^{n} \chi(id) \right| \ge S \, ? \tag{2.1}$$

The puzzle we presented was the Discrepancy Problem with $S = 2$, and $n = 12, d = 3$ satisfy (2.1). Attempting the problem for just $S = 2$ is moderately challenging, but Terence Tao successfully proved, over the course of two papers [5]−[6], that for any $S > 0$, the existence of n, d satisfying (2.1) is unfortunately guaranteed. In fact, by letting the set system $\mathcal{S}$ associated to $\mathbb{N}$ be the collection of integral multiples and generalising the notion of a colouring, Tao proves the following more general version of Problem 2.1 in [5].

Theorem 2.1 (Erdős Discrepancy Problem)**.** *Let $\mathcal{S} \coloneqq \{d\mathbb{N} : d \in \mathbb{N}\}$, V be a real or complex Hilbert space, and $f : \mathbb{N} \to V$ be a function such that $\|f(n)\|_V = 1$, for all $n \in \mathbb{N}$. Then the discrepancy of $\mathcal{S}$ under f is infinite.*

Tao's first big insight is that it suffices to consider only completely multiplicative functions, i.e., f satisfies $f(mn) = f(m)f(n)$, for all $m, n \in \mathbb{N}$. He shows that a function restricted to the surface of a unit sphere in V (as in Theorem 2.1), can be viewed as a superposition of completely multiplicative functions using a Fourier−analytic decomposition. Tao masterfully utilised this fact to call upon many known analytic number theory results, such as the relation of completely multiplicative functions with the Riemann zeta function, along with probabilistic arguments to prove Theorem 2.1 for the much more tractable case of completely multiplicative functions. At the crux of his proof in [6] for the simpler version of Theorem 2.1, is the application of the entropy method to show that two certain random variables are "sufficiently" independent of each other; we will be focusing on this method here. First we define what we mean by entropy, which is usually referred to as Shannon entropy in the literature.

Definition 2.2 ((Shannon) entropy)**.** *Let $\mathbb{P}(E)$ denote the probability of the event E occurring. Let X be a random variable that only takes on finitely values $\{x_1, \ldots, x_n\}$. Then the entropy of X is*

$$H(X) = \sum_{i=1}^{n} \mathbb{P}(X = x_i) \log \frac{1}{\mathbb{P}(X = x_i)}.$$

Note that since $0 \leq \mathbb{P}(X = x_i) \leq 1$ for all i, clearly the entropy of X is always nonnegative. Further, H has the subadditivity property in the sense that if X, Y are two finite random variables, then the pair (X, Y) is a finite random variable too, and

$$H(X), H(Y) \leq H((X, Y)) \leq H(X) + H(Y).$$

Entropy is usually interpreted as measuring the randomness of a variable and we discuss how Tao leverages this interpretation in his solution.

Tao encounters two random variables in a very general setting, but here we use a specific example to illustrate the logic of his argument, and we also take the liberty to evade technicalities when they don't contribute to the exposition. Consider the Liouville function $\lambda : \mathbb{N} \to \{-1, 1\}$ defined by $\lambda(n) = (-1)^k$, where k is the number of primes dividing n. (For example, $\lambda(3) = -1, \lambda(9) = 1$, and $\lambda(12) = -1$.) Then, for a fixed positive integer n, a large positive integer $L \to \infty$, and p ranging over the set of primes in the interval $[L/4, L/2]$, define the finite random variables

$$X_L \coloneqq (\lambda(n+1), \lambda(n+2), \ldots, \lambda(n+L)) \in \{-1, 1\}^L$$

and

$$Y_L \coloneqq (n \bmod p)_p \in \prod_p \mathbb{Z}/p\mathbb{Z}.$$

Clearly, since X_L and Y_L both depend on n, they are not independent. To be able to apply the Hoeffding's inequality−a powerful probabilistic estimate that bounds the amount by which a set of *independent* random variables can deviate from their expected values−Tao desired to show that X_L and Y_L are "sufficiently" independent, in a sense that can be precise (but we omit here). He argues by contradiction, and assumes X_L and Y_L have "high" correlation. Now, it can be shown that if X_L and Y_L have high correlation, then fixing the value of X_L reduces the possible values attainable by Y_L to an exponentially smaller set, i.e., fixing X_L reduces the entropy of Y_L:

$$H(Y_L \mid X_L) \leq H(Y_L) - \frac{\varepsilon L}{\log L},$$

where $\varepsilon > 0$ is proportional to how highly dependent Y_L is on X_L. In other words, X_L is "absorbing" $\varepsilon L / \log L$ worth of entropy from Y_L and in fact, Y_L can also be shown to absorb the same amount of entropy from X_L. So, using the subadditivity of entropy, we have

$$\begin{aligned} H(X_{2L} \mid Y_L) &\leq 2H(X_L \mid Y_L) \\ &\leq 2H(X_L) - \frac{2\varepsilon L}{\log L}. \end{aligned} \tag{2.2}$$

