Discrepancy Theory: An Algorithmic Overview

Sam Boardman

December 8, 2022

1 Introduction

Discrepancy theory, broadly speaking, is concerned with the construction of discrete sets that approximate some notion of a uniform distribution. This is especially salient—and often difficult—when the uniform distribution is continuous or has a non-trivial combinatorial structure. Indeed, examples of problems in discrepancy theory are plentiful, and largely form the core of the subfield as a coherent area of study. Nonetheless, many tools from combinatorics, computer science, and even other areas of mathematics may be applied to shed light on these problems, sometimes implying a more general method that can be used to make progress on additional problems. At the same time, the basic aim of discrepancy theory is conceptually robust—it asks not to simulate a uniform distribution of the above form, but instead design an object that represents it, capturing the uniformity in a deterministic way. In contrast, however, randomly generated objects tend to exhibit streaks, clustering, or other forms of repetition that are not always representative of the underlying phenomenon, with people tending to see patterns that are in reality a mirage of random formation (e.g. the so-called *clustering illusion*). Discrepancy theory, then, has applications to myriad problems with a spatial or combinatorial structure, such as numerical integration (forming the basis of the quasi-Monte Carlo method) and creating more exotic distributions from simpler ones (giving rise to pseudorandomness).

1.1 A Motivating First Question: How Uniform Can a Sequence of Number in [0,1] Be?

A first-order question for the area of discrepancy theory is the following: given infinite sequences of points $a_1, a_2, \dots \in [0,1]$, how uniform can these be over $[0,1]$? [1]. More formally, for any such sequence and $n \in \{1,2,\dots\}$, define the "partial sequence" $S_n = \{a_1,\dots,a_n\}$, and set $D(n) = \sup_{0\le x\le 1} ||S_n \cap [0,x]| - nx|$. $D(n)$ measures the worst possible error in approximating the expected number of points of S_n in $[0,x]$ if they are distributed uniformly and independently, namely nx, with the actual number of points of S_n in $[0,x]$, namely $S_n \cap [0,x]$. As a result of this interpretation, $D(n)$ can be thought of as a notion of discrepancy for this context. A value of $D(n) = 0$ represents complete alignment between the two quantities for all $x \in [0,1]$, although this ideal is not attainable; the quantity nx is not even integral except for countably many x. Therefore, the above question can be cast as: how small can the quantity $D(n)$ be in terms of n? The answer is on the order of $\log n$; this is far from obvious, but can be obtained by using number theory and constructing a candidate sequence accordingly.

More than just an intellectual curiosity, this question suggests an application of discrepancy theory to numerical integration of a function f over a domain D: sample the value of f as uniformly as possible over its domain, normalizing the sum by the volume of the domain divided by the number

(a) Low-discrepancy "Sobol" sequence [2]

(b) Uniform pseudorandom numbers [3]

Figure 1: The first 10000 points of two different sequences. 1a exhibits a regular, lattice-esque pattern. 1b experiences a higher degree of clustering of points and corresponding vacancies.

of samples taken. Such a technique is called a *quasi-Monte Carlo* method, and its error is bounded by the discrepancy of the sample points in the function domain—which is defined very similarly to the function D above—encouraging the use of a sequence of sample points with low discrepancy. This approach is sometimes preferable to a *Monte Carlo* method in which sample points are chosen uniformly at random. We have elucidated the difference between low-discrepancy and random sequences above; we can also juxtapose the two sequences shown above, each of which could be used as the set of sample points for numerical integration over $D = [0, 1]^2$.

1.2 Outline of Paper

Having now motivated an exploration of discrepancy theory with a concrete example of a discrepancy theoretic problem, an indication of its amenability to mathematical analysis, and its application to a computational problem, we explain the organization of the present paper and then move to a more detailed study of several problems that are representative of discrepancy theory.

It is challenging to encapsulate the breadth of problems studied in discrepancy theory and its depth of mathematical technique and application to applied mathematics and theoretical computer science. In attempt of doing such, the present paper introduces a few different problems showcasing the varied interpretations of the above description of discrepancy theory and the landscape of progress made in its study, also exemplifying key techniques and potential applications in the process.

The problem in Section 2 studies the interactions between two partitions of a finite set. Applications are immediate, and one is given. As we show, the problem is computationally tractable and relatively easy to analyze.

The problem in Section 3 studies the behavior of 2-colorings of a finite set across overlapping subsets thereof. The problem is computationally hard and is instead analyzed via randomized algorithms and hardness results.

We conclude with a discussion of the results and further directions of inquiry.

