Smoothed Analysis with Adaptive Adversaries

NIKA HAGHTALAB, University of California Berkeley, Berkeley, United States
TIM ROUGHGARDEN, Columbia University, New York, United States
ABHISHEK SHETTY, University of California Berkeley, Berkeley, United States

We prove novel algorithmic guarantees for several online problems in the smoothed analysis model. In this model, at each time step an adversary chooses an input distribution with density function bounded above pointwise by $\frac{1}{\sigma}$ times that of the uniform distribution; nature then samples an input from this distribution. Here, σ is a parameter that interpolates between the extremes of worst-case and average case analysis. Crucially, our results hold for *adaptive* adversaries that can base their choice of input distribution on the decisions of the algorithm and the realizations of the inputs in the previous time steps. An adaptive adversary can non-trivially correlate inputs at different time steps with each other and with the algorithm's current state; this appears to rule out the standard proof approaches in smoothed analysis.

This paper presents a general technique for proving smoothed algorithmic guarantees against adaptive adversaries, in effect reducing the setting of an adaptive adversary to the much simpler case of an oblivious adversary (i.e., an adversary that commits in advance to the entire sequence of input distributions). We apply this technique to prove strong smoothed guarantees for three different problems:

(1) Online learning: We consider the online prediction problem, where instances are generated from an adaptive sequence of σ-smooth distributions and the hypothesis class has VC dimension d. We bound the regret by $\tilde{O}(\sqrt{Td\ln(1/\sigma)} + d\ln(T/\sigma))$ and provide a near-matching lower bound. Our result shows that under smoothed analysis, learnability against adaptive adversaries is characterized by the finiteness of the VC dimension. This is as opposed to the worst-case analysis, where online learnability is characterized by Littlestone dimension (which is infinite even in the extremely restricted case of one-dimensional threshold functions). Our results fully answer an open question of Rakhlin et al. [64].
(2) Online discrepancy minimization: We consider the setting of the online Komlós problem, where the input is generated from an adaptive sequence of σ-smooth and isotropic distributions on the ℓ_2 unit ball. We bound the ℓ_∞ norm of the discrepancy vector by $\tilde{O}(\ln^2(\frac{nT}{\sigma}))$. This is as opposed to the worst-case analysis, where the tight discrepancy bound is $\Theta(\sqrt{T/n})$. We show such polylog(nT/σ) discrepancy guarantees are not achievable for non-isotropic σ-smooth distributions.
(3) Dispersion in online optimization: We consider online optimization with piecewise Lipschitz functions where functions with ℓ discontinuities are chosen by a smoothed adaptive adversary and show that the resulting sequence is $(\sigma/\sqrt{T\ell}, \tilde{O}(\sqrt{T\ell}))$-dispersed. That is, every ball of radius $\sigma/\sqrt{T\ell}$ is split by

The research of the second author was supported in part by NSF awards CCF-2006737 and CNS-2212745. This work is also partially supported by the NSF under CCF2145898, the ONR under N00014-24-1-2159, a C3.AI Digital Transformation Institute grant, a Berkeley AI Research and Microsoft Research Commons award, a JP Morgan Chase Faculty Fellowship, a Google research scholar faculty award, a Schmidt Sciences AI2050 award, and an Apple AI Ph.D. fellowship.
Authors' Contact Information: Nika Haghtalab, Electrical Engineering and Computer Science, University of California Berkeley, Berkeley, California, United States; e-mail: nhaghtal@gmail.com; Tim Roughgarden, Computer Science, Columbia University, New York, New York, United States; e-mail: tim.roughgarden@gmail.com; Abhishek Shetty, Electrical Engineering and Computer Science, University of California Berkeley, Berkeley, California, United States; e-mail: shetty@berkeley.edu.

ACM 0004-5411/2024/06-ART19
https://doi.org/10.1145/3656638

$\tilde{O}(\sqrt{T\ell})$ of the partitions made by these functions. This result matches the dispersion parameters of Balcan et al. [13] for oblivious smooth adversaries, up to logarithmic factors. On the other hand, worst-case sequences are trivially $(0, T)$-dispersed.[1]

CCS Concepts: • **Theory of computation → Online learning algorithms**; **Regret bounds**; **Online learning theory;**

Additional Key Words and Phrases: Smoothed analysis, online learning, regret bounds, online convex optimization, data driven algorithm design, online discrepancy minimization

ACM Reference Format:
Nika Haghtalab, Tim Roughgarden, and Abhishek Shetty. 2024. Smoothed Analysis with Adaptive Adversaries. *J. ACM* 71, 3, Article 19 (June 2024), 34 pages. https://doi.org/10.1145/3656638

1 INTRODUCTION

Smoothed analysis. Kryptonite for worst-case analysis comes in the form of algorithms for which almost all inputs are "easy" and yet rare and pathological inputs are "hard." Perhaps the most famous example is the simplex method for linear programming, which empirically always runs quickly but requires exponential time in the worst case (for all of the common pivot rules) [56]. Equally misleading is the worst-case exponential running time of many popular local search algorithms, such as the k-means clustering algorithm [8] and the 2-OPT heuristic for the **traveling salesman problem (TSP)** [67]; such behavior is literally never observed for these algorithms in practice.[2] Taken literally, worst-case analysis recommends against using the simplex method to solve linear programs or local search as a heuristic for the TSP, flatly contradicting decades of real-world experience. Thus, for some important problems and algorithms, a more nuanced analysis framework is called for.

But if not worst-case analysis, then what? Outside of applications with a stable and well-understood input distribution, average-case analysis is far too specific an approach. Spielman and Teng [69] introduced *smoothed analysis*, a novel interpolation between worst- and average-case analysis that is ideally suited for the analysis of algorithms that almost always perform well. In its original formulation, an adversary chooses an arbitrary (worst-case) input, which is then perturbed slightly by nature. Appealingly, the framework makes no assumptions about the input other than a small amount of uncertainty (e.g., due to measurement errors).

In the more modern and general formulation of smoothed analysis, an adversary directly chooses an input distribution from a family of permissible distributions; nature then samples an input from the adversary's distribution. An algorithm is evaluated by its worst-case (over the adversarially chosen input distribution) expected (over the distribution) performance. Performance guarantees in this model (e.g., on the expected running time of an algorithm) are generally parameterized by the "degree of anti-concentration" enjoyed by the allowed input distributions. The holy grail in smoothed analysis is to prove guarantees on algorithm performance that, assuming only a low level of anti-concentration in the possible input distributions, are far closer to average-case guarantees than worst-case guarantees.

[1] An extended abstract was published in the Proc. of the 62nd Annual Symposium on Foundations of Computer Science [42].
[2] Note that in all of these examples, the problem of constructing a hard instance is challenging enough to justify its own research paper!

Online learning, discrepancy minimization, and optimization. Smoothed analysis makes sense for any numerical measure of algorithm performance, but to date the vast majority of work on the topic concerns the running time of algorithms for offline problems, as in the famous examples above. Our work here focuses on *online* problems—online learning, online discrepancy minimization, and online optimization—in which the input arrives incrementally over time and an irrevocable decision must be made at each time step. Online algorithms for these problems are traditionally assessed by their solution quality or regret (with running time a secondary concern). In the smoothed analysis version of these problems, the adversary is forced to choose each piece of the input—a point from a domain, a vector, or a function—from a distribution with non-negligible anti-concentration.

The analysis of online algorithms traditionally distinguishes between *oblivious* adversaries who choose the entire input sequence up front (with knowledge only of the algorithm to be used) and *adaptive* adversaries that can condition each part of the input on the past. In the worst-case model, this distinction is relevant only for randomized algorithms, in which case adaptive adversaries choose each part of the input as a function of the algorithm's previous decisions. When the adversary itself is forced to randomize, as in the smoothed analysis model, the distinction between oblivious and adaptive adversaries takes on new meaning: while an oblivious adversary must choose a sequence of input distributions up front, an adaptive adversary can base its current choice of an input distribution on the decisions of the algorithm *and the realizations of the inputs* in previous time steps.

Online learning, discrepancy minimization and optimization play integral roles in a wide range of fields and applications, such as algorithm design [3, 7], game theory [29, 33], differential privacy [32, 44, 46], control theory [1, 2], design of medical trials [47], and robust statistics [50]. In these cases, adversary's adaptiveness both serves as a natural abstraction for correlations between past and present and is an essential piece of the technical analyses (such as algorithmic reductions) that make these methods widely applicable.

The challenge of adaptive adversaries. A basic question is: For which online problems are adaptive adversaries fundamentally more powerful than oblivious ones? In the smoothed analysis model, there is strong intuition about why a guarantee against oblivious adversaries might not extend to, or at least would be significantly harder to prove for, adaptive adversaries. A key to any smoothed analysis is, of course, to determine how to leverage the assumed anti-concentration properties of the permissible input distributions. With an oblivious adversary, the input distributions at each time step are independent of each other and of the algorithm's current state, and the assumed anti-concentration can typically be directly and separately exploited at each time step. An adaptive adversary, on the other hand, has the power to correlate inputs at different time steps with each other and with the algorithm's current state. This dependence seems to rule out the standard proof approaches in smoothed analysis.

Our approach: Preserving anti-concentration through a coupling-based reduction. We introduce a general technique for reducing smoothed analysis with adaptive adversaries to the much simpler setting of oblivious adversaries. We consider adaptive adversaries that at each time step choose an input distribution with density function bounded above pointwise by $\frac{1}{\sigma}$ times that of the uniform. The crux of our approach is a coupling argument, namely a joint distribution that connects T random variables $(X_1, \ldots, X_T)$ generated by an adaptive smooth adversary with kT random variables $Z_i^{(t)}$ for $i \in [k]$ and $t \in [T]$ that are generated i.i.d. from the uniform distribution. A key aspect of this coupling is a monotonicity property, that for $k = \tilde{\Theta}(1/\sigma)$, with high probability, $\{X_1, \ldots, X_T\} \subseteq \{Z_i^{(j)} \mid i \in [k], j \in [T]\}$.

The properties of this coupling allow us to translate typical algorithms and proofs from the setting of oblivious adversaries to that of adaptive adversaries. For example, consider an algorithm that fails only when $X_1, \ldots, X_T$ "concentrate," roughly meaning that many of the X_i's land in an *a priori* chosen set of small measure (this is a recurring theme in the smoothed analysis of algorithms). After substituting in $\{Z_i^{(j)} \mid i \in [k], j \in [T]\} \supseteq \{X_1, \ldots, X_T\}$, the likelihood of this event only increases. (See Section 2.2 for precise statements.) On the other hand, i.i.d. uniform random variables (the $Z_i^{(j)}$'s) have ideal anti-concentration properties for a smoothed analysis.

The power of our coupling technique is in its versatility. To demonstrate this, we apply our coupling approach to applications of online learning, online discrepancy minimization, and dispersion in online optimization. In each of these problems, we show that existing analyses for oblivious adversaries fundamentally boil down to a suitable anti-concentration result. For online learning — where our work resolves an open problem of Rakhlin et al. [64] — what matters is the anti-concentration of the input instances in the symmetric difference between a hypothesis and its nearest neighbor in a finite cover of the hypothesis class. For online discrepancy minimization, what matters is the anti-concentration of correlations between discrepancy vectors and inputs. For dispersion, what matters is the anti-concentration of function discontinuities in small intervals. After isolating these key steps, we prove that the coupling approach can be used to lift them (and the algorithmic guarantees that they lead to) to the general case of adaptive adversaries.

1.1 Overview of Our Results

Throughout this paper we consider σ-smooth adaptive adversaries. A σ-smooth distribution $\mathcal{D}$ is a distribution whose densities are bounded by $1/\sigma$ times the density of the uniform distribution over a domain. Formally this definition is captured as follows.

Definition 1.1 (σ-smoothness). Let $\mathcal{X}$ be a domain that supports a uniform distribution $\mathcal{U}$.[3] A measure μ on $\mathcal{X}$ is said to be σ-smooth if for all measurable subsets $A \subset \mathcal{X}$, we have $\mu(A) \leq \frac{\mathcal{U}(A)}{\sigma}$.

This parameterized definition of "sufficiently anti-concentrated" is the standard one that has been used in smoothed analysis over the past decade, for example in all analyses of the smoothed running time of local search heuristics [60]. It prevents an adversary from concentrating most of its probability mass near a specific worst-case input (as is necessary for any interesting results) without resorting to any parametric assumptions.

We focus on smoothed analysis of adaptive adversaries that at time t pick a σ-smooth distribution $\mathcal{D}_t$ after having observed earlier instances $x_1 \sim \mathcal{D}_1, \ldots, x_{t-1} \sim \mathcal{D}_{t-1}$ and algorithmic choices. We denote an adaptive sequence of σ distributions by $\boldsymbol{\mathscr{D}}$. We use $\boldsymbol{\mathscr{D}}$ to model smoothed analysis of online learning, online discrepancy, and online optimization with an adaptive adversary.

Online Learning. We work with the setting of smoothed *online adversarial (and full-information) learning*. In this setting, a learner and an adversary play a repeated game over T time steps. For a labeled pair $s = (x, y)$ and a hypothesis $h \in \mathcal{H}$, $\mathbb{I}[h(x) \neq y]$ indicates whether h makes a mistake on s. In every time step $t \in [T]$ the learner picks a hypothesis h_t and adversary picks a distribution $\mathcal{D}_t$ whose marginal on $\mathcal{X}$ is σ-smooth and then draws $s_t \sim \mathcal{D}_t$. The learner then incurs penalty of $\mathbb{I}[h(x_t) \neq y_t]$. We consider an *adaptive* σ-smooth adversary and denote it by $\boldsymbol{\mathscr{D}}$, where $\mathcal{D}_t$ is selected by an adversary that knows the algorithm and has observed $s_1, \ldots, s_{t-1}$ and $h_1, \ldots, h_{t-1}$. Our goal is to design an online algorithm $\mathcal{A}$ such that expected regret against an adaptive

[3]Such as $\mathcal{X}$ that is finite or has finite Lebesgue measure. The definition makes sense for arbitrary domains and fixed measures μ but for the sake of presentation, we restrict to the case of uniform distributions.

adversary,

$$\mathbb{E}[\textsc{Regret}(\mathcal{A}, \mathscr{D})] := \mathop{\mathbb{E}}_{\mathscr{D}}\left[\sum_{t=1}^{T} \mathbb{I}\left[h_t(x_t) \neq y_t\right] - \min_{h\in\mathcal{H}} \sum_{t=1}^{T} \mathbb{I}\left[h(x_t) \neq y_t\right]\right] \tag{1}$$

is sublinear in T. This is the most well-studied domain for the application of our techniques.

In the worst case (without smoothness), Ben-David et al. [23] showed that the optimal regret in online learning is characterized by finiteness of a combinatorial quantity known as the Littlestone dimension, more formally, it is $\textsc{Regret} = \tilde{\Theta}(\sqrt{\text{LDim}(\mathcal{F})T})$. Unfortunately, the Littlestone dimension can be large even for classes where the VC dimension is small. Rakhlin et al. [64], Haghtalab [39], and Haghtalab et al. [41] considered the smoothed analysis of online learning and asked whether regret bounds that are characterized by finiteness of $\text{VCDim}(\mathcal{H})$ are possible. For the oblivious smooth adversaries, Haghtalab [39] answered this in the positive. However, for adaptive smooth adversaries their best-known bounds are $\tilde{\Theta}(\sqrt{T \cdot \log \mathcal{N}_{[\,]}})$ where $\mathcal{N}_{[\,]}$ denotes the *bracketing number* which can be infinite even when $\text{VCDim}(\mathcal{H})$ is constant.

In this paper, we bridge the gap between smoothed analysis of online learning with adaptive and non-adaptive adversaries, answer an open problem of Rakhlin et al. [64] and Haghtalab [39], and show that regret bounds against an adaptive smooth adversary are nearly the same as those in agnostic offline learning.

Theorem 3.1 (Informal)**.** *Let $\mathcal{H}$ be a hypothesis class of VC dimension d. There is an algorithm $\mathcal{A}$ such that for any adaptive sequence of σ-smooth distributions $\mathscr{D}$ achieves a regret of*

$$\mathbb{E}[\textsc{Regret}(\mathcal{A}, \mathscr{D})] \in \tilde{O}\left(\sqrt{Td\ln\left(\frac{T}{d\sigma}\right)} + d\ln\left(\frac{T}{d\sigma}\right)\right). \tag{2}$$

We complement this by a nearly matching lower bound as follows.

Theorem 3.2 (Informal)**.** *For every d and σ such that $d\sigma \leq 1$, there exists a hypothesis class $\mathcal{H}$ with VC dimension d such that for any algorithm $\mathcal{A}$ there is a sequence of σ-smooth distributions $\mathcal{D}$ where*

$$\mathbb{E}[\textsc{Regret}(\mathcal{A}, \mathcal{D})] \in \Omega\left(\sqrt{Td\log\left(\frac{1}{\sigma d}\right)}\right). \tag{3}$$

Online Discrepancy. Our starting point is the Komlós problem. In this online discrepancy problem, we are given an online sequence of vectors $v_1, \ldots, v_T$ with $\|v_i\|_2 \leq 1$. Upon seeing v_i we need to immediately and irrevocably assign sign $\epsilon_i \in \{-1, +1\}$ to v_i. Our goal is to keep the following discrepency vector small

$$\max_{t\in[T]} \left\| \sum_{i=1}^{t} \epsilon_i v_i \right\|_\infty .$$

This problem is interesting for various norms on the inputs and the discrepancy, here we restrict ourselves to ℓ_2 and ℓ_∞ norms, respectively.

