List Decodable Mean Estimation in Nearly Linear Time

Yeshwanth Cherapanamjeri, Sidhanth Mohanty, Morris Yau

Electrical Engineering and Computer Science
University of California at Berkeley
Berkeley, USA
{yeshwanth,sidhanth,morrisyau}@berkeley.edu

Abstract—Learning from data in the presence of outliers is a fundamental problem in statistics. Until recently, no computationally efficient algorithms were known to compute the mean of a high dimensional distribution under natural assumptions in the presence of even a small fraction of outliers. In this paper, we consider robust statistics in the presence of overwhelming outliers where the majority of the dataset is introduced adversarially. With only an $\alpha < 1/2$ fraction of "inliers" (clean data) the mean of a distribution is unidentifiable. However, in their influential work, [1] introduces a polynomial time algorithm recovering the mean of distributions with bounded covariance by outputting a succinct list of $O(1/\alpha)$ candidate solutions, one of which is guaranteed to be close to the true distributional mean; a direct analog of 'List Decoding' in the theory of error correcting codes. In this work, we develop an algorithm for list decodable mean estimation in the same setting achieving up to constants the information theoretically optimal recovery, optimal sample complexity, and in nearly linear time up to polylogarithmic factors in dimension. Our conceptual innovation is to design a descent style algorithm on a nonconvex landscape, iteratively removing minima to generate a succinct list of solutions. Our runtime bottleneck is a saddle-point optimization for which we design custom primal dual solvers for generalized packing and covering SDP's under Ky-Fan norms, which may be of independent interest. We refer the reader to [2] for the full version of this paper.

Keywords—High-dimensional Statistics, Robust Estimation, Semidefinite Programming, Mathematical Optimization, Spectral Methods.

I. INTRODUCTION

Estimating the mean of data is a cardinal scientific task. The population mean can be shifted arbitrarily by a single outlier, a problem which is compounded in high dimensions where outliers can conspire to destroy the performance of even sophisticated estimators of central tendency. Robust statistics, beginning with the works of Tukey and Huber [3], [4], endeavors to design, model, and mitigate the effect of data deviating from statistical assumptions [5].

A canonical model of data corruption is the Huber contamination model [4]. Let $I(\mu)$ be a probability distribution parameterized by $\mu$. We say a dataset $X_1, X_2, \ldots, X_N$ is $\alpha$-Huber contaminated for some constant $\alpha \in [0, 1]$ if it is drawn i.i.d from $X_1, X_2, \ldots, X_N \sim \alpha I(\mu) + (1-\alpha)\mathcal{O}$ where $\mathcal{O}$ is an arbitrary outlier distribution which can be adversarial and dependent on $I(\mu)$. The goal is to estimate $\mu$ with an estimator $\hat{\mu}$ such that the two are close with respect to a meaningful metric. The Huber contamination model captures the setting where only an $\alpha$ fraction of the dataset is subject to statistical assumptions. One would hope to design estimators $\hat{\mu}$ for which $\alpha$ is as small as possible thereby tolerating the largest fraction of outliers--a quantity known as the breakdown point. The study of estimators with large breakdown points is the focus of a long and extensive body of work, which we do not attempt to survey here. For review see [5], [6].

A first observation, is that the breakdown point of a single estimator must be smaller than $1/2$. For concreteness, consider the problem of estimating the mean of a standard normal. The adversary can set up a mixture of $1/\alpha$ standard normals for which the means of the mixture components are far apart. This intrinsic difficulty also gives rise to a natural notion of recovery in the presence of overwhelming outliers. Instead of outputting a single estimator, consider outputting a list of candidate estimators $L = \{\hat{\mu}_1, \hat{\mu}_2, \ldots, \hat{\mu}_L\}$ with the guarantee that the true $\mu$ is amongst the elements of the list. This is the setting of 'List Decodable Learning' [7], [1], analogous to list decoding in the theory of error correcting codes.