2 Discrepancy Minimization and Network Flow

This section presents the following conceptual problem concerning the minimization of discrepancy, in this case constructing a set including a prescribed number of elements from each set in a partition while ensuring that the selections are uniform with respect to each set in another partition [4]. We present a polynomial-time algorithm for the problem and showcase an application thereof.

Suppose we have a finite set $A = \{a_1, \ldots, a_n\}$ representing elements of interest, and two different partitions of it, $\{B_i\}_{i=1}^r$ and $\{C_j\}_{j=1}^s$, which give two different perspectives on how the elements of A may be classified. A natural problem arising therefrom is: given natural numbers $k_1, \ldots, k_r$, construct a set $F \subset A$ that contains exactly k_i elements of B_i for each $i \in \{1, \ldots, r\}$, with the additional constraint that F is "almost uniform" over the sets C_j with respect to the choice of elements from $B_1, \ldots, B_r$ under their respective budgets $k_1, \ldots, k_r$; if the $k_1 + \cdots + k_r$ elements of F are chosen uniformly over $B_1, \ldots, B_r$, the expected number of elements of C_j in F is $\Phi_j := E[F \cap C_j] = \sum_{i=1}^r k_i \frac{|B_i \cap C_j|}{|B_i|}$ (by linearity of expectation). Φ_j may not be integral, so the "almost uniform" condition is set as $\lfloor \Phi_j \rfloor \leq |F \cap C_j| \leq \lceil \Phi_j \rceil \ \forall j \in \{1, \ldots, s\}$. In summary, we have the following discrepancy minimization problem.

Definition 2.1. *Given a set $A = \{a_1, \ldots, a_n\}$, partitions $\{B_i\}_{i=1}^r$ and $\{C_j\}_{j=1}^s$, and natural numbers $k_1, \ldots, k_r$, the* Almost Uniform Subset *problem is to exhibit a set $F \subset A$ such that $|B_i| = k_i \ \forall i \in \{1, \ldots, r\}$, and for $\Phi_j := \sum_{i=1}^r k_i \frac{|B_i \cap C_j|}{|B_i|}$, $\lfloor \Phi_j \rfloor \leq |F \cap C_j| \leq \lceil \Phi_j \rceil \ \forall j \in \{1, \ldots, s\}$.*

To better motivate the Almost Uniform Subset problem, consider the following application to designing a fair driving schedule in a variable carpool scheme.

Suppose that s people share a car for a period of r days, where for each day there is a subset of the s people riding in the car. For each day, assign one person in the corresponding subset to drive the car as fairly as possible, where the notion of fairness is that each day generates one unit of "driving obligation" divided equally among the occupants of the car on that day, and so the total number of drivers needed over r days is equal to the sum of each individual's total driving obligation (taken over each day they are in the car). The objective is to make the assignment of drivers such that the total number of days each person drivers the car is equal to their driving obligation (modulo rounding to a nearest integer).

Claim 2.2. *The above carpool scheduling problem is reducible to the* Almost Uniform Subset *problem in polynomial time.*

Proof. Set $A = \{(i, j) : \text{ person } j \text{ rides in the car on day } i\}$. Partition A into subsets $B_1, \ldots, B_r$, where B_i is the set of ordered pairs in A with i as the first component, hence the list of people riding in the car on day i, with an index i prepended. Also partition A into subsets $C_1, \ldots, C_s$, where C_j is the set of ordered pairs in A with j as the second component, hence the list of days person j rides in the car, with an index j appended. Now for F consisting of ordered pairs $(i, j) \in A$ interpreted to mean that person j drives the car on day i (i.e. $F \subset A$ defining a driving schedule), we want there to be a driver each day, i.e. $k_i = |F \cap B_i| = 1$, and we want the number of days person j drives the car, i.e. $|F \cap C_j|$, equal to their driving obligation (modulo rounding), $\Phi_j = \sum_{i=1}^r 1 \cdot \frac{|B_i \cap C_j|}{|B_i|}$, since $|B_i|$ is the number of people riding in the car on day i and $|B_i \cap C_j|$ if 1 exactly when person j rides in the car on day i and 0 otherwise. Thus finding such a set F reduces to the Almost Uniform Subset problem under the same notation. Lastly, the construction of the above sets clearly takes time polynomial in r, s. $\square$

This examples also exemplifies some of the nuances of discrepancy minimization problems. Heuristic approaches are easy to think of but generally not correct. For instance, one could attempt to assign drivers based on a fairness constraint within a subset of drivers, but some people may ride with many different groups over the set of days, accumulating ample driving obligation over time but little from days riding with particular people. This calls for a more global approach to minimizing the discrepancy. Indeed, the desired combinatorial object—the set F—is guaranteed to exist, and the Almost Uniform Subset problem is solvable in polynomial time via reduction to maximum flow.