It is not hard to see that in the fully adaptive setting, the adversary can pick a vector orthogonal to the current discrepancy vector leading to the ℓ_∞ discrepancy norm growing as $O(\sqrt{T})$. To overcome this, stochastic versions of this problem have been considered where vectors v_i are picked from a *fixed and known* distribution over a set of vectors with $\|v_i\| \leq 1$. Bansal et al. [18] use a potential-based approach to obtain a bound of $O(\log^4(nT))$ for the stochastic setting. Alweiss et al. [5] strengthen these results to hold for any sequence of inputs that is chosen by an oblivious (even deterministic) adversary and obtains $O(\log(nT))$ on the discrepancy.

We consider adversaries that pick a σ-smooth distribution $\mathcal{D}_t$ at time t after having observed the earlier instances $v_1, \ldots, v_{t-1}$ and their assigned signs $\epsilon_1, \ldots, \epsilon_{t-1}$ and then draw $v_t \sim \mathcal{D}_t$. We bound the discrepancy of this setting by $O(\log^2(nT))$.

Theorem 4.1 (Informal)**.** *Let $v_1, \ldots, v_T$ be chosen from an adaptive sequence of σ-smooth and isotropic distributions $\mathscr{D}$. Then, there is an online algorithm for deciding the sign ϵ_i of v_i, such that with high probability*

$$\max_{t \le T} \left\| \sum_{i=1}^{t} \epsilon_i v_i \right\|_\infty \le O\left(\log^2 \left(\frac{Tn}{\sigma} \right) \right).$$

We note that our adaptive isotropic assumption is mild, as even for the case of stochastic uniform inputs (which are isotropic) the first polylog(nT) bound was introduced by Bansal et al. [21] in STOC 2020. Proving discrepancy lower bounds for isotropic adaptive distributions is an interesting problem for future work. Our next theorem further justifies the use of isotropic distributions by showing that smoothness alone is not enough to achieve a polylog(nT/σ) bound on discrepancy in presence of adaptive adversaries.

Theorem 4.2 (Informal)**.** *For any online algorithm, there is an adaptive sequence of $(\frac{1}{20n^2T^2})$-smooth distributions on the unit ball such that, we have*

$$\left\| \sum_{i=1}^{T} \epsilon_i v_i \right\|_\infty \ge \Omega\left(\sqrt{\frac{T}{n}} \right)$$

with probability $1 - \exp(-\frac{T}{12})$.

Dispersion in Online Optimization. In the online optimization setting, an adversary chooses a sequence of loss functions $u_1, \ldots, u_T$ and at each time step the learner picks an instance x_t in order to minimize regret

$$\sum_{t=1}^{T} u_t(x_t) - \min_x \sum_{t=1}^{T} u_t(x).$$

Balcan et al. [13] studied this problem for piecewise Lipschitz functions and showed that regret is characterized by a quantity called *dispersion*. At a high level, a sequence of functions is called *dispersed* if no ball of small width intersects with discontinuities of many of these functions.

Definition 1.2 (Dispersion, [13]). Let $u_1, \ldots, u_T : [0,1] \to \mathbb{R}$ be a collection of functions such that u_i is piecewise Lipschitz over a partition $\mathcal{P}_i$ of $[0,1]$. We say that a partition $\mathcal{P}_i$ splits a set A if A intersects with at least two sets in $\mathcal{P}_i$. The collection of functions is called (w,k)-*dispersed* if every interval of width w is split by at most k of the partitions $\mathcal{P}_1, \ldots, \mathcal{P}_T$. This definition naturally extends to loss functions over $\mathbb{R}^d$ as well.

Additionally, Balcan et al. [13] showed that when an oblivious σ-smooth adversary picks the discontinuities of piecewise Lipschitz functions, the resulting sequence is with high probability $(\sigma(T\ell)^{\alpha-1}, O((T\ell)^\alpha))$-dispersed, where α can be any value in $[0.5, 1]$ where ℓ is the number of discontinuities. We extend this result to the case of adaptive smooth adversaries and recover almost matching bounds on dispersion parameters. Our work shows that adaptive smooth adversaries generate dispersed sequences in online optimization. This allows us to extend the power of algorithms designed for dispersed sequences, such as efficient online and private batch optimization [13], to the larger setting of adaptive adversaries.

Theorem 5.1 (Informal)**.** *Let $u_1 \ldots u_T$ be functions from $[0,1] \to \mathbb{R}$ that are piecewise Lipschitz with ℓ discontinuities each picked by a σ-smooth adaptive adversary. Then, for any $\alpha \ge 0.5$, the sequence*

Table 1. This Table Compares and Summarizes the Results of This Paper and those from Previous Works

	Worst Case	Stochastic/ Oblivious	Adaptive Smoothed
Online Learning	$\tilde{\Theta}\left(\sqrt{T \cdot \mathrm{LDim}}\right)$ [23]	$\tilde{\Theta}\left(\sqrt{T \cdot d}\right)$ [39]	$\tilde{\Theta}\left(\sqrt{T \cdot d \log\left(1/\sigma\right)}\right)$ Theorem 3.1
Online Discrepancy	$\Omega\left(\sqrt{T/n}\right)$ [68]	$O\left(\log\left(nT\right)\right)$ [5] $O\left(\log^4\left(nT\right)\right)$ [18]	$\tilde{O}\left(\log^2\left(nT/\sigma\right)\right)$ Theorem 4.1 (also isotropic)
Dispersion	$(w, T\ell)$ $\forall w$; (trivial)	$\left(\sigma(T\ell)^{\alpha-1}, O\left((T\ell)^{\alpha}\right)\right)$ [13]	$\left(\sigma(T\ell)^{\alpha-1}, \tilde{O}\left((T\ell)^{\alpha}\right)\right)$ Theorem 5.1

In this table, T is the time horizon, σ is the smoothness parameter, d is the VC dimension of the hypothesis class in online learning, n is the dimension of the space for online discrepancy, ℓ is the number of discontinuities of piecewise Lipschitz functions in online optimization, and $\alpha \in [0.5, 1]$ is arbitrary.

of functions $u_1 \ldots u_T$ is $(\sigma(T\ell)^{\alpha-1}, \tilde{O}((T\ell)^{\alpha}))$-dispersed. A summary of our results can be found in Table 1.

1.2 Related Work

In this section, we will survey other work related to the question that we study in this paper.

Online learning. Similar models of smoothed online learning have been considered in prior work. Generally, previous works have focused on oblivious adversaries, more stylized noise distributions, or the performance of specific algorithms rather than aiming for characterizing the statistical complexity of the learning problem. Rakhlin et al. [64] consider online learning when the adversary is constrained in a general way and introduce constrained versions of sequential Rademacher complexity for analyzing the regret. They work with general technique of sequential symmetrization and tangent sequences adapted to the constrained setting and show that the regret in the constrained setting is bounded by the constrained sequential Rademacher complexity. While this notion is general enough to capture our setting and has been applied successfully in other constrained adversary settings [57], the bound in terms of the constrained sequential Rademacher complexity is not explicit, and it was not clear prior to our work how to relate this notion to the statistical complexities of the learning problem such as the VC dimension (except in the special case of halfspaces with additive noise).

Gupta and Roughgarden [38] consider smoothed online learning when looking at problems in online algorithm design. They prove that while optimizing parameterized greedy heuristics for Maximum Weight Independent Set imposes regret growing linear in T in the worst-case, in the presence of smoothing (oblivious version of σ-smoothed adversary model in our paper) this problem can be learned with non-trivial sublinear regret (as long they allow per-step runtime that grows with T). Cohen-Addad and Kanade [35] consider the same problem with an emphasis on the per-step runtime being logarithmic in T. The models in these works differs from ours in the obliviousness of the smoothed adversaries.

Smoothed analysis has also been used in a number of other online settings. For linear contextual bandits, Kannan et al. [55] use smoothed analysis with Gaussian perturbations to show that the greedy algorithm achieves sublinear regret even though in the worst case it can have linear regret. Raghavan et al. [62] work in a Bayesian version (again with Gaussian perturbation) of this setting and achieve improved regret bounds for the greedy algorithm. The results considered in the above papers are focussed on the regret of particular algorithms rather than the statistical complexity of the learning problem as in our case.

Generally, our work is also related to a line of work on online learning in the presence of additional assumptions modelling properties exhibited by real life data. Rakhlin and Sridharan [63] consider settings where the learner has additional information available in terms of an estimator for future instances. They achieve regret bounds that are in terms of the path length of these estimators and can beat $\Omega(\sqrt{T})$ if the estimators are accurate. Dekel et al. [36] also considers the importance of incorporating side information in the online learning framework and show that regrets of $O(\log(T))$ in online linear optimization maybe possible when the learner has access to vectors that are weakly correlated with the future instances.

More broadly, our work is among a growing line of work on beyond the worst-case analysis of algorithms [66]. Examples of this in machine learning mostly include improved runtime and approximation guarantees of supervised (e.g., [9–11, 37, 53, 54]), and unsupervised settings (e.g., [6, 12, 14, 24, 25, 45, 59, 61, 70]).

Discrepancy. Discrepancy is well-studied area in computer science and combinatorics with rich connections to various areas. For a general overview of the area see [34]. Many classical settings such as the Spencer problem, Komlós problem, Tusnandy problem and the Beck-Fiala problem continue to inspire active research. A recent line of work has been developing algorithmic techniques for many new settings that were previously only dealt with non-constructively and were even believed to be non-tractable [15–17, 58, 65].

A setting that has also recently received attention is the online discrepancy setting. Bansal and Spencer [22] consider the setting where the inputs are all uniform on $\{-1, 1\}^n$ and get a $O(\sqrt{n}\log T)$ bound for the ℓ^∞ discrepancy. Motivated by questions in envy minimization, Bansal et al. [21] and Jiang et al. [52], consider the stochastic problem with general distributions, along with several geometric discrepancy problems such as the Tusnady problem. Bansal et al. [21] give a $O(n^2 \log T)$ discrepancy in the ℓ^∞ norm algorithm when the input is in $[-1, 1]^n$. As discussed earlier, Bansal et al. [18] provide a $\sqrt{n}\log^4(nT)$ in the same setting. They also consider various other settings such as the online Banaszczyk problem and a weighted multicolor discrepancy problem. Alweiss et al. [5] consider a non-stochastic version of the problem where the vectors are obliviously picked from $[-1, 1]^n$ and propose a beautiful randomized algorithm that achieves $\sqrt{n}\log(nT)$ bound.

Subsequent Work. Following the original publication of this paper [42, 43], several works have appeared that further contribute to the framework of smoothed analysis in online settings. A pair of works (concurrent to one another) by Block et al. [26], Haghtalab et al. [40] study the computational complexity of online learning in the smoothed setting. Their main motivation is to understand whether smoothed analysis can be used to circumvent strong impossibility results for oracle-efficient online learning [49]. Block et al. [26], Haghtalab et al. [40] answer this question in the affirmative and show that there are oracle-efficient algorithms that achieve regret depending only on the VC dimension, similar to our Theorem 3.1, albeit with worse dependence on the smoothness parameter σ. To achieve some of their results, Haghtalab et al. [40] and Block et al. [26] use and, indeed, strengthen our probability coupling approach in different ways. Their results bring a computational lens to the statistical problem studied in this work. Together, their works demonstrate that online learning is computationally as easy as offline learning, as our work establishes that that it is statistically as easy as offline learning.

Block and Simchowitz [28] also study computational complexity of online learning with smoothed adversaries for generalized linear functions in the realizable and construct algorithms that achieve optimal dependence on the smoothness parameter, bridging the statistical-computational gap between our work and those of Haghtalab et al. [40] and Block et al. [26] in this special case.

Haghtalab et al. [40] studies several other constrained and classical adversarial model, such as existing and new variants of *transductive online learning* and *prediction in small domains.* They show, through a more detailed perspective, that the probability coupling approach introduced in our work can be used to draw parallels between several different lines of work on online learning, beyond the classical worst-case setting.

Bansal et al. [19] study the problem of prefix discrepancy problem for unit vectors under a smoothed analysis setting. They show that for smoothed instances a discrepancy bound of $\sqrt{\log d + \log\log T}$ where d is the dimension and T is the time horizon which improves the dependence on the time horizon compared to known bounds for worst-case instances. Bansal et al. [20] study the offline Komlós setting (balancing ℓ_2 unit vectors in the ℓ_∞ norm) in the smoothed analysis setting. They show that, for sufficiently large number of vectors, the discrepancy of smoothed instances inversely polynomial in the dimension, resolving the Komlós conjecture for such instances.

Janardhan Kulkarni and Rothvoss [51] study the online discrepancy problem against oblivious adversaries and show (nonconstructively) that there is an algorithm that assigns signs to the vectors v_i, with $\|v_i\|_2 \leq 1$, presented online, such that $\sum_{i\leq t} \epsilon_i v_i$ is 10-subguassian for all t. This gives a discrepancy bound of $O(\sqrt{\log T})$ i.e., $\left\|\sum_{i=1}^{t} \epsilon_i v_i\right\| \leq O(\sqrt{\log T})$ at all times t, matching the lower bound for the online discrepancy problem for oblivious adversaries.

2 OVERVIEW OF THE TECHNIQUES AND ANALYSIS

We introduce a general technique for reducing smoothed analysis with adaptive adversaries to the much simpler setting of oblivious adversaries. Our main general technique is a *coupling* argument between random variables that are generated by an adaptive smooth adversary and those that are generated i.i.d. from a uniform distribution. This coupling, that is a joint distribution between two random processes, demonstrates structural properties that are ideal for preserving and analyzing anti-concentration properties of smooth adversaries. This allows us to tap into existing techniques and algorithms that are designed for oblivious smooth adversaries and only rely on some anti-concentration properties of the input.

We first give an overview of our coupling technique and its analysis in Section 2.1 and then in Section 2.2 we give a general framework for applying coupling for smoothed analysis with adaptive adversaries.

2.1 Coupling Definition and Theorem Statement

In this section, we will give an overview of the coupling between smooth adaptive adversaries and the uniform distribution. A *coupling* is a joint distribution between two random variables, or random processes, such that the marginals of this coupling are distributed according to the specified random variables. A more formal definition of a coupling is as follows.

Definition 2.1 (Coupling). Let μ and ν be two probability measures on the probability space $(\mathcal{X}, \mathcal{F})$ respectively. Then, a coupling between μ and ν is a measure γ on $(\mathcal{X}\times\mathcal{X}, \mathcal{F}\otimes\mathcal{F})$ such that for all $A \in \mathcal{F}$, we have $\gamma(A\times X) = \mu(A)$ and $\gamma(X\times A) = \nu(A)$. This definition can be generalized in a natural way to multiple measures.

Our main coupling theorem states that given any adaptive sequence of σ-smooth distributions, $\mathscr{D}$, there is a coupling between a random sequence $(X_1, \ldots, X_T) \sim \mathscr{D}$ and uniformly distributed random variables $Z_i^{(t)}$ such that (with high probability) the set of uniform random variables includes the set of adaptively generated σ-smooth variables.

Theorem 2.1. *Let $\mathscr{D}$ be an adaptive sequence of σ-smooth distribution on $\mathcal{X}$. Then, for each $k > 0$, there is a coupling Π such that $(X_1, Z_1^{(1)}, \ldots, Z_k^{(1)}, \ldots, X_t, Z_1^{(t)}, \ldots, Z_k^{(t)}) \sim \Pi$ satisfy*

a. $X_1, \ldots, X_t$ is distributed according to $\mathscr{D}$.

b. $Z_i^{(j)}$ are uniformly and independently distributed on $\mathcal{X}$.

c. $\{Z_i^{(j)} \mid j \geq t, i \in [k]\}$ are uniformly and independently distributed on $\mathcal{X}$, conditioned on $X_1, \ldots, X_{t-1}$.

d. With probability at least $1 - t(1-\sigma)^k$, $\{X_1, \ldots, X_t\} \subseteq \{Z_i^{(j)} \mid i \in [k], j \in [t]\}$.

The key aspect of this theorem is the monotonicity property $\{X_1, \ldots, X_t\} \subseteq \{Z_i^{(j)} \mid i \in [k], j \in [t]\}$ that holds with high probability. This monotonicity and the fact that $Z_i^{(t)}$ are uniform are the crucial properties that allow us to reduce algorithm design and analysis against online adaptive adversaries to those designed against oblivious stochastic adversaries. We will give examples of how this coupling will be used in Section 2.2.

In the remainder of this section, we give an overview of the construction of this coupling and the proof sketch for Theorem 2.1. For ease of exposition, we give a proof that combines elements of two subsequent works by Haghtalab et al. [40] and Block et al. [26] that generalized and simplified our original proof of this lemma appearing in [42]. Here, we restrict our proof overview to the finite universe $\mathcal{X} = [n]$ and defer the fully general case to Appendix B.

Let us first consider a single round of coupling between a random variable that is uniformly distributed over $S \subseteq [n]$ of size σn, and the uniform random variables over $[n]$. At a high level, this is done via rejection sampling. For a more detailed exploration of the connection to rejection sampling, see [27]. Let $\mathcal{D}$ be a smooth distribution, i.e., $\mathcal{D}(x) \leq \frac{\mathcal{U}(x)}{\sigma} = \frac{1}{n\sigma}$ where $\mathcal{D}(x)$ is the probability of x under $\mathcal{D}$. Draw k samples $Y_1, \ldots, Y_k$ from the uniform distribution on $[n]$. Initialize a set S that is empty. For each i, add Y_i to S with probability $n\sigma\mathcal{D}(Y_i)$. Note that crucially this is a well-defined probability due to smoothness, that is, smoothness implies $\sigma n\mathcal{D}(Y_i) \leq 1$ which allows it to be used as a probability. If S is non-empty, let X be a uniform sample from S. Else, let X be sampled according to $\mathcal{D}$ independent of $Y_1, \ldots, Y_k$.