In their influential work [1] introduces list decodable learning in the context of robust statistics. They consider the problem of estimating the mean $\mu$ of a $d$-dimensional distribution $I(\mu)$ with a bounded covariance $\text{Cov}(I(\mu)) \preceq \sigma^2 I$ for a constant $\sigma$ from $N = \frac{d}{\alpha}$ samples. Their algorithm recovers a list $L$ of $O(\frac{d}{\alpha})$ candidate means with the guarantee that there exists a $\hat{\mu}^* \in L$ achieving the recovery guarantee $||\hat{\mu}^* - \mu|| \lesssim O\left(\sigma \sqrt{\frac{\log(\frac{1}{\alpha})}{\alpha}}\right)$ with high probability $1 - \frac{1}{\text{poly}(d)}$. Furthermore, their algorithm is ‘efficient’, running in time $\text{poly}(N, d, \frac{1}{\alpha})$ via the polynomial time solvability of ellipsoidal convex programming.

A. Results

Our first contribution is an algorithm for list decodable mean estimation of covariance bounded distributions, which outputs a list $L$ of length $O(\frac{d}{\alpha})$, achieving (up to constants) the information theoretically optimal recovery $O(\frac{\sigma}{\sqrt{\alpha}})$, with
linear sample complexity \( N = \frac{d}{\alpha} \), and running in nearly linear time \( O(N \text{poly}(\frac{1}{\alpha})) \) where \( O \) omits logarithmic factors in \( d \). For the matching minimax \( \Omega(\frac{\alpha}{\sqrt{1-\alpha}}) \) lower bound see [8]. Formally, we state our main theorem.

**Theorem 1.1.** Let \( \mathcal{I}(\mu) \) be a distribution in \( \mathbb{R}^d \) with unknown mean \( \mu \in \mathbb{R} \) and bounded covariance \( \text{Cov}(\mathcal{I}(\mu)) \leq \sigma^2 I \) for a constant \( \sigma \in \mathbb{R}^+ \). Let \( \mathcal{L} := \{x_1, x_2, ..., x_N \} \) be a dataset in \( \mathbb{R}^d \) drawn i.i.d from \( \mathcal{I}(\mu) \). An adversary then selects an arbitrary dataset in \( \mathbb{R}^d \) denoted \( O := \{x'_1, x'_2, ..., x'_{(1-\alpha)N} \} \) which in particular, may depend on \( \mathcal{L} \). The algorithm is presented with the full dataset \( X := \mathcal{I} \cup \mathcal{O} \).

For any \( N \geq \frac{d}{\alpha} \), we give an algorithm outputs a list \( \mathcal{L} = \{\hat{\mu}_1, \hat{\mu}_2, ..., \hat{\mu}_{O(\frac{1}{\alpha})}\} \) of length \( O(\frac{1}{\alpha}) \) such that there exists a \( \hat{\mu}^* \in \mathcal{L} \) satisfying \( \|\hat{\mu}^* - \mu\| \leq O\left(\frac{\sigma}{\sqrt{\alpha}}\right) \) with high probability \( 1 - \frac{1}{\alpha^{d/2}} \). Furthermore, the algorithm runs in time \( O(N \text{poly}(\frac{1}{\alpha})) \).

For precise constants and failure probability see Section 4 of the full version. At a high level, we define a nonconvex cost function for which \( \mu \) is an approximate minimizer and build a ‘descent style’ algorithm to find \( \mu \). As with most nonconvex algorithms, our approach is susceptible to falling in suboptimal minima. Our key algorithmic insight is that our algorithm fails to descend the cost function exactly when our cost function necessitates the design of new packing/covering solvers for Positive Semidefinite Programs (SDP) over general Fantopes (the convex hull of the projection matrices). Positive SDP’s have seen remarkable success in areas spanning quantum computing, spectral graph theory, and approximation algorithms (See [9], [10], [11] and the references therein). Informally, a packing SDP computes the fractional number of ellipses that can be packed into a spectral norm ball which involves optimization over the spectrahedron. A natural question is whether the packing concept can be extended to balls equipped with general norms, say the sum of the top \( k \) eigenvalues (the Ky Fan norm), where for \( k = 1 \) we recover the oft studied spectral norm packing. We use results from Logo""er’s theory of operator monotonicity and operator algebras to design fast, and as far as we know the first solvers for packing/covering positive SDP’s under Ky Fan norms (see Theorem 5.13 of the full version).

**B. Related Work**

**Robust Statistics:** Robust statistics has a long history [3], [12], [4], [13]. This extensive body of work develops the theory of estimators with high breakdown points of influence functions and sensitivity curves, and of designing robust M-estimators. See [5], [6]. However, little was understood about the computational aspects of robustness which features prominently in high dimensional settings.