By iterating (2.2) with powers of 2, we can obtain

$$\sum_{i=1}^{\infty} \frac{H(X_{2^i L} \mid Y_{2^{i-1}L})}{2^i L} \leq \sum_{i=1}^{\infty} \frac{H(X_{2^i L})}{2^i L} - \sum_{i=1}^{\infty} \frac{\varepsilon}{\log(2^{i-1}L)}. \tag{2.3}$$

Note that since X_L is restricted to $\{-1,1\}^L$, $0 < H(X_L) \leq L$, and so the first two sums in (2.3) converge, while the last one can be shown to diverge to infinity, implying that we've reached a contradiction. Framed differently, if the dependence between X_L and Y_L is too high and Y_L is fixed in $\prod_p \mathbb{Z}/p\mathbb{Z}$, then at a large enough scale X_L is forced to have zero entropy, which is absurd since X_L cannot too have a fixed value as $L \to \infty$. Thus, Tao is able to conclude that the correlation between X_L and Y_L can be made arbitrarily small for sufficiently large L, allowing him to apply Hoeffding's inequality.

This argument shows how, in certain situations, entropy can provide structure to the inherent randomness of a problem, which can help salvage a seemingly hopeless state of affairs as it did for Tao.

3 Squaring the Circle

For the remainder of this article, we discuss Miklós Laczkovich's approach to solving a fascinating geometrical problem that is motivated by the Banach−Tarski Paradox. One of the striking consequences of the Pardadox is that a ball in $\mathbb{R}^3$ can be finitely decomposed and reassembled to yield a cube of *arbitrary* size. The Tarski's Circle-Squaring problem asks whether the two-dimensional analogue of this result holds. Because $\mathscr{L}^2$, the Lebesgue measure in $\mathbb{R}^2$, can be extended to a finitely additive and isometry-invariant measure on *all* subsets of $\mathbb{R}^2$ [see 7, pp. 229], it's necessary that the resulting square be of the *same* area as the disk being finitely decomposed, and therefore the Circle-Squaring problem we would like to study takes this form:

Problem 3.1 (Tarski's Circle−Squaring Problem)**.** *Can a square (or more precisely, a closed disk) be decomposed into finitely many subsets of $\mathbb{R}^2$ and reassembled to form a square (including its interior) of the same size?*

The answer is a resounding yes, and the reassembly can be achieved through just translations! This problem was posed by Alfred Tarski in 1925 and Laczkovich's was the first solution to it, published in 1990. Since Laczkovich's proof was non-constructive, an alternative constructive proof for the problem was also published in 2017 by Andrew Marks and Spencer Unger [4]. Laczkovich's proof, like Tao's, draws upon a large swathe of mathematics including geometry, analysis, group theory, graph theory, and number theory. But they also have a deeper similarity: the strategic application of discrepancy theoretic concepts guides Laczkovich's line of attack, so we introduce how discrepancy may be formalised in a geometric setting.

Definition 3.1 (Geometric Discrepancy in $\mathbb{R}^n$)**.** *Let $A \subseteq U := [0,1)^n \subset \mathbb{R}^n$ be finite and let $H \subseteq \mathbb{R}^n$ be measurable (w.r.t $\mathscr{L}^n$). Then, the discrepancy of A with respect to H is*

$$D(A,H) = \left| \frac{|A \cap H|}{|A|} - \mathscr{L}^n(H) \right|.$$

The discrepancy of $A \subseteq U$ is

$$D(A) = \sup_H D(A,H),$$

where H ranges over all half-open subboxes contained in U.

Intuitively, $D(A,H)$ is measuring how well the finite set A approximates the possibly infinite set H. We also require this slightly technical definition to simplify the statement of the next theorem.