First, let us show that the distribution of X is indeed $\mathcal{D}$. In the case when S is empty, X is distributed according to $\mathcal{D}$ since it is independently sampled from the distribution. When S is non-empty, let us consider the distribution of Y_i conditioned on the event that they were added to set S. We call this event "Y_i being accepted". The probability that Y_i is accepted is

$$\Pr[Y_i \text{ is accepted}] = \sum_{x \in [n]} \Pr[Y_i = x] \cdot \Pr[Y_i \text{ is accepted } | Y_i = x] = \sum_{x \in [n]} \frac{1}{n} \cdot n\sigma\mathcal{D}(x) = \sigma.$$

Thus, we have

$$\Pr[Y_i = x | Y_i \text{ is accepted}] = \frac{1}{\sigma} \cdot \Pr[Y_i = x] \cdot \Pr[Y_i \text{ is accepted} | Y_i = x] = \frac{1}{\sigma} \cdot \frac{1}{n} \cdot n\sigma\mathcal{D}(x) = \mathcal{D}(x).$$

Thus, any Y_i is distributed according to $\mathcal{D}$. Furthermore, we set $Z_i = Y_i$, which gives the independent uniform distribution.

It remains to show the monotonicity property. Note that we have $X_i \in \{Z_1, \ldots, Z_k\}$ whenever S is non-empty. As we saw above $Y_i \in S$ with probability σ independently of Y_j for $i \neq j$. Thus, we have that the probability that S is empty is given by $(1-\sigma)^k$. This establishes that $X_i \in \{Z_1, \ldots, Z_k\}$ with probability $1 - (1-\sigma)^k$ as required.

Next, we create a coupling for adaptive σ-smooth distributions $\mathscr{D}$. Recall that in this setting an adaptive sequence corresponds to X_τ being sampled uniformly from a distribution

$\mathscr{D}_\tau(X_1, \ldots, X_{\tau-1})$, i.e., the distribution at time τ is adaptively chosen given the earlier realizations. We construct the coupling inductively using the same ideas discussed for the single round coupling, but at each step using $\mathscr{D}_\tau(X_1, \ldots, X_{\tau-1})$. Formally, the coupling is as below:

- For $j = 1 \ldots t$,
  - Draw k samples $Y_1^{(j)}, \ldots, Y_k^{(j)}$ from the uniform distribution.
  - Let $S_j = \emptyset$.
  - For each $Y_i^{(j)}$, add $Y_i^{(j)}$ to S_j with probability $\sigma n \cdot \mathscr{D}_j(X_1, \ldots, X_{j-1})(Y_i^{(j)})$.
  - If $S_j \neq \emptyset$, then sample X_j uniformly from S_j.
  - Else, sample X_j from $\mathscr{D}_j(X_1, \ldots, X_{j-1})$.
  - Set $Z_i^{(j)} = Y_i^{(j)}$ for all i.
- Output $(X_1, Z_1^{(1)}, \ldots, Z_k^{(1)}, \ldots, X_t, Z_1^{(t)}, \ldots, Z_k^{(t)})$.

We prove that this coupling works inductively. Fixing $X_1, \ldots, X_{\tau-1}$, we get $\mathscr{D}_\tau(X_1, \ldots, X_{\tau-1})$. Note that the coupling in stage τ is similar to the single round coupling. From a similar argument, we get that X_τ is distributed according to $\mathscr{D}_\tau(X_1, \ldots, X_{\tau-1})$. Similarly, one can argue that $Z_1^{(\tau)}, \ldots, Z_k^{(\tau)}$ are independent and uniform. The monotonicity property follows from the monotonicity in each stage and a union bound.

The final main property that needs to be argued is that $Z_1^{(\tau)}, \ldots, Z_k^{(\tau)}$ are independent of all the past random variables $X_1, \ldots, X_{\tau-1}$ and $\{Z_i^{(j)} \mid i \in [k], j \leq \tau - 1\}$. The key property needed here is that in the single-round coupling, the distribution of Z_i is oblivious to the choice of the distribution $\mathcal{D}$. We prove this formally in Appendix B. This ensures that $\{Z_i^{(j)} \mid j \geq t, i \in [k]\}$ are uniform and independent of the past.

2.2 The General Framework for Applying the Coupling

In most applications where smoothed analysis has led to significant improvements over the worst-case analysis, these improvements hinge on the proof techniques and algorithmic approaches that leverage the anti-concentration properties of the smoothed input. However, as the process of creating an input becomes more and more adaptive, that is, as the adversary correlates the distribution of the current input with the realizations of earlier inputs and decisions the randomness and anti-concentration properties of the input and the state of the algorithm may weaken. Additionally, correlations between future and past instances present novel challenges to the methodology used against oblivious smooth adversaries, which often rely heavily on the independence of the input. Our coupling approach overcomes these challenges in two ways. First, by coupling an adaptive smooth process with a non-adaptive uniform process, it implicitly shows that anti-concentration properties of the input and the algorithm do not weaken significantly in presence of adaptive adversaries. Second, it allow us to lift algorithmic ideas and proof techniques that have been designed for oblivious smooth or stochastic adversaries to design and analyze algorithms that have to interact with adaptive smooth adversaries.

An important property of our coupling is its monotonicity, i.e., with high probability, $\{X_1, \ldots, X_t\} \subseteq \{Z_i^{(j)} \mid i \in [k], j \in [t]\}$. This monotonicity property paired with the fact that $Z_i^{(t)}$ are i.i.d. uniform variables are especially useful for lifting algorithms and proof techniques from the oblivious world that rely on anti-concentration. That is, if an algorithm's failure mode is only triggered when $X_1, \ldots, X_t$ concentrate, then replacing in $\{Z_i^{(j)} \mid i \in [k], j \in [t]\} \supseteq \{X_1, \ldots, X_t\}$

can only increase the likelihood of hitting the failure mode. On the other hand, i.i.d. uniform random variables $Z_i^{(t)}$s demonstrate excellent anti-concentration properties that are superior to most other offline stochastic or oblivious smooth distributions. This shows that existing techniques and algorithms that work well in the stochastic or oblivious smooth settings will continue to work well for adaptive smooth adversaries.

As a general blueprint for using our coupling for smoothed analysis with adaptive adversaries, first consider how you would handle smooth oblivious or stochastic adversaries and identify steps that rely on an anti-concentration property. Sometimes, this is more easily done by identifying where existing approaches rely on the obliviousness and stochasticity of the adversaries and then finding concentration properties, potential functions, or other monotone set functions that implicitly measure concentration of some measure. Next, apply the coupling to replace T adaptive smooth random variables with Tk i.i.d. uniform random variables and show that the previous anti-concentration (or other monotone properties) are only moderately affected by the fact that we have a larger number of random variables. Finally, use the original algorithm or technique for leveraging anti-concentration and complete the proof.

In the remainder of this section, we show how the above blueprint can be applied to three important examples from online learning, discrepancy, and optimization.

Online Learning. One key property that enables learnability in the offline agnostic, offline PAC, and oblivious smooth online setting is that a hypothesis class $\mathcal{H}$ can be approximated via a finite cover $\mathcal{H}'$ and algorithms such as ERM and Hedge can be run on $\mathcal{H}'$ without incurring a large error [39, 41]. This is due to the fact that the performance of the best hypothesis in $\mathcal{H}$ is closely approximated by the performance of the best hypothesis in $\mathcal{H}'$ when instances are drawn from an offline stochastic or an oblivious sequence of smooth distributions. At the heart of this property is an anti-concentration of measure in the class of symmetric differences between hypotheses $h \in \mathcal{H}$ and their proxies $h' \in \mathcal{H}'$. More formally, for a fixed distribution $\mathcal{D}$, such as the uniform distribution, consider $\mathcal{H}' \subseteq \mathcal{H}$ that is an ϵ-cover of $\mathcal{H}$ with respect to $\mathcal{D}$ so that for every hypothesis $h \in \mathcal{H}$ there is a proxy $h'_h \in \mathcal{H}'$ with $\Pr_{\mathcal{D}}[h(x) \neq h'_h(x)] \leq \epsilon$. The set $\mathcal{H}'$ is a good approximation for $\mathcal{H}$ under distribution $\mathcal{D}$ if not too many instances fall in any symmetric difference, that is, if with high probability,

$$\forall h \in \mathcal{H}, \frac{1}{T}\sum_{t=1}^{T} \mathbb{I}\left[h(x_t) \neq h'_h(x_t)\right] \lesssim \epsilon.$$

In the offline or oblivious smooth online setting this is done by leveraging the independence between x_ts and using techniques from the VC theory to show that each function $h\Delta h_{h'}$ is close to its expectation.

We note that $\max_{h\in\mathcal{H}} \sum_{x\in S} \mathbb{I}[h(x) \neq h'_h(x)]$, which measures concentration, is a monotone set function that only increases when replacing random variables $X_1, \ldots, X_T$ with random variables $\{Z_i^{(t)} \mid i \in [k], t \in [T]\} \supseteq \{X_1, \ldots, X_T\}$. This shows that the concentration of measure over a T-step adaptive smooth sequence of distributions $\mathscr{D}$ is bounded by the concentration of measure over a kT draws from the uniform distribution. We can now use the anti-concentration properties of i.i.d. uniform random variables and techniques from the VC theory (which were used for the oblivious smooth and stochastic case) to show that each function $h\Delta h_{h'}$ is close to its expectation.

Online Discrepancy. Most existing approaches for designing low discrepancy algorithms, such as [18, 21] control and leverage anti-concentration properties of the discrepancy vector and its correlations. In particular, Bansal et al. [18] introduces a potential function Φ_t that, roughly speaking, is $\exp(\lambda d_t^\top W)$ where W is a mixture of the future random variables and test directions. They

use the fact that X_ts are generated i.i.d. from a fixed and known distribution to bound the tail probabilities for $\exp(\lambda d_{t-1}^\top X_t) > \Phi_{t-1}$.

Note that the event $\exp(\lambda d_{t-1}^\top X_t) > \Phi_{t-1}$ is monotone, i.e.,

$$\sum_{i\in[k]} \exp(\lambda d_{t-1}^\top Z_i^{(t)}) \geq \exp(\lambda d_{t-1}^\top X_t),$$

when $X_t \in \{Z_i^{(t)} \mid i \in [k]\}$. Therefore, the coupling argument allows us to bound the tail probability of crossing the threshold $k\Phi_{t-1}$. In other words, we bound the tail probabilities of having large correlation with an adaptive σ-smooth variable X_t in terms of the tail probability of having correlations with at least one of k i.i.d. uniform random variables.

With these tail bounds in place, we now have a high probability event that $\exp\left(\lambda d_{t-1}^\top X_t\right) \leq k\Phi_{t-1}$. Then, as Bansal et al. [18] argues, when Φ_{t-1} is large and as result $\lambda d_{t-1}^\top X_t$ by comparison cannot be large, there will be only a small increase in the potential function. Since Φ_ts also measure correlations with the test vectors, an upper bound on Φ_ts also bounds the discrepancy.

It is important to note that discrepancy itself is not a monotone set function as additional vectors can significantly reduce the discrepancy and stop it from growing it large over time. However, anti-concentration techniques that are at the core of analyzing discrepancy are monotone and therefore can be easily used with our coupling.

Dispersion. At its core, dispersion is an anti-concentration property for the number of function discontinuities that fall in any sufficiently small interval. Existing results of Balcan et al. [13] leverages anti-concentration of oblivious smooth adversaries, who generate independently distributed discontinuities, and argues that the resulting sequence is dispersed with high probability. That is, when the jth discontinuity of the tth function, $d_{t,j}$, is drawn independently, with high probability for all intervals J with small width, $\sum_{t,j} \mathbb{I}\left[d_{t,j} \in J\right]$ is small. Balcan et al. [13] proves this using the independence between $d_{t,j}$s and the fact that VC dimension of the class of intervals is a constant.

In an approach that mirrors our online learning analysis, we emphasize that

$$\max_J \sum_{d_{t,j}\in S}^{T} \mathbb{I}\left[d_{t,j} \in J\right]$$

that measures concentration of function discontinuities is a monotone set function over S and only increases when replacing random variables $d_{i,t}$s with random variables $\{Z_i^{(t,j)} \mid i \in [k], t \in [T], j \in [\ell]\} \supseteq \{d_{t,j} \mid j \in [\ell], t \in [T]\}$. This shows that the concentration of discontinuities over a $T\ell$-step adaptive smooth sequence of distributions $\mathscr{D}$ is bounded by the concentration of discontinuities from a $kT\ell$-step uniform distribution. We can now use the anti-concentration properties of uniform and independent random variables and the fact that the VC dimension of intervals is small to show that adaptive smooth adversaries also create dispersed sequences.

3 REGRET BOUNDS AGAINST SMOOTH ADAPTIVE ADVERSARY

In this section, we obtain regret bounds against adaptive smooth adversaries that are solely defined in terms of VC dimension of the hypothesis class and the smoothness parameter.

Recall that an adaptive adversary at every time step $t \in [T]$ chooses $\mathcal{D}_t$ based on the actions of the learner $h_1, \ldots, h_{t-1}$ and the realizations of the previous instances $(x_1, y_1), \ldots, (x_{t-1}, y_{t-1})$ and then samples $(x_t, y_t) \sim \mathcal{D}_t$. Our main result in this section is as follows.

Theorem 3.1 (Regret Upper Bound). *Let $\mathcal{H}$ be a hypothesis class of VC dimension d. There is an algorithm $\mathcal{A}$ that, for any adaptive sequence of σ-smooth distributions $\mathscr{D}$, achieves a regret of*

$$\mathbb{E}[\textsc{Regret}(\mathcal{A}, \mathscr{D})] \leq \tilde{O}\left(\sqrt{Td \ln\left(\frac{T}{d\sigma}\right)} + d \ln\left(\frac{T}{d\sigma}\right)\right).$$

In the above $\tilde{O}$ hides factors that are $\operatorname{loglog}\left(T/d\sigma\right)$.

We complement this result by providing nearly matching lower bounds. We show that Theorem 3.1 is tight up to a multiplicative polylog(T) and polyloglog$(1/\sigma d)$ factors and an additive $d \log(T/d\sigma)$ term. We provide a proof of Theorem 3.2 in Section 3.4.

Theorem 3.2 (Regret Lower Bound). *For every d and σ such that $d\sigma \leq 1$, there exists a hypothesis class $\mathcal{H}$ with VC dimension d such that for any algorithm $\mathcal{A}$ there is a sequence of σ-smooth distributions $\mathcal{D}$ where*

$$\mathbb{E}[\textsc{Regret}(\mathcal{A}, \mathcal{D})] \in \Omega\left(\sqrt{dT \log\left(\frac{1}{\sigma d}\right)}\right).$$

In order to prove Theorem 3.1, we follow the general approach for using our coupling theorem (Theorem B.2) as outlined in Section 2.2. That is, in Section 3.1, we first review the algorithmic result of Haghtalab [39] for obtaining regret bounds against *non-adaptive* smooth adversaries and identify steps for which non-adaptivity is crucial for that approach. In Section 3.2, we then alter those steps to work for adaptive smooth adversaries via the coupling argument. Lastly, in Section 3.3, we combine the steps to complete the proof of Theorem 3.1.

3.1 Overview of Existing Approaches and their Need for Obliviousness

Haghtalab [39], Haghtalab et al. [41] considered regret-minimization problem against non-adaptive smooth adversaries. This approach considered an algorithm $\mathcal{A}$ that uses Hedge or any other standard no-regret algorithm on a finite set $\mathcal{H}'$. $\mathcal{H}'$ is chosen to be an ϵ-cover of $\mathcal{H}$ with respect to the uniform distribution. It is not hard to see (e.g., [41, Equation (1)]) that regret of algorithm $\mathcal{A}$ decomposes to the regret of Hedge on the cover $\mathcal{H}'$ and the error caused by approximating $\mathcal{H}$ by its cover $\mathcal{H}'$ as follows:

$$\mathbb{E}[\textsc{Regret}(\mathcal{A}, \mathscr{D})] \leq O\left(\sqrt{T \ln(|\mathcal{H}'|)}\right) + \mathbb{E}_{\mathscr{D}}\left[\max_{h \in \mathcal{H}} \min_{h' \in \mathcal{H}'} \sum_{t=1}^{T} 1\left(h(x_t) \neq h'(x_t)\right)\right]. \tag{4}$$

Given that any hypothesis class $\mathcal{H}$ has an ϵ-cover of size $(41/\epsilon)^{\mathrm{VCDim}(\mathcal{H})}$ (see [48] or [30, Lemma 13.6]) the first term of Equation (4) can be directly bounded by $O(\sqrt{T\,\mathrm{VCDim}(\mathcal{H}) \ln(1/\epsilon)})$. To bound the second term of Equation (4), for any $h \in \mathcal{H}$ consider the $h' \in \mathcal{H}'$ that is the proxy for h. Then, define $g_{h,h'} = h \oplus h'$ where $h \oplus h'$ is the function that is 1 if exactly one of h or h' is 1. Note that $\mathbb{E}_{x \sim U}[g_{h,h'}(x)] \leq \epsilon$, where U is the uniform distribution over $\mathcal{X}$. Let $\mathcal{G} = \{g_{h,h'} \mid \forall h \in \mathcal{H}$ and the corresponding proxy $h' \in \mathcal{H}'\}$. Note that,

$$\mathop{\mathbb{E}}_{\mathscr{D}}\left[\sup_{h \in \mathcal{H}} \inf_{h' \in \mathcal{H}'} \sum_{t=1}^{T} 1\left(h(x_t) \neq h'(x_t)\right)\right] \leq \mathop{\mathbb{E}}_{\mathscr{D}}\left[\sup_{g \in \mathcal{G}} \sum_{t=1}^{T} g\left(x_t\right)\right]. \tag{5}$$

Note that for any fixed $g_{h,h'} \in \mathcal{G}$ and even an adaptive sequence of σ-smooth distributions, $\mathbb{E}_{\mathscr{D}}[\sum_{t=1}^{T} g_{h,h'}(x_t)] \leq \sigma^{-1}\,\mathbb{E}_{\mathcal{U}}[\sum_{t=1}^{T} g_{h,h'}(x_t)] \leq T\epsilon/\sigma$.