Recent work in theoretical computer science [14], [15] designed the first algorithms for estimating the mean and covariance of high dimensional gaussians tolerating a constant fraction of outliers in polynomial time \( \text{poly}(N, d, \frac{1}{\alpha}) \). Since then, a flurry of work has emerged studying robust regression [16], [17], sparse robust regression [18], [19], fast algorithms for robustly estimating mean/covariance [20], [21], [22], statistical query hardness of robustness [23], worst case hardness [24], robust graphical models [25], and applications of the sum of squares algorithm to robust statistics [26]. See survey [27] for an overview.

**List Decodable Learning:** Despite the remarkable progress in robust statistics for large \( \alpha \) contamination, progress on the list decoding problem has been slower. This is partially owed to the intrinsic computational hardness of the problem. Even for the natural question of list decoding the mean of a high dimensional gaussian, [8] exhibits a quasipolynomial time lower bound against Statistical Query algorithms for achieving the information theoretically optimal recovery of \( \Theta\left(\sqrt{\log\left(\frac{1}{\alpha}\right)}\right) \). This stands in contrast to
large $\alpha$ robust mean estimation where nearly linear time algorithms [20] achieve optimal recovery.

In light of this hardness, a natural question is to determine whether polynomial time algorithms can at least approach the optimal recovery for the mean of a gaussian. In a series of concurrent works [28] [8], develop the first algorithms approaching the $\Theta\left(\sqrt{\log(\frac{1}{\alpha})}\right)$ recovery guarantee. At a high level, both papers achieve recovery $O\left(\frac{d}{\alpha}\right)$ for different fixed constants $c > 1$ in time $\text{poly}\left(\frac{d}{\alpha}\right)^{O(k)}$ for $k$ a positive integer greater than 2. The [8] algorithm, known as the "multi-filter", is a spectral approach reasoning about high degree polynomials of the moments of data. Furthermore, the "low degree" multi-filter achieves a suboptimal $O\left(\sqrt{\log(\frac{d}{\alpha})}\right)$ recovery guarantee for list decoding the mean of subgaussian distributions, which is fast and may be of practical value. [28] develop a convex hierarchy (sum of squares) style approach, which achieve similar guarantees for more general distributional families satisfying a poincare inequality. In particular for list decoding the mean of bounded covariance distributions they achieve the optimal $O\left(\frac{1}{\alpha}\right)$ guarantee via the polynomial time solvability of convex concave optimization. Finally, [8], [28] and a concurrent work [29] develop tools for reasoning about the high degree moments of data to break the long-standing "single-linkage" barrier in clustering mixtures of spherical gaussians.

In other statistical settings a series of concurrent works [30], [31] demonstrate information theoretic impossibility for list decoding regression even under subgaussian design. Similar barriers arise in the context of list decodable subspace recovery [32], [33] where it is information theoretically impossible to list decode a dataset for which an $\alpha$ fraction is drawn from a subgaussian distribution in a subspace. Indeed, since list decoding is a superset of learning mixture models, these hardness considerations stem from barriers in learning mixtures of linear regressions and subspace clustering. On the other hand, the above works also construct polynomial time, $d^{\text{poly}(\frac{1}{\sqrt{\alpha}})}$, algorithms for regression and subspace recovery for Gaussian design and Gaussian subspaces respectively, which holds true for a larger class of "certifiably anticoncentrated" distributions.

In this backdrop of computational and statistical hardness, and given the practical value of robust statistics, it is a natural challenge to design list decoding algorithms that are both fast and statistically optimal. The current work is a step in this direction.

**SDP Solvers:** There has been much recent interest in designing fast algorithms for positive SDP solvers due to the ubiquity of their application in approximation algorithms. We do not attempt to survey the full breath of these results and their applications in this section. We refer the interested reader to [11], [10], [34], [9] for more context on these developments. We will restrict ourselves to the following class of SDPs relevant to our work:

$$\begin{align*}
\max & \sum_{i=1}^{n} w_i \\
\text{s.t.} & \sum_{i=1}^{n} w_i A_i \preceq I \\
& \left\| \sum_{i=1}^{n} w_i B_i \right\|_k \leq k
\end{align*}$$

(Gen-Pack)

where $A_i \in S^d_+$ and $B_i \in S^n_+$. While existing fast solvers [34], [10], [11] only apply to the above setting when $k = 1$, we generalize the approach of [34] to for all $k$ with running times scaling at most polynomial in $k$. In particular, we show for small values of $k$, Gen-Pack can be solved in nearly linear time for a broad range of settings including ours and inherits the parallel, width-independent properties of [34]. See Theorem 5.13 of the full version for the exact statement of the result. However, carrying out this generalization brings with it a host of technical challenges which are explained in more detail in Section II including a more refined analysis of the power method and a novel technique to bound errors incurred in a hard-thresholding operator due to approximate eigenvector computation.