Theorem 2.3. *The* Almost Uniform Subset *problem is in* P.

Proof. Denote $\phi_{ij} = k_i \frac{|B_i \cap C_j|}{|B_i|}$ for all $1 \le i \le r, 1 \le j \le s$. We construct a flow network with source s and sink t. Let b_i be a vertex representing B_i for each $1 \le i \le r$ and c_j be a vertex representing C_j for each $1 \le j \le s$. Finally, create vertices $d_0, d_1, \dots, d_s$ that will serve as gadgets in our reduction from Almost Uniform Subset. The edges of the graph and their respective capacities are as follows: an edge (s, b_i) of capacity k_i for each i; an edge (b_i, c_i) of capacity $\lceil \phi_{ij} \rceil$ for each i, j; edges $(c_j, d_j), (d_j, t)$ of capacity $\lfloor \Phi_j \rfloor$ for each j; an edge (c_j, d_0) of capacity $\lceil \Phi_j \rceil - \lfloor \Phi_j \rfloor = 1$ for each j such that Φ_j is not integral; and an edge (d_0, t) of capacity $\sum_{i=1}^r k_i - \sum_{j=1}^s \lfloor \Phi_j \rfloor$.

The intuition for this flow network is as follows. One unit of flow that passes through the flow network corresponds to inclusion of an element of the set A in F, where the network topology and edge capacities enforce the various requirements for F. In this vein, we claim that there is a flow that saturates the edges from s and to t that places value ϕ_{ij} on each edge (b_i, c_j), value $\lfloor \Phi_j \rfloor$ on each edge (c_j, d_j), and value $\Phi_j - \lfloor \Phi_j \rfloor$ on each edge (c_j, d_0). Flow conservation at vertices b_i follows from that $\sum_{j=1}^s \phi_{ij} = k_i$ because the C_j for which $B_i \cap C_j \neq \emptyset$ partition B_i, whereas flow conservation at vertices c_j holds since $\sum_{i=1}^r \phi_{ij} = \Phi_j$; the integer part of this flow value is sent on edges (c_j, d_j) and the fractional part is sent on edges (c_j, d_0). The fractional parts may be sent to d_0 since $\sum_{i=1}^r \sum_{j=1}^s \phi_{ij} = \sum_{i=1}^r k_i$. Hence there is a flow of value $\sum_{i=1}^r k_i$. However, ϕ_{ij} is not integer-valued in general, in which case the above interpretation of the flow does not make sense. However, noting that the s-t cut $(\{s\}, V \backslash \{s\})$ has capacity $\sum_{i=1}^r k_i$, this is also the max flow value in the flow network; since its edges have integer-valued capacities, the flow integrality theorem guarantees there exists an integer-valued flow f of value $\sum_{i=1}^r k_i$.

We may now formally check the above flow interpretation. Given the above s-t cut, f must place flow k_i on each edge (s, b_i). At each vertex b_i, each unit of flow is diverted to a vertex c_j so that the total flow entering c_j from each b_i is at most $\lceil \phi_{ij} \rceil$, which is at most $|B_i \cap C_j|$ since $\frac{k_i}{|B_i|} \le 1$. On the other hand, the total flow entering c_j is at most $\lceil \Phi_j \rceil$ but at least $\lfloor \Phi_j \rfloor$ since the s-t cut $(V \backslash \{t\}, \{t\})$ only has capacity $\sum_{i=1}^r k_i$, hence the flow saturating all edges to t, and where the combined capacity of the edges (c_j, d_j) and (c_j, d_0) is $\lfloor \Phi_j \rfloor + \lceil \Phi_j \rceil - \lfloor \Phi_j \rfloor = \lceil \Phi_j \rceil$. In other words, choosing $f(b_i, c_j)$ elements of $|B_i \cap C_j|$ (these intersections are all disjoint) results in $|F \cap B_i| = k_i$ for all i and $\lfloor \Phi_j \rfloor \le |F \cap C_j| \le \lceil \Phi_j \rceil$ for all j, as desired.

The construction of the flow network is clearly in polynomial time with respect to r, s, n, and such an integral max flow can be found by Ford-Fulkerson, where $\sum_{i=1}^r k_i \le n$, in time $O(rs \cdot n)$. Constructing F from the flow may also be done in polynomial time. $\square$

3 Discrepancy of Colorings and Set-Systems

This section is about the problem of partitioning a set into two subsets—conceptualized as coloring the set with red and blue—such that the assignment of elements to colors is as uniform as possible with respect to each of a collection of subsets of the original set [5]. Focusing on these so-called set-systems yields a more dichotomous notion of discrepancy. Unlike the above discrepancy minimization problem, this class of problems is much less tractable and illustrates more general techniques for bounding minimum discrepancy and finding approximate solutions via randomized algorithms. We prove that in general this problem is NP-hard and employ randomized coloring algorithms with probabilistic analysis to obtain rough solutions to the problem.