Up to this point, the above approach applies equally to adaptive and non-adaptive adversaries. It remains to establish that with small probability over all (infinitely many) functions in $\mathcal{G}$, the realized value of g is close to its expected value. This is where existing approaches rely on obliviousness of the adversary. *When the adversary is non-adaptive, instances $x_t \sim \mathcal{D}_t$ are independently (but not necessarily identically) distributed.* Existing approaches such as [39] leverage the independence between the instances. Though the instances are not identically distributed, the independence allows one to adapt standard techniques such as symmetrization to establish uniform convergence. Formally, previous work establishes that when $\boldsymbol{\mathcal{D}}$ is a *non-adaptive* sequence of smooth distributions,

$$\mathop{\mathbb{E}}_{\boldsymbol{\mathcal{D}}}\left[\sup_{g\in\mathcal{G}}\sum_{t=1}^{T} g(x_t)\right] \le \frac{T\epsilon}{\sigma} + O\left(\sqrt{Td\ln\left(\frac{T}{\sigma}\right)}\right). \tag{6}$$

Using $\epsilon = \sigma T^{-1/2}$ in Equations (6) and (4) gives an upper bound on the regret against an oblivious smooth adversary that only depends on VC dimension of $\mathcal{H}$ and the smoothness parameters.

3.2 Reducing Adaptivity to Obliviousness via the Coupling

We emphasize that Equation (6) is the only step in existing approach that relies on the obliviousness of the adversary. In this section, we show how the coupling lemma can be used to obtain an upper bound analogous to the Equation (6) for adaptive adversaries. The main result of this section is as follows,

Lemma 3.3. *Let $\mathcal{G}$ be defined as described in Section 3.1, $d = \mathrm{VCDim}(\mathcal{H})$, and let $\boldsymbol{\mathcal{D}}$ be an adaptive sequence of σ-smooth distributions. We have*

$$\mathop{\mathbb{E}}_{\boldsymbol{\mathcal{D}}}\left[\sup_{g\in\mathcal{G}}\sum_{i=1}^{T} g(x_i)\right] \le O\left(\sqrt{\frac{\epsilon}{\sigma}T\ln(T)\,d\ln\left(1/\epsilon\right)} + T\ln(T)\frac{\epsilon}{\sigma}\right)$$

for any $\epsilon > \frac{\sigma d\log\left(4e^2/\epsilon\right)}{5T\ln(T)}$.

Proof of Lemma 3.3. Here we bound the value of a T-step adaptive process. To prove this lemma, we use the coupling described in Section 2.1 to reduce the problem of bounding the value of a T-step adaptive process by the value of the a $\tilde{O}(T/\sigma)$-step uniform process. We then bound the value of the uniform process using the fact that uniform process is an oblivious process.

Claim 3.4. *Let $\alpha = 10\ln(T)$ and $k = \alpha/\sigma$, and let $\boldsymbol{\mathcal{U}}$ denote the uniform distribution over the domain. We have*

$$\mathop{\mathbb{E}}_{\boldsymbol{\mathcal{D}}}\left[\sup_{g\in\mathcal{G}}\sum_{i=1}^{T} g(x_i)\right] \le T^2(1-\sigma)^{\frac{\alpha}{\sigma}} + \mathop{\mathbb{E}}_{\boldsymbol{\mathcal{U}}}\left[\sup_{g\in\mathcal{G}}\sum_{\substack{i\in[k]\\ j\in[T]}} g\left(Z_i^{(j)}\right)\right].$$

Proof of Claim 3.4. Consider the coupling $X_1,\ldots X_T, Z_1^{(1)},\ldots Z_k^{(T)}$ described in Appendix B.2 for for $k = \alpha/\sigma$ and $\alpha = 10\ln(T)$. We will denote this by Π. First note that every $g \in \mathcal{G}$ is positive, since it is a symmetric difference between two functions h and h'. Therefore, for any two sets A and B, such that $A \subseteq B$, we have

$$\sup_{g\in\mathcal{G}}\sum_{x\in A} g(x) \le \sup_{g\in\mathcal{G}}\sum_{x\in B} g(x)$$

Let $\mathcal{E}$ denote the event $\{X_1, \ldots, X_T\} \notin \{Z_i^{(j)} \mid i \in [k], j \in [T]\}$. From Theorem 2.1, we know that $\Pr[\mathcal{E}] \leq T(1-\sigma)^{\frac{\alpha}{\sigma}}$. Moreover, from Theorem 2.1 we have that $X_1 \ldots X_T$ is distributed according to $\mathscr{D}$ and $Z_i^{(j)}$ are i.i.d. according to $\mathcal{U}$, thus

$$\mathop{\mathbb{E}}_{\mathscr{D}}\left[\sup_{g\in\mathcal{G}}\sum_{i=1}^{T} g(x_i)\right] = \mathop{\mathbb{E}}_{\Pi}\left[\sup_{g\in\mathcal{G}}\sum_{i=1}^{T} g(X_i)\right] \text{ and } \mathop{\mathbb{E}}_{\mathcal{U}}\left[\sup_{g\in\mathcal{G}}\sum_{\substack{i\in[k]\\ j\in[T]}} g\left(Z_i^{(j)}\right)\right] = \mathop{\mathbb{E}}_{\Pi}\left[\sup_{g\in\mathcal{G}}\sum_{\substack{i\in[k]\\ j\in[T]}} g\left(Z_i^{(j)}\right)\right]. \quad (7)$$

Next note that

$$\begin{aligned}
\mathop{\mathbb{E}}_{\Pi}\left[\sup_{g\in\mathcal{G}}\sum_{i=1}^{T} g(X_i)\right] &= \mathop{\mathbb{E}}_{\Pi}\left[\mathbb{I}(\mathcal{E})\cdot\sup_{g\in\mathcal{G}}\sum_{i=1}^{T} g(X_i)\right] + \mathop{\mathbb{E}}_{\Pi}\left[\mathbb{I}\left(\overline{\mathcal{E}}\right)\cdot\sup_{g\in\mathcal{G}}\sum_{i=1}^{T} g(X_i)\right] \\
&\leq T^2(1-\sigma)^{\frac{\alpha}{\sigma}} + \mathop{\mathbb{E}}_{\Pi}\left[\mathbb{I}\left(\overline{\mathcal{E}}\right)\cdot\sup_{g\in\mathcal{G}}\sum_{i=1}^{T} g(X_i)\right] \\
&\leq T^2(1-\sigma)^{\frac{\alpha}{\sigma}} + \mathop{\mathbb{E}}_{\Pi}\left[\mathbb{I}\left(\overline{\mathcal{E}}\right)\cdot\sup_{g\in\mathcal{G}}\sum_{i,j} g\left(Z_i^{(j)}\right)\right] \\
&\leq T^2(1-\sigma)^{\frac{\alpha}{\sigma}} + \mathop{\mathbb{E}}_{\Pi}\left[\sup_{g\in\mathcal{G}}\sum_{i,j} g\left(Z_i^{(j)}\right)\right],
\end{aligned}$$

where the second transition uses the fact that $\Pr[\mathcal{E}] \leq T(1-\sigma)^{\frac{\alpha}{\sigma}}$ and that $\sup_{g\in\mathcal{G}}\sum_{i=1}^{T} g(X_i) \leq T$ given that $\forall g \in \mathcal{G}, g(x) \leq 1$. The third transition uses the fact that conditioned on $\overline{\mathcal{E}}$, $\{X_1, \ldots, X_T\} \subseteq \{Z_i^{(j)} \mid i \in [k], j \in [T]\}$. Using Equation (7) completes the proof of Claim 3.4. □

Claim 3.5. *For any k and any $\epsilon > \frac{120 d \log(4e^2/\epsilon)}{Tk}$, we have*

$$\mathop{\mathbb{E}}_{\mathcal{U}}\left[\sup_{g\in\mathcal{G}}\sum_{i\in[k],j\in[T]} g\left(Z_i^{(j)}\right)\right] \leq 72\sqrt{\epsilon\, T\, k\, d \log\left(1/\epsilon\right)} + T\, k\, \epsilon.$$

Proof sketch of Claim 3.5. The crux of this proof is that random variables $Z_i^{(j)}$ are drawn i.i.d. from the uniform distribution, therefore, standard VC theory arguments provide uniform convergence bounds for them. We use Bernstein-style uniform convergence bound and leverage the fact that for all $g \in \mathcal{G}$, $\mathbb{E}_{\mathcal{U}}[g(Z)] \leq \epsilon$ to get a variance that shrinks with ϵ. That is, in Lemma A.2, we have that error grows as $\tilde{O}(\sqrt{\epsilon T d})$ whereas if just a Hoeffding bound were used, the error would grow as $\tilde{O}(\sqrt{Td})$ which would have resulted in a regret of $\tilde{O}(\sqrt{Td\sigma^{-1}})$ instead of $\tilde{O}(\sqrt{Td\log(1/\sigma)})$. The proof of this claim follows from [30, Theorem 13.7] and is included in Appendix A for completeness. □

Combining Claims 3.4 and 3.5, replacing in values of $\alpha = 10\ln(T)$, $k = \alpha/\sigma$, and $(1-\sigma)^{\alpha/\sigma} \leq \exp(-\alpha)$, we have that

$$\mathop{\mathbb{E}}_{\mathscr{D}}\left[\sup_{g\in\mathcal{G}}\sum_{i=1}^{T} g(x_i)\right] \leq T^2\exp(-\alpha) + O\left(\sqrt{\frac{\epsilon}{\sigma}T\ln(T)d\log\left(1/\epsilon\right)} + T\ln(T)\frac{\epsilon}{\sigma}\right)$$
$$\leq O\left(\sqrt{\frac{\epsilon}{\sigma}T\ln(T)d\log\left(1/\epsilon\right)} + T\ln(T)\frac{\epsilon}{\sigma}\right),$$

where the last transition is due to $T^2\exp(-10\ln(T)) \in o(1)$. This completes the proof of Lemma 3.3. □

3.3 Proof of Theorem 3.1

The proof of Theorem 3.1 follows the proof outline for oblivious smooth adversaries described with Section 3.1 with the exception of using Lemma 3.3 that holds for adaptive smooth adversaries in place of Equation (6) bound.

Let $d = \text{VCDim}(\mathcal{H})$. Using the regret decomposition from Equation (4), an upper bound on the size of an ϵ-cover such as $|\mathcal{H}| \leq (41/\epsilon)^d$ (see [48] or [30, Lemma 13.6]), and Lemma 3.3, we have

$$\mathbb{E}[\textsc{Regret}(\mathcal{A},\mathscr{D})] \leq O\left(\sqrt{Td\ln\left(\frac{1}{\epsilon}\right)}\right) + \mathop{\mathbb{E}}_{\mathscr{D}}\left[\sup_{g\in\mathcal{G}}\sum_{t=1}^{T} g(x_t)\right]$$
$$\leq O\left(\sqrt{Td\ln\left(\frac{1}{\epsilon}\right)} + \sqrt{\frac{\epsilon}{\sigma}T\ln(T)d\log\left(1/\epsilon\right)} + T\ln(T)\frac{\epsilon}{\sigma}\right),$$

Recall that we needed $\epsilon > \frac{120d\sigma\log\left(4e^2/\epsilon\right)}{T\log T}$. This can be satisfied by setting $\epsilon = O(\frac{d\sigma}{T\log T}\log(\frac{T\log T}{d\sigma}))$ and we have that

$$\mathbb{E}[\textsc{Regret}(\mathcal{A},\mathscr{D})] \leq \tilde{O}\left(\sqrt{Td\ln\left(\frac{T}{d\sigma}\right)} + d\ln\left(\frac{T}{d\sigma}\right)\right)$$

as required.

3.4 Proof of Theorem 3.2

In this section, we provide a proof for the tightness of our regret bounds. In order to do this, we first formally define the notion of Littlestone dimension of a class.

Definition 3.1 (Littlestone Dimension, [23]). Let $\mathcal{X}$ be an instance space and $\mathcal{F}$ be a hypothesis class on $\mathcal{X}$. A mistake tree is a full binary decision tree whose internal nodes are labelled by elements of $\mathcal{X}$. For every choice of labels $\{y_i\}_{i=1}^d$, Every root to leaf path in the mistake tree corresponds to a sequence $\{(x_i,y_i)\}_{i=1}^d$ by associating a label y_i to a node depending on whether it is the left or right child of its parent. A mistake tree of depth d is said to be shattered by a class $\mathcal{F}$ if for any root to leaf path $\{(x_i,y_i)\}_{i=1}^d$, there is a function $f\in\mathcal{F}$ such that $f(x_i) = y_i$ for all $i \leq d$. The Littlestone dimension of the class $\mathcal{F}$ denoted by $\text{LDim}(\mathcal{F})$ is the largest depth of a mistake tree shattered by the class $\mathcal{F}$.

As an example, the Littlestone dimension of the class of thresholds on $\{1,\ldots,n\}$ is $\log_2(n)$. The following theorem shows that the Littlestone dimension captures the regret in the online learning

game against a class. We will only need the lower bound but we will state the full theorem for completeness.

Theorem 3.6 ([4, 23]). *Let $\mathcal{X}$ be an instance space and $\mathcal{F}$ be a hypothesis class on $\mathcal{X}$. Then, there exists an online learning algorithm $\mathcal{A}$ such that*

$$\textsc{Regret}(\mathcal{A}) \leq O\left(\sqrt{\text{LDim}(\mathcal{F})\, T}\right).$$

Furthermore, for any algorithm $\mathcal{A}'$, we have that

$$\textsc{Regret}\left(\mathcal{A}'\right) \geq \Omega\left(\sqrt{\text{LDim}(\mathcal{F})\, T}\right).$$

Using the above theorem, we lower bound the regret in the online learning against smoothed adversaries. We do this by reducing the smoothed case to the worst case for a related class and lower bound the worst case regret using the above theorem.

Proof of Theorem 3.2. We will first construct a class on the domain $[1/\sigma] = \{1, \ldots, \frac{1}{\sigma}\}$ with VC dimension d and Littlestone dimension $\Theta(d \log(1/d\sigma))$. For simplicity, assume σ^{-1} and d to be powers of two. Divide $[1/\sigma]$ into d subsets each of equal size, denoted by A_i. On each of these subsets instantiate the class of thresholds, i.e., for each $\gamma \in A_i$, $h_\gamma(x) = \mathbb{I}[x \geq \gamma]$ for $x \in A_i$ and 0 for $x \notin A_i$. For a d-tuple of thresholds $(h_{\gamma_1} \ldots h_{\gamma_d})$ with $\gamma_i \in A_i$, define the function

$$h_{\gamma_1, \ldots, \gamma_d}(x) = \sum_{i=1}^{d} \mathbb{I}[x \in A_i]\, h_{\gamma_i}(x).$$

This function can be seen as the union of the thresholds h_{γ_i}. Define $\mathcal{H}$ to be the class of all such functions. Note that this class has VC dimension d. The VC dimension is at most d since if any more than d points would mean at least one of the A_i must have two points but this cannot be shattered by thresholds on A_i. The VC dimension can be seen to be at least d by taking one point in each of the A_i.

We claim that this class has Littlestone dimension $\Theta(d \log(1/\sigma d))$. At a high level, the Littlestone dimension of the class of thresholds defined over A_i is $\log_2(1/\sigma d)$. Moreover, our definition of a d-tuple threshold is a disjoint union of d thresholds. This allows us to combine the mistake trees for $A_1, \ldots, A_d$, by gluing a copy of the mistake tree for A_{i+1} at each of the leaves of the mistake tree for A_i, recursively. This results in a mistake tree of depth $\Theta(d \log(1/\sigma d))$. For more detail, see Lemma C.1.