**Semirandom Graph Inference:** The study of problems that are typically computationally hard in the worst case in semirandom graph models was initiated by [35] and perpetuated by [36]. A specific problem of interest to us studied by [36] for which nearly optimal algorithms were given by [37] is the semirandom independent set problem where the set of edges between a planted independent set and the remaining (adversarially chosen) graph come from a randomized model. In a similar vein [1] studies a planted partition where instead of an independent set the given graph is some other sparse random graph (albeit directed). Our results improve upon the statistical guarantees of [1] as well as give faster algorithms, however both [1] and our work fall short of capturing the results of [37] due to the directed model we work in. However, we believe the hurdle is a technical point rather than an inherent shortcoming of our approach.

**Sample Complexity:** The following lemma of [1] achieves linear sample complexity which suffices for our algorithm.

**Lemma 1.2** ([1, Proposition 1.1]). Suppose $\mathcal{I}(\mu)$ is a distribution on $\mathbb{R}^d$ with mean $\mu$ and covariance $\text{Cov}(I(\mu)) \preceq \sigma^2 I$ for a constant $\sigma > 0$. Then given $n \geq d$ samples from $\mathcal{I}(\mu)$, with probability $1 - \exp\left(\frac{-c}{n\sigma^2}\right)$ there exists a subset $I \in [n]$ of size $|I| \geq \frac{d}{2}$ such that $\left\| \frac{1}{|I|} \sum_{i \in I} (x_i - \mu)(x_i - \mu)^T \right\| \leq 24\sigma^2 I$.

Taking $N = O\left(\frac{d}{\alpha}\right)$, for the rest of the paper we will adjust $\sigma$ by a constant and assume the inlier set $I$ satisfies
\[ \frac{1}{\lambda_1} \sum_{i \in I} (x_i - \mu)(x_i - \mu)^T \leq \sigma^2 I. \]

**Notation:** We will frequently use \( S_n^+ \) to denote the set of positive semidefinite matrices with dimension \( n \). For \( A \in S_n^+ \), we will frequently write the ordered eigenvalue decomposition of \( A = \sum_{i=1}^n \lambda_i u_i u_i^T \) with \( \lambda_1 \geq \ldots \geq \lambda_n \) and for any matrix, \( M, \sigma_i(M) \) denotes its \( i^{th} \) singular value.

The Ky–Fan matrix \( k \)-norm, \( M \), is defined as the sum of the top-\( k \) singular values of \( M \); i.e. \( \|M\|_k := \sum_{i=1}^k \sigma_i(M) \). Notably, \( \|M\|_1 \) is the operator norm and \( \|M\|_\infty \) is the trace norm. However, we will stick with \( \|\cdot\|_k \) for operator norm and \( \|\cdot\|_\infty \) for trace norm. Continuing along these lines, we also define the \( \ell \)-Fantope, denoted by \( F_\ell \) and characterized as \( F_\ell = \{ M \in S_n^+ : \text{Tr} M = \ell \text{ and } \|M\|_1 \leq 1 \} \).

Finally, given \( \{b_i \geq 0\}_{i=1}^N \), we define the set \( \Phi_b(\gamma) = \{ w_i \geq 0 : \sum_{i=1}^N w_i = \gamma \text{ and } w_i \leq b_i \} \). For a set of vectors, \( V = [v_1, \ldots, v_k] \), we will use \( P^+_V \) to denote the projection onto the orthogonal subspace of the span of \( v_i \).

II. TECHNIQUES

First we present an inefficient algorithm for list decodable mean estimation. Although it is inefficient, it captures the core ideas and foreshadows the difficulties encountered by our efficient algorithm. At a high level, the inefficient algorithm greedily searches through the dataset for subsets of points with small covariance with the goal of finding the subset of inliers.