Definition 3.2. *For $x = (a,b) \in \mathbb{R}^2$, let $\operatorname{frac}(x) = (a - \lfloor a \rfloor, b - \lfloor b \rfloor)$. Then, for $u \in \mathbb{R}^2$, $X = \{x_1, x_2\} \subseteq \mathbb{R}^2$, and $N \in \mathbb{N}$,*

$$F_N(u,X) = \{\operatorname{frac}(u + n_1 x_1 + n_2 x_2) : 0 \leq n_i \leq N-1\}.$$

The following translation−equidecomposability criterion for certain special measurable sets of $\mathbb{R}^2$ is central to proving the equidecomposability of the circle and square.

Theorem 3.1 (Criterion for equidecomposability)**.** *Let H_1 and H_2 be measurable sets contained in $U := [0,1) \times [0,1)$ with $\mathscr{L}^2(H_1) = \mathscr{L}^2(H_2) \neq 0$. Suppose there exists $X = \{x_1, x_2\} \subseteq U$ such that*

- *$\{(1,0),(0,1)\} \cup X$ is linearly independent over $\mathbb{Q}$.*
- *There is a function $\psi : \mathbb{N} \to [0,\infty)$ so that*

  $$\sum_{k=1}^{\infty} \frac{\psi(2^k)}{2^k} < \infty,$$

  and for any $u \in \mathbb{R}^2$, $N \in \mathbb{N}$, and $j \in \{1,2\}$,

  $$D(F_N(u,X), H_j) \leq \frac{\psi(N)}{N^2}.$$

Then, H_1 is translation−equidecomposable to H_2.

The circle and the square are equidecomposable because of this theorem, and a large part of Laczkovich's work involves proving the existence of a suitable pair of vectors x_1, x_2 in $\mathbb{R}^2$ that satisfy the two stated conditions. A very intriguing aspect of Theorem 3.1 is that it's asserting a connection between the equidecomposability of H_1, H_2 and the interaction of their discrepancies with certain special sequences. Therefore, to gain some insight into the hypothesis of Theorem 3.1, we consider a one−dimensional equidecomposability problem adapted from Laczkovich's original paper [3].

A finite set $T \subset \mathbb{R}$ is said to *decompose intervals of length* $d > 0$, if whenever I, J are subintervals of $[0, 1)$ with $\mathscr{L}(I) = \mathscr{L}(J) = d$, then I can be finitely decomposed into $\{E_1, \dots, E_n\}$ satisfying $J = \bigcup_{i=1}^{n}(E_i + t_i)$, with all $t_i \in T$, i.e., we can obtain a decomposition for J by translating a suitable decomposition of I using numbers from T. We wish to find a set T that decomposes intervals of length d, for every $d \in [1/2, 1)$. So, fixing two subintervals $I, J \subseteq [0, 1)$ of length $d \in [1/2, 1)$, we see that a decomposition of I into J via T exists if and only if there exists a bijection $\phi : I \to J$ with $\phi(x) - x \in T$ for all $x \in I$. Further, if $A \subset I$, $B \subset J$ are finite, then clearly such a bijection ϕ exists only if

$$|\{x + t : x \in A, t \in T\} \cap J| \geq |A| \text{ and } |\{y - t : y \in B, t \in T\} \cap I| \geq |B| . \tag{3.4}$$

Now, suppose T is of the form $T = \{na + k : n, k \in \mathbb{Z}, |n|, |k| \leq K\}$, for some fixed $a \in \mathbb{R}, K \in \mathbb{N}$. Then, let $A_N := I \cap \{na + k : n, k \in \mathbb{Z}, 0 \leq n < N\}$ and $B_N := J \cap \{na + k : n, k \in \mathbb{Z}, 0 \leq n < N\}$, for $N \in \mathbb{N}$. Since $I, J \subseteq [0, 1)$, we have $na + k \in I$ (or J) for some $k \in \mathbb{Z}$ if and only if $\mathrm{frac}(na) \in I$ (or J). Thus, letting $S_N := \{\mathrm{frac}(na) : 0 \leq n < N\}$, and remembering that $\mathscr{L}(I) = \mathscr{L}(J)$, we have

$$\begin{aligned}||A_N| - |B_N|| &= ||S_N \cap I| - |S_N \cap J|| \\ &= N \left| \left(\frac{|S_N \cap I|}{N} - \mathscr{L}(I) \right) - \left(\frac{|S_N \cap J|}{N} - \mathscr{L}(J) \right) \right| \\ &\geq N \left| D(S_N, I) - D(S_N, J) \right| ,\end{aligned}$$