Next consider the set $[0, 1]$ and divide it into contiguous subintervals of length σ. We define the projection function $\Pi : [0, 1] \to [1/\sigma]$ by $\Pi(x) = i$ if x is in the ith subinterval. Define the class $\mathcal{G}$ on $[0, 1]$ by composing $\mathcal{H}$ with Π, i.e., $\mathcal{G} = \{g : g = h \circ \Pi\}$. Note that the uniform distribution on each subinterval is σ-smooth. Thus, in a smoothed online learning game with the class $\mathcal{G}$, an adversary who plays only uniform distributions on the subintervals defined above corresponds to an adversary in the worst-case online learning game on $[1/\sigma]$ against class $\mathcal{H}$. In particular, any algorithm for $\mathcal{G}$ against such an adversary can be converted to an algorithm for $\mathcal{H}$ with the same regret. From Theorem 3.6, we have that the regret against $\mathcal{H}$ is lower bounded by

$$\sqrt{T\text{LDim}(\mathcal{H})} = \sqrt{dT \log\left(1/\sigma d\right)}$$

Thus, the regret in the smoothed online learning game for $\mathcal{G}$ is lower bounded by $\sqrt{dT \log\left(1/\sigma d\right)}$ as required. We note that this reduction goes through even for non-adaptive smooth adversaries. □

4 DISCREPANCY

In this section, we consider the online vector balancing problem with adaptive smooth adversaries and achieve bounds that are almost as small as the stochastic setting where instances are drawn from the uniform distributions.

Recall that in the online vector balancing or discrepancy problem, at every round t the algorithm sees a new vector X_t with bounded norm and has to assign a sign $\epsilon_t \in \{-1, 1\}$ to it. The goal of the algorithm is to ensure that for all $t \le T$,

$$\left\| \sum_{i=1}^{t} \epsilon_i X_i \right\|_\infty$$

is small. This problem is studied under different choice of norms, but we restrict our our discussion to the infinity norm. In the adaptive adversarial model, where the adversary's choice of vector X_t could depend on the past choices of the algorithm and the adversary, i.e., $\epsilon_1, \ldots, \epsilon_{t-1}$ and $X_1, \ldots, X_{t-1}$, no algorithm can obtain discrepancy bound of $O(\sqrt{T})$. On the other hand, recent works of Bansal et al. [18] and Alweiss et al. [5] have shown that polylog(nT) discrepancy bounds are achievable when X_ts are drawn from a fixed distribution or are fixed by an oblivious adversary in advance.

We consider the online discrepancy problem under against an adaptive σ-smooth adversary. That is, the adversary chooses a σ-smooth distribution for X_t after having observed $\epsilon_1, \ldots, \epsilon_{t-1}$ and $X_1, \ldots, X_{t-1}$. We also restrict our attention to the isotropic case where the covariance matrix $\mathbb{E}_{X_t}[X_t X_t^\top] = cI$ for some c.

In this section, we give discrepancy bounds that smoothly interpolate between the stochastic and adaptive cases.

Theorem 4.1. *Let $\mathscr{D}$ be an adaptive sequence of σ-smooth distributions, such that the distribution of X_i, with $\|X_i\| \le 1$, at time i is decided after observing $X_1, \ldots, X_{i-1}, \epsilon_1, \ldots, \epsilon_{i-1}$. Furthermore, let $\mathbb{E}_{X_t}[X_t X_t^\top] = cI$ for some some $c \in [0, 1/n]$. Then, there is an online algorithm for deciding the sign ϵ_i of X_i such that with probability $1 - T^{-4}$ for all $t \le T$*

$$\left\| \sum_{i=1}^{t} \epsilon_i X_i \right\| \le O\left(\log^2 \left(\frac{Tn}{\sigma} \right) \right).$$

We complement this upper bound by showing that we cannot get the logarithmic dependence on smoothness parameter σ, n and T simultaneously without further assumptions on the distribution such as isotropy.

Theorem 4.2. *For any online algorithm, there is an adaptive sequence of $\left(1/20n^2T^2\right)$-smooth distributions on the unit ball such that, we have*

$$\left\| \sum_{i=1}^{T} \epsilon_i v_i \right\|_\infty \ge \Omega\left(\sqrt{\frac{T}{n}} \right)$$

with probability $1 - \exp\left(-T/12\right)$.

4.1 Overview of Existing Approaches and their Need for Obliviousness

Bansal et al. [18] consider various versions of the online discrepancy problem where the vectors are chosen stochastically from a fixed known distribution. One such problem is the stochastic online variant of the Komlós problem, where the input vectors come from a fixed distribution supported on the unit Euclidean ball, and the algorithms goal is to minimize the infinity norm of

the discrepancy vector, i.e., $\|d_t\|_\infty$. To do this, Bansal et al. [18] introduced the following potential function

$$\Phi_t = \mathop{\mathbb{E}}_{W\sim p}\left[\cosh\left(\lambda d_t^\top W\right)\right],$$

where p denotes a mixture between sampling from the fixed distribution the vectors are drawn from and the basis vectors e_is. This potential can be seen as the exponential moment of the random variable $d_{t-1}^\top W$ that both bounds $\lambda d_{t-1}^\top X_t \le O\left(\log\left(T\Phi_{t-1}\right)\right)$ and induces an anti-concentration constraint on the correlations of the discrepancy vector d_{t-1}. [18] then uses an algorithm that at time t observes X_t and picks the sign ϵ_t that minimizes the increase in the potential function $\Phi_t - \Phi_{t-1}$, that is $\Delta\Phi = \mathbb{E}_{W\sim p}[\cosh(\lambda(d_{t-1} + \epsilon_t X_t)^\top W)] - \mathbb{E}_{W\sim p}[\cosh(\lambda d_{t-1}^\top W)]$. At the heart of the analysis of [18] is to show that in expectation over the choice ofX_t from the fixed distribution, $\Delta\Phi$ remains small at every time step. It is not hard to see that once the expected increase in the potential is upper bounded, standard martingale techniques can be used to bound the potential and thus the discrepancy at every time step.

To bound $\Delta\Phi$, Bansal et al. [18] considers Taylor expansion of the potential function as follows

$$\Delta\Phi \lesssim \epsilon_t\lambda \mathop{\mathbb{E}}_{W\sim p}\left[\sinh\left(\lambda d_{t-1}^\top W\right) X_t^\top W\right] + \lambda^2 \mathop{\mathbb{E}}_{W\sim p}\left[\left|\sinh\left(\lambda d_{t-1}^\top W\right)\right| \cdot W^\top X_t X_t^\top W\right]. \tag{8}$$

Bansal et al. [18] leverages the the obliviousness of the adversary, i.e., the fact that X_t arrive from a fixed distribution, and isotropy of X to directly bound the linear and quadratic terms of the Taylor expansion as follows.

The second term of Equation (8) is bounded using the isotropy of the vector X_t as follows

$$\lambda^2 \mathop{\mathbb{E}}_{W\sim p}\left|\sinh\left(\lambda d_{t-1}^\top W\right)\right| W^\top X_t X_t^\top W \le \frac{1}{n}\lambda^2 \mathop{\mathbb{E}}_{W\sim p}\left|\sinh\left(\lambda d_{t-1}^\top W\right)\right|.$$

As for the first term of Equation (8), note that since the algorithm picks ϵ_t to minimize the potential rise, it is sufficient to upper bound $\mathbb{E}_{X_t}[-|\lambda\,\mathbb{E}_{W\sim p}[\sinh(\lambda d_{t-1}^\top W)X_t^\top W]|]$. Since the potential is the exponential moment of the $\lambda d_{t-1}^\top X_t$ and X_ts are drawn from an oblivious distribution, we have that $\lambda d_{t-1}^\top X_t \le O(\log(T\Phi_{t-1}))$ with high probability. Thus, we get

$$\begin{aligned}\mathop{\mathbb{E}}_{X_t}\left[\left|\lambda \mathop{\mathbb{E}}_{W\sim p}\sinh\left(\lambda d_{t-1}^\top W\right) X_t^\top W\right|\right] &\gtrsim \frac{1}{\ln(T\Phi_{t-1})}\mathop{\mathbb{E}}_{X_t}\left[\lambda^2 \mathop{\mathbb{E}}_{W\sim p}\left[\sinh\left(\lambda d_{t-1}^\top W\right) d_{t-1}^\top X_t X_t^\top W\right]\right]\\ &\gtrsim \frac{\lambda}{n\ln(T\Phi_{t-1})}\mathop{\mathbb{E}}_{W\sim p}\left[\left|\sinh\left(\lambda d_{t-1}^\top W\right)\right| - 2\right],\end{aligned}$$

using the fact that $a\sinh(a) \ge \left|\sinh(a)\right| - 2$ and the isotopy of the distribution. Summing these two terms, we get

$$\begin{aligned}\Delta\Phi &\lesssim -\frac{\lambda}{n\ln(T\Phi_{t-1})}\mathop{\mathbb{E}}_{W\sim p}\left[\left|\sinh\left(\lambda d_{t-1}^\top W\right)\right| - 2\right] + \frac{1}{n}\lambda^2 \mathop{\mathbb{E}}_{W\sim p}\left|\sinh\left(\lambda d_{t-1}^\top W\right)\right|\\ &\lesssim 2.\end{aligned}$$

We choose λ such that $\lambda^{-1} \le \log(T\Phi_{t-1})$ if $\Phi \le \text{poly}(T)$. This tells us that that if the potential is small, then the change in the potential is small as required.

Let us now review the steps where the obliviousness of the adversary was crucial for the analysis of Bansal et al. [18]. The main step is the definition and the interpretation of the potential function, that controls the moments of $d_{t-1}^\top X_t$ assuming that X_t comes from a fixed distribution and the future vector that are represented in $W \sim p$. That is, obliviousness is primarily used to show that $\lambda d_{t-1}^\top X_t \le O(\ln(T\Phi_{t-1}))$. In an adaptive (smooth) setting where the distribution of X_t and the future vectors differ and are unknown an adversary can correlate X_t and the future vectors with

d_{t-1}. It is not immediately clear how to directly adapt the potential function to account for the an evolving sequence of distributions. A possible approach for directly altering the potential function is to work with the worst-case evolution of smooth distribution across a single time step. This seems both algorithmically challenging to deal with and, as we see next, unnecessary.

4.2 From Adaptive to Oblivious through Coupling

We emphasize that the main step in which Bansal et al. [18] leveraged the obliviousness of the adversary is to show that their potential function defined over random X_t and a random $W \sim p$ that balances between future observations and the standard basis has the property that $\lambda d_{t-1}^\top X_t \leq O(\ln(T\Phi_{t-1}))$. We use the coupling argument to show that a similarly defined potential function in our case also demonstrates the same bounds. The main observation that allows us to move from the oblivious adversary to the adaptive adversary is that the coupling discussed in Section 2.1 gives us a way to upper bound the probability that $d_{t-1}^\top X_t$ is large under an adaptive sequence of smooth distributions in terms of the probability under the uniform distribution.

Let us start by defining the algorithm that obtains our results of Theorem 4.1 analogously to the algorithm of Bansal et al. [18] for the uniform distribution. At step t, our algorithm observes vectors the discrepancy vector d_{t-1} (which is a function of $\epsilon_1 \ldots, \epsilon_{t-1}$ and the previous vectors) and receives a new vector X_t that is to be colored. Let ϵ_t denote the sign that our algorithm will assign to X_t and let $d_t = d_{t-1} + \epsilon_t X_t$. Let p denote the following distribution.

$$\begin{cases} Z \sim \mathcal{U} & \text{with probability } \frac{1}{2} \\ e_i \text{ where } e_i \sim p_{\text{basis}} & \text{with probability } \frac{1}{2} \end{cases},$$

where p_{basis} is the uniform distribution on the standard basis vectors (with both positive and negative signs). Defined the potential function

$$\Phi_t = \mathop{\mathbb{E}}_{W\sim p}\left[\cosh\left(\lambda d_t^\top W\right)\right],$$

for $\lambda = 1000\ln(knT)$ where k is a parameter to be set later. At step t observing X_t our algorithm greedily picks the ϵ_t minimizes the potential difference, that is

$$\Phi_t - \Phi_{t-1} = \mathop{\mathbb{E}}_{W\sim p}\left[\cosh\left(\lambda(d_{t-1} + \epsilon_t X_t)^\top W\right)\right] - \mathop{\mathbb{E}}_{W\sim p}\left[\cosh\left(\lambda d_{t-1}^\top W\right)\right].$$

The following lemma uses the coupling argument to bound the probability tails of $d_{t-1}^\top X_t$.

Lemma 4.3. *Consider any fixed d_{t-1} vector and X_t that is sampled from an arbitrary σ-smooth distribution. Then,*

$$\Pr_{X_t}\left[\lambda d_{t-1}^\top X_t \geq 4\ln\left(\frac{4k\Phi_{t-1}}{\delta}\right)\right] \leq (1-\sigma)^k + \delta.$$

Proof. We will use the coupling from Appendix B. In particular, we can use a single-step coupling from Lemma B.1 that shows that there exists a coupling Π on $(\tilde{X}_t, Z_1^{(t)}, \ldots, Z_k^{(t)})$ such that $\tilde{X}_t$ has the same distribution as $X_t, Z_1^{(t)}, \ldots, Z_k^{(t)}$ are uniformly and independently distributed and with probability at most $(1-\sigma)^k$, we have $\tilde{X}_t \notin \{Z_1^{(t)}, \ldots, Z_k^{(t)}\}$. Let $\mathcal{E}$ denote the event where

$\tilde{X}_t \notin \{Z_1^{(t)}, \ldots, Z_k^{(t)}\}$. Then, for any θ

$$\begin{aligned}
\Pr_{X_t}\left[\lambda d_{t-1}^\top X_t \geq \theta\right] &= \Pr\left[\exp\left(\lambda d_{t-1}^\top X_t\right) \geq \exp(\theta)\right] \\
&= \Pr_{\Pi}\left[\mathcal{E} \wedge \left\{\exp\left(\lambda d_{t-1}^\top \tilde{X}_t\right) \geq \exp(\theta)\right\}\right] + \Pr_{\Pi}\left[\overline{\mathcal{E}} \wedge \left\{\exp\left(\lambda d_{t-1}^\top \tilde{X}_t\right) \geq \exp(\theta)\right\}\right] \\
&\leq (1-\sigma)^k + \Pr_{\Pi}\left[\overline{\mathcal{E}} \wedge \left\{\sum_{i=1}^k \exp\left(\lambda d_{t-1}^\top Z_i^{(t)}\right) \geq \exp(\theta)\right\}\right] \\
&\leq (1-\sigma)^k + \Pr_{\Pi}\left[\sum_{i=1}^k \exp\left(\lambda d_{t-1}^\top Z_i^{(t)}\right) \geq \exp(\theta)\right] \\
&\leq (1-\sigma)^k + \exp(-\theta)\mathop{\mathbb{E}}_{\Pi}\left[\sum_{i=1}^k \exp\left(\lambda d_{t-1}^\top Z_i^{(t)}\right)\right] \qquad \text{(By Markov inequality)} \\
&\leq (1-\sigma)^k + 2\exp(-\theta)\mathop{\mathbb{E}}_{\Pi}\left[\sum_{i=1}^k \cosh\left(\lambda d_{t-1}^\top Z_i^{(t)}\right)\right] \qquad \text{(By } \exp(x) \leq 2\cosh(x)\text{)} \\
&\leq (1-\sigma)^k + 4\exp(-\theta)\sum_{i=1}^k \mathop{\mathbb{E}}_{W\sim p}\left[\cosh\left(\lambda d_{t-1}^\top W\right)\right] \qquad (p \text{ is w.p. } 0.5 \text{ uniform}) \\
&\leq (1-\sigma)^k + 4k\Phi_{t-1}\exp(-\theta),
\end{aligned}$$

Setting $\theta = \ln(\frac{4k\Phi_{t-1}}{\delta})$ completes the proof. □

4.3 Proof of Theorem 4.1

Our proof follows the same approach as that of Bansal et al. [18] outlined in Section 4.1 and aims to bound $\mathbb{E}_{X_t}[\Phi_t] - \Phi_{t-1}$ at every time step. The main technical challenge is to upperbound the linear term $\mathbb{E}_{X_t}[-|L(X_t)|]$ in $\Delta\Phi_t$ as a function of the correlation between d_{t-1} and X_t drawn from a σ-smooth distribution. We then use our Lemma 4.3 that controls this correlation to bound the linear term.

Recall from Section 4.2 that our algorithm observes X_t and picks the ϵ_t that minimizes the potential difference, that is

$$\Phi_t - \Phi_{t-1} = \mathop{\mathbb{E}}_{W\sim p}\left[\cosh\left(\lambda(d_{t-1} + \epsilon_t X_t)^\top W\right)\right] - \mathop{\mathbb{E}}_{W\sim p}\left[\cosh\left(\lambda d_{t-1}^\top W\right)\right].$$

The next lemma shows that when the potential at time $t-1$ is small, the expected increase in Φ_t over the choice of X_t is small.

Lemma 4.4. *At any time t, if $\Phi_{t-1} \leq T^6$, then $\mathbb{E}_{X_t}[\Phi_t] - \Phi_{t-1} \leq 2$.*

Proof. Denote $\Delta\Phi = \Phi_t - \Phi_{t-1}$. As in [18], we decompose this as

$$\begin{aligned}\Delta\Phi(X_t) &= \mathop{\mathbb{E}}_{W\sim p}\left[\cosh\left(\lambda(d_{t-1}^\top + \epsilon_t X_t)W\right)\right] - \mathop{\mathbb{E}}_{W\sim p}\left[\cosh\left(\lambda(d_{t-1}^\top)W\right)\right] \\ &\le \epsilon_t\lambda \mathop{\mathbb{E}}_{W\sim p}\left[\sinh\left(\lambda d_{t-1}^\top W\right)X_t^\top W\right] + \lambda^2 \mathop{\mathbb{E}}_{W\sim p}\left[\left|\sinh\left(\lambda d_{t-1}^\top W\right)\right| W^\top X_t X_t^\top W\right] \\ &\quad + \lambda^2 \mathop{\mathbb{E}}_{W\sim p}\left[W^\top X_t X_t^\top W\right].\end{aligned}$$

Using notation similar to that of Bansal et al. [18], we will denote the first term in last equation as $\epsilon_t L(X_t)$, the second as $Q(X_t)$ and the third as $Q_*(X_t)$. We need to upper bound $\mathbb{E}_{X_t}[\Delta\Phi(X_t)]$ and thus it suffices to bound these three quantities.