**Inefficient Algorithm:** Our inefficient algorithm is a list decoding analogy to the nonconvex weight minimization procedure first proposed in [14]. Let \( L \) be a list initialized to be the empty set. Let \( b \) be a vector initialized to be \( \left( \frac{2}{\alpha N}, \frac{2}{\alpha N}, \ldots, \frac{2}{\alpha N} \right) \in \mathbb{R}^N \). The algorithm iterates the following loop for \( \frac{\alpha}{2} \) iterations.

1) First, solve the optimization problem

\[
\hat{w} = \arg \min_{w \in \Phi_b} \left\| \sum_{i=1}^N w_i (x - \mu(w))(x - \mu(w))^T \right\|_k.
\]

Where \( \mu(w) = \sum_{i=1}^N w_i x_i \).

2) Second, append \( \hat{\mu} = \sum_{i=1}^N \hat{w}_i x_i \) to \( L \).

3) Third, update \( b \) such that \( b_i = \hat{b}_i - \hat{w}_i \).

We claim the algorithm outputs a list \( L \) of length \( \frac{2}{\alpha} \) and that there exists a \( \hat{\mu}^* \in L \) satisfying \( \|\hat{\mu}^* - \mu\|_k \leq O(\frac{\sqrt{N}}{\alpha}) \).

Next we outline the proof of correctness.

**Proof Outline:** We proceed by contradiction and assume \( \|\hat{\mu} - \mu\|_k \geq \frac{10\sigma}{\sqrt{\alpha}} \) for all \( \hat{\mu} \in L \). Consider the first iteration. The scaled indicator of the inliers \( \frac{1}{\sqrt{N}} [i \in I] \) is feasible for Eq. (1). Thus, we have \( \|\sum_{i=1}^N w_i (x_i - \mu(w))(x_i - \mu(w))^T \|_k \leq 4\sigma^2 \). It is a fact that given two subsets of the data that are both covariance bounded, if the means of the subsets are far apart then the subsets don’t overlap substantially. This fact extends beyond subsets and holds true even for the soft weights that we are considering here (see Fact A.3 of the full version). Applying this fact we conclude \( \sum_{i \in I} \hat{w} \leq \frac{2}{\alpha} \). By assumption, subsequent iterations of the algorithm continue to output \( \mu \) far away from the true mean so a substantial fraction of the inlier weight is preserved enabling the above argument to go through repeatedly. Formally, this would be argued inductively (see Corollary 4.4 of the full version).

Thus, at every iteration \( \sum_{i \in I} \hat{w} \leq \frac{2}{\alpha} \). Notice that any algorithm that removes more outlier weight than inlier weight at a ratio \( \sum_{i \in O} \hat{w}_i \geq \frac{2}{\alpha} \sum_{i \in I} \hat{w}_i \) will eventually remove all the outlier weight leaving more than \( \frac{1}{\alpha} \) of the inlier weight intact. Since the total inlier weight is initialized to be \( \sum_{i \in I} b_i = 2 \), we have at the second to last iteration a dataset comprised entirely of inliers which implies \( \|\hat{\mu} - \mu\|_k \leq \frac{10\sigma}{\sqrt{\alpha}} \), which is a contradiction.

**Sanitizing the Dataset:** Abstracting the guarantees of our inefficient algorithm, we say that an algorithm "sanitizes" a dataset if it outputs a tuple \((\mu, \hat{w})\) where

\[
\sum_{i=1}^N \hat{w}_i \geq \Omega(1)
\]

satisfying the following conditions. If \( \|\hat{\mu} - \mu\|_k \leq O(\frac{\sigma}{\sqrt{\alpha}}) \) then \( \sum_{i \in O} \hat{w}_i \geq \frac{2}{\alpha} \sum_{i \in I} \hat{w}_i \). Any algorithm that sanitizes the dataset iteratively, is guaranteed to succeed as a list decoding algorithm. This is made formal in Section 4 of the full version.

**Descent Style Formulation:** The optimization problem Eq. (1) is nonconvex and hard to solve directly. A novel approach to minimizing Eq. (1) is to replace \( \mu(w) \) with a parameter \( \nu \) and define a cost function \( f(\nu) \). First introduced in [20] in the context of robust mean estimation and later in robust covariance estimation [22] consider the function \( f(\nu) \) defined as follows:

\[
f(\nu) := \min_{w \in \Phi_b} \left\| \sum_{i=1}^N w_i (x - \nu)(x - \nu)^T \right\|_k
\]

where \( b_i = \frac{1}{\alpha N} \) for all \( i \in [N] \). This formulation has two appealing aspects. Firstly, the cost function can be computed efficiently via convex concave optimization. Indeed, the operator norm can be replaced by the maximization over its associated fantope \( F_1 \)

\[
f(\nu) := \min_{w \in \Phi_b} \max_{M \in F_1} \left\| M, \sum_{i=1}^N w_i (x_i - \nu)(x_i - \nu)^T \right\|
\]