Definition 3.1. *A set-system is a tuple (V, C), where $V = \{1, \ldots, n\}$ is a set of elements and $C = \{S_1, \ldots, S_m\}$ is a collection of subsets of V.*

The objective is to color the vertices of V two colors, "red" and "blue", such that the sets in C are as balanced as possible with respect to color.

Definition 3.2. *(Coloring) A red-blue coloring of V is a function $\chi : V \to \{-1, 1\}$, where -1 corresponds to red and 1 corresponds to blue.*

Therefore, the sum of the values of χ over a set S states the difference between the number of elements in S colored blue and colored red—the extent to which balance of the colors is not achieved. We define our notion of discrepancy accordingly.

Definition 3.3. *The discrepancy of a coloring χ for a set S is the quantity* $\operatorname{disc}(\chi, S) = |\chi(S)|$, *where $\chi(S) := \sum_{i \in S} \chi(i)$. The discrepancy of the coloring χ for the set-system (V, C) is the quantity* $\operatorname{disc}(\chi, C) = \max_{S \in C} |\chi(S)|$.

We are interested in the existence and construction of a coloring with minimum discrepancy.

Definition 3.4 (Discrepancy)**.** *The discrepancy of a set-system (V, C) is the quantity* $\operatorname{disc}(C) = \min_{\chi \in [V \to \{-1,1\}]} \max_{S \in C} |\chi(S)|$.

Noting that $\operatorname{disc}(C) \leq \max_{S \in C} |S|$, the discrepancy of a set-system is $O(\max_{S \in C} |S|)$, which is $O(n)$ since necessarily $|S| \leq n$. Observe that the monochromatic coloring makes the first bound sharp, so if $\max_{S \in C} |S|$ is $\Theta(n)$, there are colorings of discrepancy $\Theta(n)$. On the other hand, if the sets are disjoint, then there is a coloring using alternating colors for each set such that the discrepancy of the coloring is $O(1)$.

Given the spectrum of possible colorings and set structures, salient questions that immediately arise include the existence of general bounds on the discrepancy of set-systems as well as efficient algorithms for computing the discrepancy and a coloring that achieves it.

One greedy approach for constructing a low-discrepancy coloring is to iterate through the sets and alternate the colors red and blue for elements that have not yet been colored. While this achieves $O(1)$ discrepancy for at least the first set, subsequent sets may happen to consist of a series of elements that were previously colored, say, red, thereby incurring $\Theta(n)$ discrepancy.

Alternatively, coloring each element uniformly at random and independently results in expected discrepancy of 0 for each set; there may be deviations from 0, and this approach does not take advantage of the structure of the sets, but it does limit the probability of obtaining a high-discrepancy coloring (e.g. from the above worst-case scenarios). To do this, we recall the following well-known corollary of the Chernoff bound.

Lemma 3.5. *If $X_1, \ldots, X_n$ are independent random variables satisfying $P(X_i = -1) = P(X_i = 1) = \frac{1}{2}$, and $X = \sum_{i=1}^n X_i$, then for $\lambda \geq 0$, $P(|X| \geq \lambda\sqrt{n}) \leq 2e^{-\lambda^2/2}$.*

Theorem 3.6. *Let (V, C) be a set-system. Construct a random coloring $\chi : V \to \{-1, 1\}$ by setting $P(\chi(i) = -1) = P(\chi(i) = 1) = \frac{1}{2}$ with $\chi(1), \ldots, \chi(n)$ mutually independent. Then $P(\mathrm{disc}(\chi, C) \leq 2\sqrt{\max_k |S_k| \log m}) \geq 1 - \frac{2}{m}$, and $\mathrm{disc}(C)$ is $O(\sqrt{n \log m})$.*

Proof. For each $S_i \in C$, observe $\chi(S_i)$ is a sum of $|S_i|$ $\{0, 1\}$-valued uniform independent random variables. Thus by the Chernoff bound corollary, $P(\mathrm{disc}(\chi, S) \geq 2\sqrt{|S_i| \log m}) = P(|\chi(S_i)| \geq 2\sqrt{\log m}\sqrt{|S_i|}) \leq 2e^{-(2\sqrt{\log m})^2/2} = 2e^{-2\log m} = \frac{2}{m^2}$. Hence by taking a union bound and monotonicity, $P(\mathrm{disc}(\chi, C) \geq 2\sqrt{\max_k |S_k| \log m}) \leq \sum_{i=1}^m P(\mathrm{disc}(\chi, S) \geq 2\sqrt{\max_k |S_k| \log m}) \leq m \cdot \frac{2}{m^2} = \frac{2}{m}$. In particular, there exists a coloring χ with $\mathrm{disc}(\chi, C) < 2\sqrt{\max_k |S_k| \log m}$, so $\mathrm{disc}(C) < 2\sqrt{\max_k |S_k| \log m}$, which is $O(\sqrt{n \log m})$. $\square$