Our approach for upper bounding $\mathbb{E}_{X_t}[Q(X_t)]$ and $\mathbb{E}_{X_t}[Q_*(X_t)]$ is similar to that of Bansal et al. [18] and uses that fact that the distribution of X is isotropic (without the need to bring in smoothness). We state these bounds in the following claim and include the proof of them for completeness in Appendix D.

Claim 4.5. *Let Q and Q_* be defined as above. Then,*

$$\mathop{\mathbb{E}}_{X_t}\left[Q(X_t)\right] \le c\lambda^2 \mathop{\mathbb{E}}_{W\sim p}\left[\left|\sinh\left(\lambda d_{t-1}^\top W\right)\right|\right] \quad \text{and} \quad \mathop{\mathbb{E}}_{X_t}\left[Q_*(X_t)\right] \le \frac{c\lambda^2}{n}.$$

To upper bound $\mathbb{E}[\epsilon_t L(X_t)]$, we need to use both the smoothness of X_t and their isotropic nature. First note that since ϵ_t is chosen to minimize the potential drop, we can bound $\mathbb{E}_{X_t}\left[\epsilon_t L(X_t)\right] \le -\mathbb{E}_{X_t}\left[\left|L(X_t)\right|\right]$. So it's sufficient to lower bound $\mathbb{E}_{X_t}\left[\left|L(X_t)\right|\right]$.

Claim 4.6. *Let L be defined as above. Then,*

$$\mathop{\mathbb{E}}_{X_t}\left[\left|L(X_t)\right|\right] \ge \frac{c\lambda}{\ln\left(4k\Phi_{t-1}/\delta\right)} \mathop{\mathbb{E}}_{W\sim p}\left[\left|\sinh\left(\lambda d_{t-1}^\top W\right)\right|\right] - 1$$

Proof of Claim 4.6. Let $B = \ln\left(4k\Phi_{t-1}/\delta\right)$ and let G be the event that $\lambda\left|d_{t-1}^\top X_t\right| \le B$. Note that $\left|L(X_t)\right| \ge L(X_t)\cdot f(X_t)/\left\|f\right\|_\infty$ for any function f. We will use the function $f(X_t) = d_{t-1}^\top X_t \cdot \mathbb{I}[X_t \in G]$ and note that $\left\|f\right\|_\infty \le B/\lambda$. This allows us to decompose $|L|$ further as follows.

$$\begin{aligned}\mathop{\mathbb{E}}_{X_t}\left[\left|L(X_t)\right|\right] &\ge \mathop{\mathbb{E}}_{X_t}\left[\frac{\lambda^2}{B}\mathop{\mathbb{E}}_{W\sim p}\left[\sinh\left(\lambda d_{t-1}^\top W\right) d_{t-1}^\top X_t X_t^\top W \cdot \mathbb{I}(X_t \in G)\right]\right] \\ &= \frac{\lambda^2}{B}\mathop{\mathbb{E}}_{W\sim p}\left[\sinh\left(\lambda d_{t-1}^\top W\right) d_{t-1}^\top \mathop{\mathbb{E}}_{X_t}[X_t X_t^\top] W\right] \\ &\quad - \frac{\lambda^2}{B}\mathop{\mathbb{E}}_{W\sim p}\left[\sinh\left(\lambda d_{t-1}^\top W\right) d_{t-1}^\top \mathop{\mathbb{E}}_{X_t}\left[X_t X_t^\top \mathbb{I}(X_t \notin G)\right] W\right].\end{aligned}$$

Looking at the second term in the above equation and using the fact that X is an isotropic distribution and Lemma 4.3 (which used the smoothness of X), we have

$$\left\|\mathop{\mathbb{E}}_{X_t}\left[X_t X_t^\top \mathbb{I}(X_t \notin G)\right]\right\|_{\text{op}} \le \Pr[X_t \notin G] \le (1-\sigma)^k + \delta.$$

Ensuring that $k >> \sigma^{-1}\ln(1/\delta)$ by $k = 100\sigma^{-1}\ln\left(T\ln(T)\right)$ and noting that $\|d_{t-1}\| \le T$

$$d_{t-1}^\top \mathop{\mathbb{E}}_{X_t}\left[X_t X_t^\top \mathbb{I}(X_t \notin G)\right] W \le 2\delta T.$$

Picking $\delta^{-1} = 2\lambda\Phi_{t-1}T$, we get

$$\lambda\left|d_{t-1}^\top \mathop{\mathbb{E}}_{X_t}\left[X_tX_t^\top \mathbb{I}\left(X_t \notin G\right)\right] W\right| \le \Phi_{t-1}^{-1}.$$

Now let us consider the first term of the above decomposition. Using the fact that X is an isotropic random variable, we have

$$\begin{aligned}\frac{\lambda^2}{B}\mathop{\mathbb{E}}_{W\sim p}\left[\sinh\left(\lambda d_{t-1}^\top W\right) d_{t-1}^\top \mathop{\mathbb{E}}_{X_t}[X_tX_t^\top]W\right] &= \frac{c\lambda}{B}\mathop{\mathbb{E}}_{W\sim p}\left[\sinh\left(\lambda d_{t-1}^\top W\right)\lambda d_{t-1}^\top W\right]\\ &\ge \frac{c\lambda}{B}\mathop{\mathbb{E}}_{W\sim p}\left[\left|\sinh\left(\lambda d_{t-1}^\top W\right)\right| - 2\right],\end{aligned}$$

where the last inequality used the fact that $a\sinh(a) \ge \left|\sinh(a)\right| - 2$. Putting the inequalities together, we get

$$\begin{aligned}\mathop{\mathbb{E}}_{X_t}\left[\left|L\left(X_t\right)\right|\right] &\ge \frac{c\lambda}{B}\mathop{\mathbb{E}}_{W\sim p}\left[\left|\sinh\left(\lambda d_{t-1}^\top W\right)\right| - 2\right] - \frac{c\lambda}{B}\Phi_{t-1}^{-1}\mathop{\mathbb{E}}_{W\sim p}\left[\left|\sinh\left(\lambda d_{t-1}^\top W\right)\right|\right]\\ &\ge \frac{c\lambda}{B}\mathop{\mathbb{E}}_{W\sim p}\left[\left|\sinh\left(\lambda d_{t-1}^\top W\right)\right|\right] - \frac{2c\lambda}{B} - \frac{\lambda}{B}\\ &\ge \frac{c\lambda}{B}\mathop{\mathbb{E}}_{W\sim p}\left[\left|\sinh\left(\lambda d_{t-1}^\top W\right)\right|\right] - 1,\end{aligned}$$

where the second transition is by the definition of Φ_{t-1} and the third transition is by the values of $\lambda^{-1} = 1000\ln(knT)$, $B = \ln(8\lambda kT\Phi_{t-1}^2)$, and the assumption that $\Phi_{t-1} \le T^6$. This completes the proof of Claim 4.6. □

We now use Claims 4.5 and 4.5 to finish the proof of Lemma 4.4 as follows.

$$\begin{aligned}\mathop{\mathbb{E}}_{X_t}\left[\Delta\Phi\left(X_t\right)\right] &\le \mathop{\mathbb{E}}_{X_t}\left[-|L| + Q + Q_*\right]\\ [5pt] &\le -\frac{c\lambda}{B}\mathop{\mathbb{E}}_{W\sim p}\left[\left|\sinh\left(\lambda d_{t-1}^\top W\right)\right|\right] + 1 + c\lambda^2\mathop{\mathbb{E}}_{W\sim p}\left[\left|\sinh\left(\lambda d_{t-1}^\top W\right)\right|\right] + \frac{c\lambda^2}{n}\\ &\le 2\end{aligned}$$

Here, we use the fact that $\lambda \le B^{-1}$ which follows from $\lambda^{-1} = 1000\ln(knT)$, $B = \ln(8\lambda kT\Phi_{t-1}^2)$, and the assumption that $\Phi_{t-1} \le T^6$. This completes the proof of Lemma 4.4. □

Note that the above argument gives us $\mathbb{E}_{X_t}\left[\Delta\Phi|\Phi_{t-1}\right] \le 2$ given that $\Phi_{t-1} \le T^6$. We truncate Φ_t at T^6, i.e., setting $\tilde{\Phi}_t = \Phi_t$ till $\Phi_t \le T^6$ and $\tilde{\Phi}_t = T^6$ afterwards. Using this and the Doob maximal martingale inequality, it follows that $\Phi_t \le T^6$ with probability $1 - T^4$ as required.

Next, we will see why bounding the potential suffices to bound the discrepancy. Recall that the potential was defined as $\Phi_t = \mathbb{E}_{W\sim p}[\cosh(\lambda d_t^\top W_i)]$. Since with probability $1/2$, p samples uniformly from the set of basis vectors p_{basis} and given that $\exp(x) \le 2\cosh(x)$, we have $\exp(\lambda\left|d_t^\top e_i\right|) \le \sum_{i=1}^n \exp(\lambda\left|d_t^\top e_j\right|) \le 8n\Phi_t$ for all basis vectors e_j. Thus, we have

$$\|d_t\|_\infty = \left\|\sum_{i=1}^t \epsilon_i X_i\right\| \le \lambda^{-1}\ln\left(4n\Phi_t\right).$$

Recall that $\lambda^{-1} = 1000 \ln(\frac{nT \ln(T)}{\sigma})$, which gives us that

$$\left\| \sum_{i=1}^{t} \epsilon_i X_i \right\| \leq \tilde{O}\left(\ln^2 \left(\frac{nT}{\sigma} \right) \right)$$

as required.

4.4 Proof of Theorem 4.2

Here, we show that the isotropy condition is required for our online discrepancy upper bound. Recall that the worst-case adversary for discrepancy generated vectors that were orthogonal to the current discrepancy vector at each time. The idea for this proof is that even with the smoothness requirements, the adversary can generate vectors such that the inner products are concentrated near zero, leading to high discrepancy. Let the discrepancy vector at time t be denoted by d_t. Consider the set $S_t = \{x : \|x\|_2 \leq 1, \left|\langle x, d_{t-1}\rangle\right| \leq n^{-2}T^{-2}\|d_{t-1}\|_2\}$. Note that the uniform distribution on S_t is $cn^{-2}T^{-2}$ smooth for some constant c. To see this, let $\mathcal{U}$ denote the uniform distribution on the unit ball and let V_n denote the volume of the unit ball in n dimensions. Then,

$$\begin{aligned}
\Pr_{X \sim \mathcal{U}}[X \in S_t] &= \frac{1}{V_n} \int_{-n^{-2}T^{-2}}^{n^{-2}T^{-2}} \left(1 - x^2\right)^{\frac{n-1}{2}} V_{n-1} dx \\
&\geq \frac{1}{V_n} \int_{-n^{-2}T^{-2}}^{n^{-2}T^{-2}} \left(1 - \frac{1}{n^4T^4}\right)^{\frac{n-1}{2}} V_{n-1} dx \\
&\geq \frac{V_{n-1}}{V_n} \cdot \frac{1}{2n^2T^2} \\
&\geq \frac{1}{20n^2T^2}.
\end{aligned}$$

The second inequality follows by noting that $(1 - n^{-4}T^{-4})^{\frac{n-1}{2}} \geq 1/4$. With this, we describe the adversary's strategy. At time t, the adversary picks v_t uniformly from S_t. We will measure the squared 2-norm of the discrepancy vector.

$$\begin{aligned}
\|d_t\|_2^2 &= \|\epsilon_t v_t + d_{t-1}\|_2^2 \\
&= \epsilon_t^2 \|v_t\|_2^2 + \|d_{t-1}\|_2^2 + 2\langle v_t, d_t \rangle \\
&\geq \|v_t\|_2^2 + \|d_{t-1}\|_2^2 - \frac{2\|d_{t-1}\|_2}{n^2T^2} \\
&\geq \|v_t\|_2^2 + \|d_{t-1}\|_2^2 - \frac{2}{n^2T} \\
&\geq \sum_{i=1}^{t} \|v_i\|_2^2 - \frac{2t}{n^2T}.
\end{aligned}$$

Note that $\Pr\left[\|v_i\|_2 \leq 1/2\right] \leq 2^{-(n-1)}$. This can be seen by noting that the probability can be computed with an integral similar to the one above but with ball of radius $1/2$ instead of the ball of radius 1. Also, note that the lengths $\|v_i\|_2$ are independent across i (even though v_i themselves are not independent). Denote z_i as a random variable which is 1 if $\|v_i\| \geq 1/2$ and 0 otherwise. Then,

$$\sum_{i=1}^{t} \|v_i\|_2^2 \geq \frac{1}{4} \sum_{i=1}^{t} z_i.$$

Applying a Chernoff bound to z_i, we get

$$\Pr\left[\sum_{i=1}^{t}\|v_i\|_2^2 \le \frac{t}{8}\left(1-2^{-(d-1)}\right)\right] \le e^{-\frac{t}{12}}.$$

Thus with probability $1-e^{-\frac{t}{12}}$,

$$\|d_t\|_2^2 \ge \frac{t}{16} - \frac{2t}{n^2T} \ge \frac{t}{20}.$$

We get the desired result by relating the 2-norm and ∞-norm.

This shows that we cannot get the logarithmic dependence on smoothness parameter σ, n and T simultaneously without further assumptions on the distribution such as isotropy.

5 ADAPTIVE SMOOTH ADVERSARIES AND DISPERSED SEQUENCES

In this section, we consider the problem of online optimization and show that adaptive smooth adversaries create *dispersed* sequences. Recall that in the online optimization settings, an adversary chooses a sequence of functions $u_1, \ldots, u_T$ such that $u_t : \mathcal{X} \to [0,1]$ and the learner responds by taking instances $x_1, \ldots, x_T \in \mathcal{X}$ with a goal of minimizing the regret. The main theorem of this section shows that when u_is are piecewise Lipschitz functions and are chosen by an adaptive smooth adversary in such a way that the discontinuities of these functions are is smoothed, the resulting sequence of functions is dispersed.

Theorem 5.1 (Adaptive Smoothness Leads to Dispersion). *Let $u_1, \ldots, u_T$ be functions from $[0,1] \to \mathbb{R}$ that are piecewise Lipschitz with ℓ discontinuities each. Let $d_{i,j}$ denote the discontinuities of u_i and that are sampled from an adaptive sequence of σ-smooth distributions. Then, for any $\alpha \ge 0.5$, with probability $1-\delta$ the sequence of functions $u_1 \ldots u_T$ is (w,k)-dispersed for*

$$w = \sigma(T\ell)^{\alpha-1} \quad \text{and} \quad k = \tilde{O}\left((T\ell)^{\alpha}\ln\left(\frac{1}{\delta}\right) + \ln\left(\frac{1}{\sigma}\right)\right).$$

5.1 Overview of Balcan et al. [13] and the Need for Obliviousness

Balcan et al. [13, Lemma 13] showed a similar result to Theorem 5.1 but for sequences that are generated by an oblivious smooth adversary. The crux of their argument is showing that for the number of points that can lie in any ball of small radius is small when these points are drawn *independently* from a non-adaptive sequence of σ-smooth distributions. More formally, they show that ℓ points are picked from a non-adaptive sequence of σ-smooth distributions over $[0,1]$, then with probability $1-\delta$, any interval of width w contains at most

$$O\left(\frac{T\ell w}{\sigma} + \sqrt{T\ell\log\left(\frac{1}{\delta}\right)}\right) \tag{9}$$

points. Setting $w = \sigma(T\ell)^{\alpha-1}$ for an $\alpha \ge 0.5$ then [13] showed that for a *non-adaptive* smooth adversary, with probability $1-\delta$, $u_1 \ldots u_T$ is $(\sigma(T\ell)^{\alpha-1}, O((T\ell)^{\alpha}\ln(\frac{1}{\delta})))$-dispersed.

The only step in the existing analysis that requires the adversary to be non-adaptive is that of proving Equation (9). Here, Balcan et al. [13] relies on the obliviousness of the adversary an uses the fact that points drawn from a non-adaptive sequence of smooth distributions are independently (but not identically) distributed. Their approach leverages this independence between the instances and the fact that VC dimension of intervals is 2 to use the double sampling and symmetrization tricks from VC theory and establish a uniform convergence property on the number of instances that can fall in any interval of width w.

5.2 Reducing Adaptivity to Obliviousness for Dispersion via the Coupling

We emphasize that Equation (9) is the only step in the existing approach that relies on the obliviousness of the adversary. In this section, we show how the coupling lemma can be used to obtain (almost) the same upper bound as of Equation (9) for adaptive adversaries. Our approach is essentially the same as the proof of Lemma 3.3 used for regret minimization, where we had to bound the expected maximum number of smooth adaptive instances that can fall in any function $g \in \mathcal{G}$ of bounded VC dimension. In this case, we can apply the same results to the class of intervals, which has a VC dimension of 2, and bound the number of discontinuities than fall in any interval. We make another small change to our previous approach to achieve high probability bounds instead of bounds on the expectation.