Secondly, for \( \alpha > \frac{2}{3} \) (robust mean estimation), a crucial insight of [20] is that \( f(\nu) \approx \) approximates the squared distance from \( \nu \) to the mean \( \mu \). Then a good estimate of the mean is the minimizer of the cost.

\[
\hat{\mu} := \arg \min_{\nu \in \mathbb{R}^d} f(\nu) \approx \arg \min_{\nu \in \mathbb{R}^d} \|\nu - \mu\|^2
\]
In their setting the minimization in Eq. (2) can be performed by a descent style algorithm.

Substantial challenges arise when designing such a cost function for list decodable mean estimation. Chiefly, the inliers are unidentifiable from the dataset so there is no function of the data that approximates the distance to the true mean. Our solution is to design a function that either approximates the distance to the true mean, or when the approximation is poor, prove there exists a corresponding dual procedure that sanitizes the dataset. This win-win observation can be made algorithmic and is the subject of Section 4 of the full version.

A. Our Approach

Designing Cost: We make extensive use of the Fan-Neumann’s min max theorem we have

$\max_{\nu} \min_{M \in F} \{ \langle M, b \rangle : \nu \} = \max_{\nu} \min_{M \in F} \{ \langle M, b \rangle : \nu \} \geq \max_{\nu} \min_{M \in F} \{ \langle M, b \rangle : \nu \}$

This set of matrices, denoted $F$, is a tight relaxation for simultaneous rank and orthogonality constraints on the positive semidefinite cone. This also makes it amenable to semidefinite optimization. We define

$F = \{ M \in \mathbb{R}^{d \times d} : 0 \preceq M \preceq I \text{ and } \text{Tr}(M) = \ell \}$. 

Optimization over the Fan-Neumann’s min max theorem provides a variational characterization of the principal subspace of a symmetric matrix $B \in \mathbb{R}^{d \times d}$, Indeed the Ky Fan Theorem, states that the Ky Fan Norm defined to be the sum of the $\ell$ largest eigenvalues of a psd matrix is equal to

$$\|B\|_\ell := \sum_{i=1}^\ell \lambda_i(B) = \max_{Q^TQ=I} \langle B, QQ^T \rangle = \max_{M \in F} \{ \langle B, M \rangle : \nu \}.$$  

(3)

Here the first equality is an extremal property known as Ky Fan’s Maximum Principle, and the second equality follows because the rank $\ell$ projection matrices are extremal points of $F$. See [39]. We use this principle to generalize the min-max problem considered in the previous section. Let $\text{Cost}_{X,b,\ell}(\nu) : \mathbb{R}^d \to \mathbb{R}^+$ be defined

$$\text{Cost}_{X,b,\ell}(\nu) = \min_{w \in \Phi} \max_{M \in F} \{ \sum_{i=1}^N w_i (X_i - \nu) (X_i - \nu)^T, M \} = \min_{w \in \Phi} \left\| \sum_{i=1}^N w_i (X_i - \nu) (X_i - \nu)^T \right\|_\ell$$

(4)

We call the above min-max formulation the dual and the associated minimizer $w^*$ the dual minimizer or dual weights. By Von Neumann’s min max theorem we have

$$\text{Cost}_{X,b,\ell}(\nu) = \max_{M \in F} \min_{w \in \Phi} \{ \sum_{i=1}^N w_i (X_i - \nu) (X_i - \nu)^T, M \}$$

Where we refer to the maximizer $M^*$ as the primal maximizer. For the remainder of this section we will set $\ell = 1$ and $b = (\frac{1}{\alpha N}, ..., \frac{1}{\alpha N}) \in \mathbb{R}^N$ and drop the subscripts in $\text{Cost}(\cdot)$.