We now have an upper bound on the discrepancy of a set-system that was not clear a priori, and an algorithm with polynomial expected runtime to produce a coloring with such a discrepancy. Nonetheless, we will obtain a sharper bound and find corresponding improved colorings with polynomial expected time. This leads us to a key theorem in the study of set-system discrepancy.

Theorem 3.7 (Spencer)**.** *Let (V, C) be a set-system. If $m \leq n$, then $\mathrm{disc}(C) \leq 6\sqrt{n}$. If $m > n$, then $\mathrm{disc}(C)$ is $O(\sqrt{n \log(\frac{m}{n})})$.*

3.1 An Algorithmic Version of Spencer's Result

We now algorithmically compute a coloring that achieves the discrepancy claimed by Spencer's above theorem. We do this iteratively by relaxing the notion of a coloring to a gradient. The approach is due to Lovett and Meka [6].

Definition 3.8 (Fractional Coloring)**.** *A fractional coloring of V is a function $x : V \to [-1, 1]$. By abuse of notation we also use x to denote the fractional coloring as an n-tuple, i.e. $x = (x(1), \ldots, x(n))$. For $S \in C$, denote $x(S) = \sum_{i \in S} x(i)$ the discrepancy of the set S (under the fractional coloring x).*

The algorithm relies on starting at a fractional coloring of $x \equiv 0$, which has discrepancy 0, applying a random but judicious perturbation to the coloring so that the discrepancy of the sets does not change too much but eventually x is close to integral, and then rounding to a proper coloring while trying to avoid a significant change in the discrepancy of the sets.

With this in mind, we define several notions pertaining to fractional colorings and discrepancy of sets.

Definition 3.9. *Let $x_0, x_1, x_2, \ldots$ be a sequence of fractional colorings. We say that an element i is alive after time $t-1$ if $|x_{t-1}(i)| < 1$ and is frozen after time $t-1$ if $|x_{t-1}(i)| \geq 1 - \delta$. We say that a set S_j is dangerous after time $t-1$ if $|x_{t-1}(S_j) - x_0(S_j)| \geq \lambda_j - \delta$. Here, $\lambda_1, \ldots, \lambda_m, \delta$ are fixed positive constants.*

We now use these concepts to define a random update to the fractional coloring x_{t-1}.

Definition 3.10. *Let k be the number of alive elements at time 0, which without loss of generality are given by $[k]$. $V^t \subset \mathbb{R}^n$ is the subspace of points $(v_1, \ldots, v_n)$ such that if element i is frozen after time $t-1$, then $v_i = 0$, and if the set S_j is dangerous after time $t-1$, then $\sum_{i \in S_j \cap [k]} v_i = 0$.*

Definition 3.11. *For a subspace $V \subset \mathbb{R}^n$ of dimension d, we say that a random d-dimensional vector $g \in V$ is distributed according to $N(V)$ if $g \equiv c_1 v_1 + \cdots + c_d v_d$ for $c_1, \ldots, c_d \sim N(0,1)$ independent and $\{v_1, \ldots, v_d\}$ an orthonormal basis for V. $N(V)$ is called the standard multivariate normal distribution supported on V, and by rotational invariance, the definition does not depend on the choice of orthonormal basis.*

Next, we state our algorithm of interest.

Algorithm 1 Attempts to compute a fractional coloring x_T with discrepancy close to x_0 that freezes at least half of the remaining unfrozen variables in x_0

```
Initialize x_0 and V^0 = R^k × {0}^{n-k}
Set γ ≤ 1/n^2 and δ = (10 log n)γ
Set T = 16/(3γ^2)
Fix λ_1, ..., λ_m > 0: Σ_{j=1}^m e^{-λ_j^2/16} ≤ k/16
for t = 1, ..., T do
    Draw g ~ N(V^t)
    x_t ← x_{t-1} + γg
    Compute V^{t+1}
end for
return x_T
```

The idea is that the algorithm takes a random walk starting with the all-0 fractional coloring—for which all sets have discrepancy 0—and gradually completes the coloring by randomly updating the color variables x_t in a direction as to preserve colors near -1 or 1 and the discrepancy of sets with relatively high discrepancy. We want to prove the following result.