Lemma 5.2. *Let $\mathcal{J}$ be the set of all intervals of width at most w over $[0,1]$. For $i \in [T]$ and $j \in [\ell]$, let $d_{i,j}$ be drawn from a $T\ell$-step adaptive sequence of σ-smooth random variables over $[0,1]$. Then, with probability $1-\delta$,*

$$\max_{J\in\mathcal{J}} \sum_{\substack{i\in[T]\\ j\in[\ell]}} \mathbb{I}\left[d_{i,j}\in J\right] < \frac{T\ell w}{\sigma}\ln\left(\frac{2T\ell}{\delta}\right) + 10\sqrt{\frac{T\ell w}{\sigma}\ln\left(\frac{2T\ell}{\delta}\right)\ln\left(\frac{1}{\delta}\right)} + 10\log\left(\frac{10T\ell\log\left(2T\ell/\delta\right)}{\sigma\delta}\right)$$

Proof. Let $\mathscr{D}$ represent the $T\ell$-step adaptive sequence of σ-smooth distributions from which $d_{i,j}$s are drawn. Let $k = \frac{\ln(2T\ell/\delta)}{\sigma}$ and consider the coupling Π described in Appendix B.2 over $(d_{i,j}, Z_1^{(i,j)} \dots Z_k^{(i,j)})_{i\in[T],j\in[\ell]}$, where $d_{i,j}$s are distributed according to $\mathscr{D}$ and $Z_m^{(i,j)}$s are distributed according to the uniform distribution over $[0,1]$. Let $\mathcal{E}$ be the event $\{d_{i,j} \mid \forall i \in [T], j \in [\ell]\} \nsubseteq \{Z_m^{(i,j)} \mid \forall m \in [k], i \in [T], j \in [\ell]\}$. By Theorem 2.1, $\Pr[\mathcal{E}] \le T\ell(1-\sigma)^k$.

We now bound the probability that the number of instances $d_{i,j}$s that fall in any interval of size w is bigger than a threshold θ, using the coupling argument. We have

$$\begin{aligned}
\Pr_{\mathscr{D}}\left[\max_{J\in\mathcal{J}}\sum_{i,j}\mathbb{I}\left[d_{i,j}\in J\right]\ge\theta\right] &= \Pr_{\Pi}\left[\max_{J\in\mathcal{J}}\sum_{i,j}\mathbb{I}\left[d_{i,j}\in J\right]\ge\theta\right]\\
&= \Pr_{\Pi}\left[\mathcal{E}\wedge\max_{J\in\mathcal{J}}\sum_{i,j}\mathbb{I}\left[d_{i,j}\in J\right]\ge\theta\right]\\
&\quad+\Pr_{\Pi}\left[\overline{\mathcal{E}}\wedge\max_{J\in\mathcal{J}}\sum_{i,j}\mathbb{I}\left[d_{i,j}\in J\right]\ge\theta\right]\\
&\le T\ell\,(1-\sigma)^k+\Pr_{\Pi}\left[\overline{\mathcal{E}}\wedge\max_{J\in\mathcal{J}}\sum_{i,j}\mathbb{I}\left[d_{i,j}\in J\right]\ge\theta\right]\\
&\le T\ell\,(1-\sigma)^k+\Pr_{\Pi}\left[\overline{\mathcal{E}}\wedge\max_{J\in\mathcal{J}}\sum_{i,j,m}\mathbb{I}\left[Z_m^{(i,j)}\in J\right]\ge\theta\right]\\
&\le T\ell\,(1-\sigma)^k+\Pr_{\Pi}\left[\max_{J\in\mathcal{J}}\sum_{i,j,m}\mathbb{I}\left[Z_m^{(i,j)}\in J\right]\ge t\right].
\end{aligned}$$

Now, using uniform convergence bounds (see e.g., [31, Page 201]) for $\mathcal{J}$, which has a VC dimension of 2 and the fact that for any $J \in \mathcal{J}$, $\Pr[Z_m^{(i,j)} \in J] \leq w$, we have that

$$\Pr_{\mathcal{U}}\left[\max_{J\in\mathcal{J}} \sum_{i,j,m} \mathbb{I}\left[Z_m^{(i,j)} \in J\right] \geq T\ell kw + 10\sqrt{T\ell wk \ln(T\ell k/\delta)} + 10\log\left(10T\ell k/\delta\right)\right] \leq \frac{\delta}{2}.$$

Replacing in values of $k = \frac{\ln(2T\ell/\delta)}{\sigma}$ and using the result of the above coupling, we have

$$\Pr\left[\max_{J\in\mathcal{J}} \sum_{i,j} \mathbb{I}\left[d_{i,j} \in J\right] \geq \frac{T\ell w}{\sigma}\log\left(\frac{2T\ell}{\delta}\right) + 10\sqrt{\frac{Tw\ell}{\sigma}\log\left(\frac{2T\ell}{\delta}\right)\ln\left(\frac{1}{\delta}\right)} + 10\log\left(\frac{10T\ell\log\left(2T\ell/\delta\right)}{\sigma\delta}\right)\right] \leq \delta$$

as required. □

5.3 Proof of Theorem 5.1

The proof of this theorem follows directly from Lemma 5.2 and by setting $w = \sigma(T\ell)^{\alpha-1}$ for $\alpha \geq 0.5$. □

We note that Theorem 5.1 shows that even adaptive smooth adversaries generate sequence of functions that are sufficiently dispersed. This result enables us to directly tap into the results and algorithms of Balcan et al. [13] that show that online optimizing on any dispersed sequence enjoys improved runtime and regret bounds.

APPENDICES

A UNIFORM CONVERGENCE BOUNDS UNDER INDEPENDENCE

Lemma A.1 (Lemma 13.5 and Theorem 13.7 in [30]). *Let $\mathcal{A}$ be a countable class of measurable subsets of $\mathcal{X}$ with $\text{VCDim}(\mathcal{A}) = d$. Let $Z_1, \ldots Z_n$ be independent random variables taking values in $\mathcal{X}$. Assume that $\Pr[X_i \in A] \leq \epsilon$ for all $A \in \mathcal{A}$. Let*

$$Q = \frac{1}{\sqrt{n}} \sup_{A\in\mathcal{A}} \sum_{i=1}^{n} \left(\mathbb{I}\left[X_i \in A\right] - \Pr\left[X_i \in A\right]\right).$$

Then,

$$\mathbb{E}\left[Q\right] \leq 72\sqrt{\epsilon d \log\left(\frac{4e^2}{\epsilon}\right)}$$

whenever $\epsilon \geq \frac{120d\log\left(\frac{4e^2}{\epsilon}\right)}{n}$.

We use the above theorem to get the required bound for the expected maximum of the process indexed by a VC class under our coupling.

Lemma A.2. *Let $\mathcal{G}$ be a class with $\text{VCDim}(\mathcal{G}) = d$ and $g \in \mathcal{G}$, $\mathbb{E}\, g(\gamma) \leq \epsilon$ where γ is uniformly distributed. Then, for $\{\gamma_i\}_{i\in[Tk]}$ independently and uniformly distributed,*

$$\mathbb{E}\left[\sup_{g\in\mathcal{G}} \sum_{i} g\left(\gamma_i\right)\right] \leq 72\sqrt{\epsilon Tkd\log\left(1/\epsilon\right)} + Tk\epsilon$$

for $\epsilon > \frac{120d\log\left(4e^2/\epsilon\right)}{Tk}$.

Proof. Consider the random variable $Q = \frac{1}{\sqrt{Tk}}[\sup_{g\in\mathcal{G}} \sum_{i=1}^{Tk} g(\gamma_i) - \mathbb{E}[g(\gamma_i)]]$ where γ_i are independent uniform random variables. Note that $\mathbb{E}[g(\gamma_i)] \le \epsilon$. Note that this satisfies the conditions of Lemma A.1 Thus,

$$\mathbb{E}\left[Q\right] \le 72\sqrt{\epsilon d \log\left(\frac{4e^2}{\epsilon}\right)},$$

whenever $\epsilon \ge \frac{120d\log(\frac{4e^2}{\epsilon})}{Tk}$. Thus, we have

$$\mathbb{E}\left[\sup_{g\in\mathcal{G}} \sum_{i=1}^{Tk} g\left(\gamma_i\right) - \mathbb{E}\left[g\left(\gamma_i\right)\right]\right] \le 72\sqrt{\epsilon Tkd \log\left(\frac{4e^2}{\epsilon}\right)}.$$

Recalling that $\mathbb{E}\left[g\left(\gamma_i\right)\right] \le \epsilon$, we get the desired result. □

B COUPLING ARGUMENT

In this section, we will produce a coupling between a adaptive sequence of σ-smooth distributions $\mathscr{D}$ and independent draws from the uniform distribution. In fact, we will prove the argument for a more general setting where smoothness is defined with respect to a general measure μ over the domain $\mathcal{X}$. This proof is based on a generalization and simplification by Block et al. [26] and Haghtalab et al. [40] of our original coupling argument that appeared in [42].

That is, a distribution $\mathcal{D}$ is σ-smooth with respect to μ if for any $S \subseteq \mathcal{X}$, we have $\mathcal{D}(S) \le \frac{\mu(S)}{\sigma}$. Using the Radon-Nikodym theorem, we can prove that this is equivalent to

$$\frac{d\mathcal{D}}{d\mu} \le \frac{1}{\sigma}$$

where $\frac{d\mathcal{D}}{d\mu}$ represents the Radon-Nikodym derivative of $\mathcal{D}$ with respect to μ. For readers unfamilar with measure-theoretic notation, it suffices to think of $\frac{d\mathcal{D}}{d\mu}$ as the ratio of either the probability density functions or the probability mass functions of $\mathcal{D}$ and μ. In particular, for uniform distributions this corresponds to Definition 1.1.

B.1 Warm-up: Coupling for a Single Round

As a warm-up, let us look at the coupling for a single smooth distribution $\mathcal{D}$. Consider the following coupling.

- Draw k samples $Y_1 \dots Y_k$ from μ.
- Initialize $S = \emptyset$.
- For each i, add Y_i to S with probability $\sigma \cdot \frac{d\mathcal{D}}{d\mu}$.
- If S is non-empty, pick X_1 randomly from S. Else, then sample X_1 independently from $\mathcal{D}$.
- Output $(X_1, Z_1, \dots Z_k)$.

The key thing to note is that the above algorithm is well-defined due to smoothness. That is, smoothness implies $\sigma\frac{d\mathcal{D}}{d\mu} \le 1$ which allows it to be used as a probability. In the following lemma, we capture the required properties of the coupling.

Lemma B.1. *Let $(X_1, Z_1, \dots Z_k)$ be as above. Then,*

a. X_1 is distributed according to $\mathcal{D}$.
b. Z_i is distributed according to μ.

c. Furthermore, $Z_1, \ldots, Z_k$ are independent.
d. With probability $1-(1-\sigma)^k$, $X_1 \in \{Z_1, \ldots, Z_k\}$.

Proof. For any set $A \subset \mathcal{X}$, we have

$$\begin{aligned}
\Pr[X_1 \in A] &= \Pr[S \text{ is empty}] \Pr\left[X_1 \in A | S \text{ is empty}\right] \\
&\quad + \Pr\left[X_1 \in A | S \text{ is non-empty}\right] \cdot \Pr[S \text{ is non-empty}] \\
&= \Pr[S \text{ is empty}]\mathcal{D}(A) + \Pr\left[Y_i \in A | Y_i \in S\right] \cdot \Pr[S \text{ is non-empty}] \\
&= \Pr[S \text{ is empty}]\mathcal{D}(A) + \frac{\Pr\left[Y_i \in S | Y_i \in A\right] \cdot \Pr[Y_i \in A] \cdot \Pr[S \text{ is non-empty}]}{\Pr[Y_i \in S]} \\
&= \Pr[S \text{ is empty}]\mathcal{D}(A) + \frac{\int_A \sigma \frac{d\mathcal{D}}{d\mu} d\mu \cdot \Pr[S \text{ is non-empty}]}{\Pr[Y_i \in S]} \\
&= \Pr[S \text{ is empty}]\mathcal{D}(A) + \frac{\int_A \sigma \frac{d\mathcal{D}}{d\mu} d\mu \cdot \Pr[S \text{ is non-empty}]}{\int_{\mathcal{X}} \sigma \frac{d\mathcal{D}}{d\mu} d\mu} \\
&= \Pr[S \text{ is empty}]\mathcal{D}(A) + \Pr[S \text{ is non-empty}]\mathcal{D}(A) \\
&= \mathcal{D}(A).
\end{aligned}$$

This proves that the distribution of X_1 is $\mathcal{D}$. The distribution Z_i according to μ and their independence follows from that of Y_i.

Finally, note that $X_1 \notin \{Z_1, \ldots, Z_k\}$ only if S is empty. For each Y_i, we saw above that the $\Pr[Y_i \in S] = \int_{\mathcal{X}} \sigma \frac{d\mathcal{D}}{d\mu} d\mu = \sigma$. Thus, the probability that S is empty is bounded by $(1-\sigma)^k$ as required. □

B.2 Adaptive Coupling

Moving to the case of a sequence of distributions, given a smooth sequence of distribution $\mathscr{D}$, we would like to find a coupling with a sequence of independent samples from the uniform distribution. We first note that an adaptively chosen sequence of distribution $\mathscr{D}$ corresponds to a sequence of distributions $\mathscr{D}_i$ such that $X_i \sim \mathscr{D}_i$ where $\mathscr{D}_i$ depends on the instantiations of X_j for $j < i$. To make this dependence explicit will denote this as $\mathscr{D}_i(X_1, \ldots X_{i-1})$. We would like to construct a coupling similar to the one in Appendix B.1. Consider the following coupling.

— For $j = 1 \ldots t$,
  – Draw k samples $Y_1^{(j)}, \ldots, Y_k^{(j)}$ from μ.
  – Initialized $S_j = \emptyset$.
  – For each i, add $Y_i^{(j)}$ to S_j with probability $\sigma \cdot \frac{d\mathscr{D}_j(X_1, \ldots, X_{j-1})}{d\mu}$.
  – If S_j is non-empty, pick X_j randomly from S_j. Else, then sample X_j independently from $\mathscr{D}_j\left(X_1, \ldots, X_{j-1}\right)$.
  – Set $Z_i^{(j)} = Y_i^{(j)}$.
— Output $(X_1, Z_1^{(1)}, \ldots, Z_k^{(1)}, \ldots, X_t, Z_1^{(t)}, \ldots, Z_k^{(t)})$.

Theorem B.2. *Let $(X_1, Z_1^{(1)}, \ldots, Z_k^{(1)}, \ldots, X_t, Z_1^{(t)}, \ldots, Z_k^{(t)})$ be as above. Then,*
a. $X_1, \ldots, X_t$ is distributed according $\mathscr{D}$.
b. $Z_i^{(j)}$ are distributed independently according to μ.

c. *Furthermore,* $\{Z_i^{(j)} \mid j \geq t, i \in [k]\}$ *are independently distributed as* μ*, conditioned on* $X_1, \ldots, X_{t-1}$.

d. *With probability at least* $1 - t\,(1-\sigma)^k$, $\{X_1, \ldots, X_t\} \subseteq \{Z_i^{(j)}\}_{i \in [k], j \in [t]}$.

Proof. To see that $X_1 \ldots X_t$ is distributed according to $\mathscr{D}$, note that from the construction and Lemma B.1, we have that conditioned on $X_1 \ldots X_{j-1}$, X_j is distributed according to $\mathscr{D}_j(X_1, \ldots, X_{i-1})$ as required.

Note that $Z_i^{(j)} = Y_i^{(j)}$, and their distribution does not depend on $X_1 \ldots X_{j-1}$, we have that $Z_i^{(j)}$ are independently distributed according to μ even conditioned on $X_1 \ldots X_{j-1}$.

As in Lemma B.1, we have that the probability that $X_j \notin \{Z_i^{(j)}\}$ is bounded by $(1-\sigma)^k$. By the union bound, we have

$$\Pr\left[\exists j : X_j \notin \{Z_i^{(j)}\}\right] \leq t \cdot (1-\sigma)^k$$

as required. □

C PROOFS FROM SECTION 3

Lemma C.1. *Let* $\mathcal{H}$ *be the class defined on* $\left[1/\sigma\right]$ *as the disjoint union of* d *thresholds as in Section 3.4. Then, the Littlestone dimension of* $\mathcal{H}$ *is lower bounded by* $\Omega(\sqrt{d \log(1/d\sigma)})$.