An Easier Problem: To aid in exposition, we illustrate our algorithmic approach on the simpler and well understood problem of finding the $k = \frac{1}{\alpha}$ means of data drawn from a mixture of $k$ bounded covariance distributions. That is $x_1, ..., x_N \sim \frac{1}{k} \sum_{i=1}^k D(\mu_i)$ for a distribution $D(\mu) \subseteq I$ with means $\{\mu_i\}_{i=1}^k$ and let $T_i$ denote the set of points in each cluster $i \in [k]$. Consider a vector $\nu$ that is further than $O(\sqrt{K})$ away from all the means $\{\mu_i\}_{i=1}^k$. By standard duality arguments, we see that $\text{Cost}(\nu)$ is a good approximation to the distance to the closest cluster center denoted $\mu^*$ comprised of points $T^*$. Furthermore, $\mu^* - \nu$ is almost completely contained in the top-$O(k)$ singular subspace of $M^*$, denoted $V$. We may now project all the data points onto the affine subspace $V$ offset to $\nu$ forming the set $X' := \{\Pi_V (x_i - \nu)\}_{i=1}^N$. The second observation is that a randomly chosen point $\tilde{x} \in T^*$ satisfies $\|\Pi_V (\tilde{x} - \mu^*)\| \leq O(\sqrt{K})$ with constant probability. Due to the fact that $\mu^* - \nu$ is almost completely contained in $V$, we get by picking a set of $p = O(k)$ random data points $R := \{x'_1, x'_2, ..., x'_{p}\} \in X'$, that there exists a point $\tilde{x}' \in R$ substantially closer to $\mu^*$ than $\nu$ with high probability $1 - \frac{1}{\text{poly}(d)}$. We can efficiently certify this progress by computing the value of $\text{Cost}(\tilde{x}')$. By iterating this procedure we converge to within $O(\sqrt{K})$ of the mean of a cluster center.

List Decoding Main Lemma: In analogy to clustering, one should hope that for any $\nu \in \mathbb{R}^d$ further than $O(\sqrt{\frac{1}{\alpha N}})$ from $\mu$, that $\text{Cost}(\nu) \approx \|\nu - \mu\|^2$. Although this is impossible, it turns out that when it is false, there exists a corresponding “dual procedure” for outputting a sanitizing tuple. More precisely, we claim that either $\frac{1}{\alpha} \|\nu - \mu\|^2 \leq \text{Cost}(\nu) \leq 1.1 \|\nu - \mu\|^2$, or a simple procedure outputs a set of weights $w$ identifying vastly more outliers than inliers i.e $\sum_{i \in \mathcal{I}} w_i \geq \frac{1}{2} \sum_{i \in \mathcal{E}} w_i$, or both.

The dual procedure is as follows. Let $\tilde{\Sigma} := \sum_{i=1}^m w_i (x_i - \nu)(x_i - \nu)^T$ be the weighted second moment matrix centered at $\nu$. Let $V$ be the top $O(\frac{1}{\alpha})$ eigenspace of $\tilde{\Sigma}$. We project the dataset onto the affine subspace $V$ with offset $\nu$. We then sort the points $\{\Pi_V (x_i - \nu)\}_{i=1}^N$ by Euclidean lengths. This sorting determines an ordering of the weights $w_1^*, ..., w_N^*$. We pass through the sorted list, and find the smallest $m \in [N]$ such that $\sum_{i=1}^m w_i^* \geq 0.5$. We set $w_i = w_i^*$ for $i = 1, ..., m$ and $w_i = 0$ for $i > m$. The following lemma guarantees

$$\sum_{i \in \mathcal{I}} w_i \geq \frac{1}{2} \sum_{i \in \mathcal{E}} w_i.$$  

Lemma II.1. (Nonalgorithmic Filtering with Exact Cost Evaluation) Let $\nu \in \mathbb{R}^d$ be any vector satisfying $\|\nu - \mu\| \geq O(\sqrt{\frac{1}{\alpha N}})$. Let $\text{Cost}_{X,b,\ell}(\nu)$ be defined as in Eq. (4) for $b = (\frac{1}{N}, ..., \frac{1}{N}) \in \mathbb{R}^N$ and $\ell = \frac{1}{\alpha}$. Let $w^* \in \Phi$ be the corresponding dual minimizer. Let $\tilde{w}$ be defined as follows

$$\tilde{w} := \arg \min_{p_i \in [0, w_i^*]} \sum_{i=1}^N \frac{p_i \|\Pi_V (x_i - \nu)\|}{\|p_i\|_{\ell}}$$

for $V$ the subspace defined above. Then either the cost is a constant factor approximation to the distance to the true
mean, $0.4\|\nu - \mu\|^2 \leq \text{Cost}_{X,b,i}(\nu) \leq 1.1\|\nu - \mu\|^2$, or $\hat{w}$ identifies a set of weights with vastly more outliers than inliers, $\sum_{i \in O} \hat{w}_i \geq \frac{3}{2} \sum_{i \in T} \hat{w}_i$ (or both).