Theorem 3.12. *Let (V, C) be a set-system with $m > n$. With at least fixed positive probability, repeating Algorithm 1 for polynomially many iterations, with the first iteration taking $x_0 \equiv (0, \ldots, 0)$ and each successive iteration taking $x_0 \equiv x_T$ from the previous iteration and x_T^* denoting the terminal fractional coloring for the final iteration, yields a proper coloring*

$$x(i) = \begin{cases} \operatorname{sign}(x_T^*(i)) & \text{with probability } \frac{1+|x_T^*(i)|}{2} \\ -\operatorname{sign}(x_T^*(i)) & \text{with probability } \frac{1-|x_T^*(i)|}{2} \end{cases} \quad \forall 1 \leq i \leq n$$

that has $O(\sqrt{n \log(\frac{m}{n})})$ discrepancy.

Therefore, by the theory of probability amplification for randomized algorithms, a coloring of $O(\sqrt{n \log(\frac{m}{n})})$ discrepancy may be found in expected polynomial time (since the number of algorithm executions needed is geometric with fixed parameter, which is at least the lower bound on the probability of success).

To prove Theorem 3.12, we follow the exposition of [5]. We emphasize the structure of the proof and its conceptually salient computations; exhaustive details are given in [6].

Our goals are thus: show that x_t remains a valid fractional coloring with high probability; show that the change in the discrepancy of any of the sets is small with high probability; and prove that at least $\frac{k}{2}$ elements become frozen with high probability.

We prove the first two statements immediately, then traverse a list of propositions needed to prove the third statement. Lastly, we synthesize these three statements to conclude Theorem 3.12.

By construction of V^t, the algorithm can only update elements i that are not frozen after time $t-1$, i.e. $|x_{t-1}(i)| < 1 - \delta$. Without loss of generality, $v_1, \ldots, v_d$ as in $N(V^t)$ are standard basis vectors. Then the quantity $x_t(i) - x_{t-1}(i)$ is a $N(0, \gamma^2)$-distributed random variable, so for C sufficiently large we have $|x_t(i)| \leq 1 - \delta + C\sqrt{\log(T)}\gamma \leq 1$ (asymptotically) with arbitrarily high probability (e.g. Chebyshev's inequality), as desired.

Analogously, the algorithm can only induce changes in the discrepancy of sets S_j that are not dangerous after time $t-1$, i.e. $|x_{t-1}(S_j) - x_0(S_j)| < \lambda_j - \delta$. As above, then the quantity $x_t(S_j) - x_{t-1}(S_j)$ is a $N(0, \leq \gamma^2|S_j|)$ random variable (see Claim 3.15) and hence (triangle inequality) for C sufficiently large we have $|x_t(S_j) - x_0(S_j)| \leq \lambda_j - \delta + C\sqrt{\log T}\sqrt{|S_j|}\gamma \leq \lambda_j + \frac{1}{n}$ (asymptotically) with arbitrarily high probability, as desired.

We now state the following elementary lemmas about the multivariate normal distribution.

Lemma 3.13. *Let $V \subset \mathbb{R}^n$ be a subspace. If $g \sim N(V)$, $\forall u \in \mathbb{R}^n\ \exists \sigma \leq ||u|| : \langle g, u \rangle \sim N(0, \sigma^2)$, where $\langle \cdot, \cdot \rangle$ denotes the dot product in $\mathbb{R}^n$.*

Lemma 3.14. *Let $V \subset \mathbb{R}^n$ be a d-dimensional subspace and $g \sim N(V)$. For $i = 1, \ldots, n$ define $\sigma_i : \langle g, e_i \rangle \sim N(0, \sigma_i^2)$ as guaranteed by Lemma 3.13. Then $\sum_{i=1}^n \sigma_i^2 = d$.*

Now turn to bounding the change in discrepancy during each iteration.

Claim 3.15. *The change in discrepancy of a set S_j that is not dangerous after time $t-1$ from time $t-1$ to time t is distributed as $N(0, \sigma_j^2)$, where $\sigma_j^2 \leq \gamma^2|S_j|$*

Proof. Without loss of generality, $v_1, \ldots, v_d$ as in $N(V^t)$ are standard basis vectors. Then the quantity $x_t(S_j) - x_{t-1}(S_j)$ is the sum of at most $|S_j|$ independent $N(0, \gamma^2)$-distributed random variables; use that normal distributions are preserved under sums and additivity of variance to conclude. □

Lemma 3.16. *The probability that more than $\frac{k}{8}$ sets become dangerous during the execution of the algorithm is at most $\frac{1}{8}$.*

Proof. Applying Claim 3.15 and analyzing a martingale associated with the change in discrepancy for each set S_j, it follows that $P(|x_T(S_j) - x_0(S_j)| \geq \lambda_j\sqrt{|S_j|}) \leq 2e^{-(\lambda_j^2|S_j|)/(T\gamma^2|S_j|)} = 2e^{-3\lambda_j^2/16}$. Combining with the condition $\sum_{j=1}^m e^{-\lambda_j^2/16} \leq \frac{k}{16}$ will imply that the desired probability is bounded by $\frac{1}{8}$.