where in the last step, we've used the reverse triangle inequality. But, from (3.4), we also have that $||A_N| - |B_N|| \leq K + K = 2K$. Thus, we have

$$N \left| D(S_N, I) - D(S_N, J) \right| \leq 2K. \tag{3.5}$$

But it is a simple fact of discrepancy theory that the sequence $\{ND(S_N)\}_{N\in\mathbb{N}}$ is unbounded [see 2, pp. 105]. So we can fix a sufficiently large N and an interval $I \subseteq [0, 1)$, having $\mathscr{L}(I) \geq 1/2$, such that $ND(S_N, I) > 2K + 2$. Further, it's not very difficult to show that there exists an interval $J \subseteq [0, 1)$ with $\mathscr{L}(J) = \mathscr{L}(I)$ and $D(S_N, J) \leq 2/N$. Thus, we have found a contradiction to (3.5), implying that T cannot be of the form we assumed. But, if we assume $T = \{na + kb + l : |n|, |k|, |l| \leq K\}$, with $a, b, 1$ linearly independent over $\mathbb{Q}$, then similar reasoning for this case shows the analogue of (3.5) is

$$N \left| D(S'_N, I) - D(S'_N, J) \right| \leq C, \tag{3.6}$$

where $S'_N := \{\mathrm{frac}(na + kb) : 0 \leq n, k \leq N\}$ and C is a constant. The essential point is that due to the two degrees of freedom available (i.e., n and k), the sequence $\{ND(S'_N)\}$ is no longer unbounded and so in this case (3.6), doesn't obstruct T from being of the assumed form: it may be possible that T decomposes all intervals of length $d \in [1/2, 1)$. Indeed, the one-dimensional analogue of Theorem 3.1 implies this is true and the mysterious second condition of the theorem's hypothesis is a clever way to prevent the occurrence of an obstruction like (3.5); also, note the similarity between the F_N's of Theorem 3.1 and the S'_N's of (3.6).

We do not pretend that this brief introduction clarifies all the details of Laczkovich's strategy, however, we hope it illuminates the power and naturalness of the concept of discrepancy. Like we did just after deriving (3.5), Laczkovich, after sufficiently analyzing the geometry of the problem, calls upon the general results of discrepancy theory and diophantine analysis to Square the Circle. The complete proof can be found in both [3] and [7].

4 Conclusion

As may have become clear in the course of our exposition, discrepancy resides in the muddy details, but a fact, which may have not been as obvious, is these arguments would be much muddier if it weren't for the structure provided by discrepancy theoretic concepts. It goes without saying that there is a wealth of fascinating applications where discrepancy helps remedy a less than ideal situation (as for Tao), but also where it inspires the main proof strategy (as for Laczkovich), and the interested reader might like to refer to [1] for an impressive compilation of some of these.

5 Acknowledgment

I would like to express sincere gratitude to Professor Brock Schmutzler for teaching me all the analysis I know, and for giving me the freedom and opportunity to explore my wide mathematical interests while fulfilling this writing requirement for Geometric Analysis.

References

[1] Bernard Chazelle. *The Discrepancy Method: Randomness and Complexity.* Cambridge University Press, 2000.

[2] L. Kuipers and H. Niederreiter. *Uniform Distribution of Sequences.* John Wiley & Sons, 1974.

[3] Miklós Laczkovich. "Equidecomposability and discrepancy; a solution of Tarski's circle-squaring problem". In: *J. reine angew. Math* 404 (1990), pp. 71–117.

[4] Andrew Marks and Spencer Unger. "Borel circle squaring". In: *Annals of Mathematics* 186.2 (2017), pp. 581–605. URL: `https://annals.math.princeton.edu/2017/186-2/p04`.

[5] Terence Tao. "The Erdős discrepancy problem". In: *Discrete Analysis* 1 (2016), p. 27. URL: `https://arxiv.org/abs/1509.05363`.

[6] Terence Tao. "The logarithmically averaged Chowla and Elliott conjecture for two-point correlations". In: *Forum of Mathematics, Pi* 4.8 (2016). URL: `https://arxiv.org/abs/1509.05422`.

[7] Stan Wagon and Grzegorz Tomkowicz. *The Banach-Tarski Paradox.* 2nd ed. Encyclopedia of Mathematics and Its Applications. Cambridge University Press, 2016.