Proof. In order to prove this associate to each string $\{0,1\}^{d \log(1/\sigma d)}$ a function in $\mathcal{H}$ as follows. Partition the string into blocks of size $\frac{1}{\sigma d}$. We think of each of these blocks as forming a binary search tree for the subset A_i by associating 1 to the right child of a node and 0 to the left child. Thus, every path on this tree corresponds to a threshold by associating it with the threshold consistent with the labels along the path. Doing this association separately for each block, we can associate the set of strings $\{0,1\}^{d \log(1/\sigma d)}$ with a binary search tree with the leaves labeled by elements in $\mathcal{H}$. Also, note that this forms a fully shattered tree as required by the definition of the Littlestone dimension. Thus, the Littlestone dimension of $\mathcal{H}$ is $d \log\left(1/\sigma d\right)$. □

D PROOFS FROM SECTION 4

Lemma D.1 ([18]).

$$\mathop{\mathbb{E}}_{X_t}\left[Q\left(X_t\right)\right] \leq c\lambda^2 \mathop{\mathbb{E}}_{W \sim p}\left|\sinh\left(\lambda d_{t-1}^\top W\right)\right|$$

and

$$\mathop{\mathbb{E}}_{X_t}\left[Q_*\left(X_t\right)\right] \leq \frac{c\lambda^2}{n}$$

Proof.

$$\begin{aligned}
\mathop{\mathbb{E}}_{X_t}\left[Q\left(X_t\right)\right] &= \mathop{\mathbb{E}}_{X_t}\left[\lambda^2 \mathop{\mathbb{E}}_{W \sim p}\left|\sinh\left(\lambda d_{t-1}^\top W\right)\right| W^\top X_t X_t^\top W\right] \\
&= \lambda^2 \mathop{\mathbb{E}}_{W \sim p}\left|\sinh\left(\lambda d_{t-1}^\top W\right)\right| W^\top \mathop{\mathbb{E}}_{X_t}\left[X_t X_t^\top\right] W \\
&= c\lambda^2 \mathop{\mathbb{E}}_{W \sim p}\left|\sinh\left(\lambda d_{t-1}^\top W\right)\right|
\end{aligned}$$

Similarly,

$$\begin{aligned}\mathop{\mathbb{E}}_{X_t}\left[Q_*(X_t)\right] &= \mathop{\mathbb{E}}_{X_t}\left[\lambda^2 \mathop{\mathbb{E}}_{W\sim p} W_j^\top X_t X_t^\top W\right] \\ &\leq \frac{c}{n}\lambda^2\end{aligned}$$

as required. □

ACKNOWLEDGMENTS

This work was partially done while Haghtalab and Shetty were visitors at the Simons Institute for the Theory of Computing.

REFERENCES

[1] Naman Agarwal, Nataly Brukhim, Elad Hazan, and Zhou Lu. 2020. Boosting for control of dynamical systems. In *Proceedings of the 37th International Conference on Machine Learning, (ICML'20)*, Vol. 119. PMLR, 96–103.

[2] Naman Agarwal, Elad Hazan, Anirudha Majumdar, and Karan Singh. 2021. A regret minimization approach to iterative learning control. In *Proceedings of the 38th International Conference on Machine Learning (ICML'21)*, Vol. 139. PMLR, 100–109.

[3] Zeyuan Allen-Zhu, Zhenyu Liao, and Lorenzo Orecchia. 2015. Spectral sparsification and regret minimization beyond matrix multiplicative updates. In *Proceedings of the 47th Annual ACM on Symposium on Theory of Computing (STOC'15)*. 237–245.

[4] Noga Alon, Omri Ben-Eliezer, Yuval Dagan, Shay Moran, Moni Naor, and Eylon Yogev. 2021. Adversarial laws of large numbers and optimal regret in online classification. In *Proceedings of the 53rd Annual ACM Symposium on Theory of Computing (STOC'21)*. 447–455.

[5] Ryan Alweiss, Yang P. Liu, and Mehtaab Sawhney. 2021. Discrepancy minimization via a self-balancing walk. In *53rd Annual ACM Symposium on Theory of Computing (STOC'21)*. 14–20.

[6] Sanjeev Arora, Rong Ge, and Ankur Moitra. 2012. Learning topic models – going beyond SVD. In *Proceedings of the 53rd Annual Symposium on Foundations of Computer Science (FOCS'12)*. 1–10.

[7] Sanjeev Arora, Elad Hazan, and Satyen Kale. 2012. The multiplicative weights update method: A meta-algorithm and applications. *Theory of Computing* 8, 6 (2012), 121–164.

[8] David Arthur and Sergei Vassilvitskii. 2006. How slow is the k-means method?. In *Proceedings of the 22nd Symposium on Computational Geometry (SoCG'06)*. 144–153.

[9] Pranjal Awasthi, Maria-Florina Balcan, Nika Haghtalab, and Ruth Urner. 2015. Efficient learning of linear separators under bounded noise. In *Conference on Learning Theory (COLT'15)*. 167–190.

[10] Pranjal Awasthi, Maria-Florina Balcan, Nika Haghtalab, and Hongyang Zhang. 2016. Learning and 1-bit compressed sensing under asymmetric noise. In *Conference on Learning Theory (COLT'16)*. 152–192.

[11] Pranjal Awasthi, Avrim Blum, Nika Haghtalab, and Yishay Mansour. 2017. Efficient PAC learning from the crowd. In *Conference on Learning Theory (COLT'17)*. 127–150.

[12] Maria-Florina Balcan, Avrim Blum, and Anupam Gupta. 2013. Clustering under approximation stability. *J. ACM* 60, 2, Article 8 (May 2013), 34 pages.

[13] Maria-Florina Balcan, Travis Dick, and Ellen Vitercik. 2018. Dispersion for data-driven algorithm design, online learning, and private optimization. In *Proceedings of the 59th Annual Symposium on Foundations of Computer Science (FOCS'18)*. 603–614.

[14] Maria-Florina Balcan, Nika Haghtalab, and Colin White. 2020. K-center clustering under perturbation resilience. *ACM Trans. Algorithms* 16, 2, Article 22 (March 2020), 39 pages.

[15] Nikhil Bansal. 2010. Constructive algorithms for discrepancy minimization. In *Proceedings of the 51st Annual Symposium on Foundations of Computer Science (FOCS'10)*. 3–10.

[16] Nikhil Bansal, Daniel Dadush, Shashwat Garg, and Shachar Lovett. 2018. The Gram-Schmidt walk: A cure for the Banaszczyk blues. In *Proceedings of the 50th Annual ACM Symposium on Theory of Computing (STOC'18)*. 587–597.

[17] Nikhil Bansal and Shashwat Garg. 2017. Algorithmic discrepancy beyond partial coloring. In *Proceedings of the 49th Annual ACM Symposium on Theory of Computing (STOC'17)*. 914–926.

[18] Nikhil Bansal, Haotian Jiang, Raghu Meka, Sahil Singla, and Makrand Sinha. 2021. Online discrepancy minimization for stochastic arrivals. In *Proceedings of the 2021 ACM-SIAM Symposium on Discrete Algorithms (SODA'21)*. 2842–2861.

[19] Nikhil Bansal, Haotian Jiang, Raghu Meka, Sahil Singla, and Makrand Sinha. 2022. Prefix discrepancy, smoothed analysis, and combinatorial vector balancing. In *13th Innovations in Theoretical Computer Science Conference (ITCS'22) (LIPIcs, Vol. 215)*. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 13:1–13:22.

[20] Nikhil Bansal, Haotian Jiang, Raghu Meka, Sahil Singla, and Makrand Sinha. 2022. Smoothed analysis of the Komlós conjecture. In *49th International Colloquium on Automata, Languages, and Programming (ICALP'22) (LIPIcs, Vol. 229)*. 14:1–14:12.

[21] Nikhil Bansal, Haotian Jiang, Sahil Singla, and Makrand Sinha. 2020. Online vector balancing and geometric discrepancy. In *Proceedings of the 52nd Annual ACM Symposium on Theory of Computing (STOC'20)*. 1139–1152.

[22] Nikhil Bansal and Joel H. Spencer. 2020. On-line balancing of random inputs. *Random Struct. Algorithms* 57, 4 (2020), 879–891.

[23] Shai Ben-David, Dávid Pál, and Shai Shalev-Shwartz. 2009. Agnostic online learning. In *Proceedings of the 22nd Annual Conference on Learning Theory (COLT'09)*.

[24] Aditya Bhaskara, Aidao Chen, Aidan Perreault, and Aravindan Vijayaraghavan. 2019. Smoothed analysis in unsupervised learning via decoupling. In *Proceedings of the 60th Annual Symposium on Foundations of Computer Science (FOCS'19)*. 582–610.

[25] Yonatan Bilu and Nathan Linial. 2012. Are stable instances easy? *Combinatorics, Probability and Computing* 21, 5 (2012), 643–660.

[26] Adam Block, Yuval Dagan, Noah Golowich, and Alexander Rakhlin. 2022. Smoothed online learning is as easy as statistical learning. In *Conference on Learning Theory (COLT'22)*, Vol. 178. PMLR, 1716–1786.

[27] Adam Block and Yury Polyanskiy. 2023. The sample complexity of approximate rejection sampling with applications to smoothed online learning. In *Conference on Learning Theory (COLT'23)*, Vol. 195. PMLR, 228–273.

[28] Adam Block and Max Simchowitz. 2022. Efficient and near-optimal smoothed online learning for generalized linear functions. In *Advances in Neural Information Processing Systems (NeurIPS'22)*. 36, 7477–7489.

[29] Avrim Blum and Yishay Mansour. 2007. Learning, regret minimization, and equilibria. In *Algorithmic Game Theory*, Noam Nisan, Tim Roughgarden, Eva Tardos, and Vijay V. Editors Vazirani (Eds.). Cambridge University Press, 79–102.

[30] Stéphane Boucheron, Gábor Lugosi, and Pascal Massart. 2013. *Concentration Inequalities: A Nonasymptotic Theory of Independence*. OUP Oxford.

[31] Olivier Bousquet, Stéphane Boucheron, and Gábor Lugosi. 2003. Introduction to statistical learning theory. In *Summer School on Machine Learning*. Springer, 169–207.

[32] Mark Bun, Roi Livni, and Shay Moran. 2020. An equivalence between private classification and online prediction. In *Proceeding of the 61st Annual Symposium on Foundations of Computer Science (FOCS'20)*. 389–402.

[33] Nicolò Cesa-Bianchi and Gábor Lugosi. 2006. *Prediction, Learning, and Games*. Cambridge University Press.

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

[35] Vincent Cohen-Addad and Varun Kanade. 2017. Online optimization of smoothed piecewise constant functions. In *Proceedings of the 20th International Conference on Artificial Intelligence and Statistics (AISTATS'17)*. 412–420.

[36] Ofer Dekel, Arthur Flajolet, Nika Haghtalab, and Patrick Jaillet. 2017. Online learning with a hint. In *Advances in Neural Information Processing Systems (NeurIPS'17)*. 30, 5299–5308.

[37] Ilias Diakonikolas, Themis Gouleakis, and Christos Tzamos. 2019. Distribution-independent PAC learning of halfspaces with Massart noise. In *Advances in Neural Information Processing Systems (NeurIPS'19)*. 32, 4749–4760.

[38] Rishi Gupta and Tim Roughgarden. 2017. A PAC approach to application-specific algorithm selection. *SIAM J. Comput.* 46, 3 (2017), 992–1017.

[39] Nika Haghtalab. 2018. *Foundation of Machine Learning, by the People, for the People*. Ph. D. Dissertation. Carnegie Mellon University.

[40] Nika Haghtalab, Yanjun Han, Abhishek Shetty, and Kunhe Yang. 2022. Oracle-efficient online learning for beyond worst-case adversaries. In *Advances in Neural Information Processing Systems (NeurIPS'22)*. 36, 4072–4084.

[41] Nika Haghtalab, Tim Roughgarden, and Abhishek Shetty. 2020. Smoothed analysis of online and differentially private learning. In *Advances in Neural Information Processing Systems (NeurIPS'20)*. 34, 9203–9215.

[42] Nika Haghtalab, Tim Roughgarden, and Abhishek Shetty. 2021. Smoothed analysis with adaptive adversaries. In *Proceedings of the 62nd Annual Symposium on Foundations of Computer Science (FOCS'21)*. 942–953.

[43] Nika Haghtalab, Tim Roughgarden, and Abhishek Shetty. 2021. Smoothed analysis with adaptive adversaries. *CoRR* abs/2102.08446 (2021).

[44] Moritz Hardt, Katrina Ligett, and Frank McSherry. 2012. A simple and practical algorithm for differentially private data release. In *Advances in Neural Information Processing Systems (NeuRIPS'12)*. 25, 2348–2356.

[45] Moritz Hardt and Aaron Roth. 2013. Beyond worst-case analysis in private singular vector computation. In *Proceedings of the 45th Annual ACM Symposium on Theory of Computing (STOC'13)*. 331–340.

[46] Moritz Hardt and Guy N. Rothblum. 2010. A multiplicative weights mechanism for privacy-preserving data analysis. In *Proceeding of the 51st Annual Symposium on Foundations of Computer Science (FOCS'10)*. 61–70.

[47] Christopher Harshaw, Fredrik Sävje, Daniel A. Spielman, and Peng Zhang. 2019. Balancing covariates in randomized experiments using the Gram-Schmidt walk. *CoRR* abs/1911.03071 (2019). arXiv:1911.03071
[48] David Haussler. 1995. Sphere packing numbers for subsets of the Boolean n-cube with bounded Vapnik-Chervonenkis dimension. *Journal of Combinatorial Theory, Series A* 69, 2 (1995), 217–232.
[49] Elad Hazan and Tomer Koren. 2016. The computational power of optimization in online learning. In *Proceedings of the 48th Annual ACM Symposium on Theory of Computing (STOC'16)*. 128–141.
[50] Samuel B. Hopkins, Jerry Li, and Fred Zhang. 2020. Robust and heavy-tailed mean estimation made simple, via regret minimization. In *Advances in Neural Information Processing Systems (NeuRIPS'20)*. 30, 11902–11912.
[51] Victor Reis Janardhan Kulkarni and Thomas Rothvoss. 2024. Optimal online discrepancy minimization. In *Proceedings of the 56th Annual ACM Symposium on Theory of Computing (STOC'24)*.
[52] Haotian Jiang, Janardhan Kulkarni, and Sahil Singla. 2019. Online geometric discrepancy for stochastic arrivals with applications to envy minimization. *CoRR* abs/1910.01073 (2019). arXiv:1910.01073
[53] Adam Tauman Kalai, Alex Samorodnitsky, and Shang-Hua Teng. 2009. Learning and smoothed analysis. In *Proceedings of the 50th Symposium on Foundations of Computer Science (FOCS'09)*. 395–404.
[54] Adam Tauman Kalai and Shang-Hua Teng. 2008. Decision trees are PAC-learnable from most product distributions: A smoothed analysis. *CoRR* abs/0812.0933 (2008). arXiv:0812.0933
[55] Sampath Kannan, Jamie H. Morgenstern, Aaron Roth, Bo Waggoner, and Zhiwei Steven Wu. 2018. A smoothed analysis of the greedy algorithm for the linear contextual bandit problem. In *Advances in Neural Information Processing Systems (NeurIPS'18)*. 31, 2227–2236.
[56] Victor Klee and George J. Minty. 1972. How good is the simplex algorithm. *Inequalities* 3, 3 (1972), 159–175.
[57] Akshay Krishnamurthy, Alekh Agarwal, Tzu-Kuo Huang, Hal Daumé III, and John Langford. 2019. Active learning for cost-sensitive classification. *J. Mach. Learn. Res.* 20 (2019), 65:1–65:50.
[58] Shachar Lovett and Raghu Meka. 2015. Constructive discrepancy minimization by walking on the edges. *SIAM J. Comput.* 44, 5 (2015), 1573–1582.
[59] Konstantin Makarychev, Yury Makarychev, and Aravindan Vijayaraghavan. 2014. Bilu–Linial stable instances of max cut and minimum multiway cut. In *Proceedings of the 25th Annual ACM-SIAM Symposium on Discrete Algorithms (SODA'14)*. 890–906.
[60] Bodo Manthey. 2021. *Smoothed Analysis of Local Search*. Cambridge University Press, 285–308.
[61] Rafail Ostrovsky, Yuval Rabani, Leonard J. Schulman, and Chaitanya Swamy. 2013. The effectiveness of Lloyd-type methods for the k-means problem. *J. ACM* 59, 6, Article 28 (2013).
[62] Manish Raghavan, Aleksandrs Slivkins, Jennifer Vaughan Wortman, and Zhiwei Steven Wu. 2018. The externalities of exploration and how data diversity helps exploitation. In *Proceedings of the 31st Conference On Learning Theory (COLT'18)*. 1724–1738.
[63] Alexander Rakhlin and Karthik Sridharan. 2013. Optimization, learning, and games with predictable sequences. In *Advances in Neural Information Processing Systems (NeurIPS'13)*. 26, 3066–3074.
[64] Alexander Rakhlin, Karthik Sridharan, and Ambuj Tewari. 2011. Online learning: Stochastic, constrained, and smoothed adversaries. In *Advances in Neural Information Processing Systems (NeurIPS'11)*. 24, 1764–1772.
[65] Thomas Rothvoss. 2017. Constructive discrepancy minimization for convex sets. *SIAM J. Comput.* 46, 1 (2017), 224–234.
[66] Tim Roughgarden. 2020. *Beyond the Worst-Case Analysis of Algorithms*. Cambridge University Press.
[67] Alejandro A. Schäffer. 1991. Simple local search problems that are hard to solve. *SIAM Journal on Computing* 20, 1 (1991), 56–87.
[68] Joel Spencer. 1994. *Ten Lectures on the Probabilistic Method* (2nd edition). Society for Industrial and Applied Mathematics.
[69] Daniel A. Spielman and Shang-Hua Teng. 2004. Smoothed analysis: Why the simplex algorithm usually takes polynomial time. *J. ACM* 51, 3 (2004), 385–463.
[70] Aravindan Vijayaraghavan, Abhratanu Dutta, and Alex Wang. 2017. Clustering stable instances of Euclidean k-means. In *Advances in Neural Information Processing Systems (NeurIPS'17)*. 30, 6500–6509.

Received 1 December 2022; revised 12 November 2023; accepted 21 February 2024