□

Condition on this event as follows.

Lemma 3.17. *At least $\frac{k}{2}$ elements become frozen during the execution of the algorithm with probability at least $\frac{21}{32}$*

Proof. Let P' be the probability measure obtained by conditioning on the event that no more than $\frac{k}{8}$ sets become dangerous during the execution of the algorithm. Under this event, if fewer than $\frac{k}{2}$ elements become frozen, then for any t the dimension of V^t is at least $k - \frac{k}{2} - \frac{k}{8} = \frac{3k}{8}$. Then $E'[\sum_{i=1}^n x_t(i)^2 - x_{t-1}(i)^2] \geq \frac{3k}{8}\gamma^2$ due to Lemma 3.14. By linearity $E'[\sum_{t=1}^T(\sum_{i=1}^n x_t(i)^2 -$

$x_{t-1}(i)^2)| \leq \frac{k}{2}$ elements become frozen] $\geq T\frac{3k}{8}\gamma^2 = 2k$. Applying the law of total expectation yields that $P'(\leq \frac{k}{2}$ elements become frozen) $\leq \frac{1}{4}$. Now by the law of total probability, we deduce $P(\geq \frac{k}{2}$ elements become frozen) $\geq \frac{7}{8} \cdot \frac{3}{4} = \frac{21}{32}$. □

Combining the first two statements with Lemma 3.17 (e.g. by a union bound), with high probability the algorithm keeps x_t a valid fractional coloring with low discrepancy increments and freezes at least half of the unfrozen variables. Hence with fixed positive probability the algorithm may be applied $O(\log n)$ times to achieve a low discrepancy fractional coloring with all variables frozen. Noting that taking $\lambda_j = 8\sqrt{\log(\frac{m}{k})}$ $\forall 1 \leq j \leq m$ satisfies $\sum_{j=1}^{m} e^{-\lambda_j^2/16} \leq \frac{k}{16}$, we can obtain an upper bound for the total change in discrepancy after $O(\log n)$ executions of the algorithm and starting from $x_0 = (0, \ldots, 0)$ by looking at a corresponding infinite series for infinitely many iterations, obtaining $C\sqrt{n\log(\frac{m}{n})}$ for the total discrepancy upper bound for some $C > 0$ fixed. By construction, the proper coloring defined in Theorem 3.12 satisfies $E[x(i)] = x_T(i)$ for all i. By analyzing deviations via a Chernoff bound, the post-processing rounding of the terminal fractional coloring to a proper coloring will not incur much extra discrepancy in any set with high probability, in which case this proper coloring will still have discrepancy $O(\sqrt{n\log(\frac{m}{n})})$. Additional details are available in Section 6 of [6].

3.2 Complexity of Discrepancy

Having proved an upper bound on discrepancy and an algorithm to achieve such a coloring in expected polynomial time, the following hardness result shows that there is little recourse for finding much sharper bounds deterministically in polynomial time, let alone the corresponding colorings.

Theorem 3.18. *The problem of deciding, given a set-system with $m = O(n)$ and such that it has discrepancy 0 or discrepancy $\Omega(\sqrt{n})$, which of the two discrepancies the set-system has is* NP*-hard.*

The reduction is from the Max-2-2-Set-Splitting problem, which is the topic of the manuscript [7], and involves working with a set system for which the first part of Spencer's theorem is sharp up to constant factors, the so-called Hadamard set system.

4 Discussion

The problems studied in Section 2 and Section 3 illustrate the coherence yet diversity of discrepancy theory in their similarities and differences. On the one hand, both involve choosing elements from some universal set U that should induce balance with respect to predefined subsets of U. The Almost Uniform Subset problem is more restrictive in the choice of elements—a prescribed number k_i must come from each of a collection of partitioning subsets B_i—while the problem of minimizing the discrepancy of a set-system (U, C) may be pursued by coloring any choice of the elements red (or blue). On the other hand, the Almost Uniform Subset problem asks for the chosen subset of elements to be uniform with respect to a different collection of partitioning subsets C_j, whereas the problem of minimizing the discrepancy of a set-system requires that the distribution of colors be balanced across potentially overlapping subsets of U.

The above juxtaposition of problem features suggests that discrepancy theory is not organized hierarchically but rather consists of a zoo of problems constituting different interpretations and contexts of uniformity. The computational complexity of such problems is not clear a priori; the above analysis suggested that neither problem was a special case of the other, but the present paper established that one of them can be solved efficiently and deterministically (Theorem 2.3) while the other (likely) cannot (Theorem 3.18). Nonetheless, the application of randomness can sometimes remedy this hardness. This ranges from simplistic attempts to sample uniform outcomes by uniform randomness (Theorem 3.6) to more savvy, combinatorially aware random walks on the space of possible solutions that find uniformity iteratively (Theorem 3.12), with a corresponding improvement in obtained discrepancy to boot.

The techniques used throughout the present paper are more general than may be apparent. Beyond probabilistic techniques—which probe the relationship between randomness and discrepancy—the notion of a fractional coloring gives a more continuous way to think about colorings, paving the way for placement in systems of equations and amenability to methods in linear algebra, not unlike the way updates to the coloring were chosen in Algorithm 1. Indeed, Section 2.1 of [5] gives a simpler, deterministic way to use linear algebra to make a proper coloring from a fractional coloring, obtaining a discrepancy bound for set-systems that is sometimes better than the ones we have presented here. For more continuous notions of discrepancy, such as in the motivating problem that appears in Section 1.1, Fourier analysis plays a prominent role in uncovering their nature; [1] demonstrates the utility of Fourier analysis and a variety of other approaches for discrepancy theoretic problems.

In addition to the application of discrepancy theory to numerical integration suggested in Section 1.1, discrepancy theory enjoys a rich interplay with pseudorandomness. The most straightforward way this arises is in the use of low-discrepancy objects to generate pseudorandom sequences, but moreover discrepancy may be used as a metric for sampling from a large random collection, with implications for probability amplification for randomized algorithms. Chapter 9 of [1] again offers a good survey of this relationship.

As noted by [4], there are other possible applications of network flow to discrepancy theoretic problems. Nonetheless, the contemporary literature on combinatorial discrepancy theory focuses largely on set-systems and a generalization to real-valued matrices [5]. One prolific open problem contained therein is the Beck-Fiala conjecture, which is the statement that for any set-system (V, C), $\mathrm{disc}(C)$ is $O(\sqrt{d(C)})$, where $d(C)$ is the degree of the set-system, i.e. the largest number of sets in C that contain any fixed element of V. A bound that gets close to this is by Banaszczyk, which states that $\mathrm{disc}(C)$ is $O(\sqrt{d(C)\log m})$; the proof uses convex geometry as a central ingredient [8]. More generally, a recent cutting-edge idea consists of derandomizing a certain stochastic process to constructively achieve state-of-the-art bounds across several discrepancy theoretic settings while still discovering new ones [9]. In summary, there are many avenues for further progress in discrepancy theory, ranging from individual problems to broad theories, and with potential applications as ubiquitous as the notions of uniformity and balance.

5 Appendix

To see a video presentation based on this manuscript, refer to the EECS 572, Fall 2022 Piazza page on or after December 9, 2022.

References

[1] Bernard Chazelle. *The Discrepancy Method.* Princeton, New Jersey: Cambridge University Press, 2000.

[2] Robert Dodier. *Low discrepancy 10000*. 2006. URL: https://commons.wikimedia.org/wiki/File:Low_discrepancy_10000.png.

[3] Robert Dodier. *Random 10000*. 2006. URL: https://commons.wikimedia.org/wiki/File:Random_10000.png.

[4] Robert Kleinberg. *The Dinitz, Hopcroft-Karp, and Push-Relabel Algorithms*. URL: https://www.cs.cornell.edu/courses/cs6820/2020fa/handouts/dinitz.pdf.

[5] Nikhil Bansal. *Algorithmic Aspects of Combinatorial Discrepancy*. 2014.

[6] Shachar Lovett and Raghu Meka. "Constructive Discrepancy Minimization by Walking on the Edges". In: *FOCS* (2012), pp. 61–67.

[7] Moses Charikar, Alantha Newman, and Aleksandar Nikolov. "Tight Hardness Results for Minimizing Discrepancy". In: *Proceedings of the Twenty-Second Annual ACM-SIAM Symposium on Discrete Algorithms*. SODA '11. San Francisco, California: Society for Industrial and Applied Mathematics, 2011, pp. 1607–1614.

[8] Aleksandar Nikolov. *Prague Summer School: Discrepancy Theory*. 2018. URL: https://www.cs.toronto.edu/~anikolov/Prague18/Lectures/lect3.pdf.

[9] Nikhil Bansal, Aditi Laddha, and Santosh S. Vempala. *A Unified Approach to Discrepancy Minimization*. URL: https://arxiv.org/pdf/2205.01023.pdf.