In Lemma 4.5 of the full version we state the algorithmic version of the above lemma. There it is important to take into account technicalities involving the approximate evaluation of $\text{Cost}_{X,b,i}(\cdot)$, and provide a procedure for making progress when the cost is a constant approximation $\|\nu - \mu\|^2$. This will be done in a manner akin to the procedure for clustering described earlier. Nevertheless, Lemma II.1 captures the key guarantee that ensures our main algorithms in Section 4 succeed.

B. Generalized Packing/Covering Solvers and Improved Power Method Analysis

We start by considering the simpler problem of computing $\text{Cost}_{X,b,1}(\nu)$. The approach taken in [20] is to reduce the problem to a packing SDP via the introduction of an additional parameter $\lambda$; specifically, they solve the following packing SDP:

$$\max_{w_i \geq 0} \sum_{i=1}^{N} w_i \quad \text{subject to} \quad \sum_{i=1}^{N} w_i (X_i - \nu)(X_i - \nu)^\top \leq \lambda$$

for which there exist fast linear-time solvers [34], [10]. It can be shown that the value of the above program when viewed as a function of $\lambda$ is monotonic, continuous and attains the value 1 precisely when $\lambda = \text{Cost}_{X,b,1}(\nu)$. Therefore, by performing a binary search over $\lambda$, one obtains accurate estimates of $w^*$ and $\text{Cost}_{X,b,1}(\nu)$.

However, a similar approach for the problem of computing $\text{Cost}_{X,b,i}(\nu)$ results in the following SDP:

$$\max_{w_i \geq 0} \sum_{i=1}^{N} w_i \quad \text{subject to} \quad \sum_{i=1}^{N} w_i (X_i - \nu)(X_i - \nu)^\top \leq \lambda$$

which does not fall into the standard class of packing SDPs. We extend and generalize fast linear time solvers for packing/covering primal dual pairs they consider:

| Packing (Dual) | Covering (Primal) |
|---------------|-------------------|
| $\min_{M} \text{Tr } M$ | $\max_{M \geq 0} \sum_{i=1}^{N} w_i$ |
| Subject to: $\langle A_i, M \rangle \geq 1$ | Subject to: $\sum_{i=1}^{N} w_i A_i \leq I$ |

where $A_i \in \mathbb{S}_+^N$. The solver of [34] start by initializing a set of weights, $w_i$, feasible for Packing-SDP. Subsequently, in each iteration, $t$, they first compute the matrix

$$P_t = \exp(\sum_{i=1}^{N} w_i A_i) \Big/ \text{Tr} \exp(\sum_{i=1}^{N} w_i A_i).$$

The algorithm then proceeds to increment the weights of all $i$ such that $\langle P_t, A_i \rangle \leq (1 + \varepsilon)$ for a user defined accuracy parameter, $\varepsilon$, by a multiplicative factor. Intuitively, these indices correspond to “directions”, $A_i$, along which $\sum_{i=1}^{N} w_i A_i$ is small and therefore, their weights can be increased in the dual formulation. By incorporating a standard regret analysis from [40] for the matrices, $P_t$, they show that one either outputs a primal feasible, $M$, with $\text{Tr } M \leq 1$ or a dual feasible $w$ with $\sum_{i=1}^{N} w_i \geq (1 - \varepsilon)$.

The construction of our solver follows the same broad outline as in [34]. While the regret guarantees we employ are a generalization of those used in [34], they still follow straightforwardly from standard regret bounds for mirror descent based algorithms [41]. Instead, the main challenge of our solver is computational. The matrix $P(t)$ can be viewed as a maximizer to $f(X) = \langle X, F \rangle - \langle X, \log X \rangle$ where $F = \sum_{i=1}^{N} w_i A_i$ in $\mathcal{F}_1$. In our setting, we instead are required to compute the maximizer of $f$ in $(\mathcal{F}_t/\ell)$ which we show is given by the following: Let $H$ and $\tau^*$ be defined as:

$$H = \exp(F) = \sum_{i=1}^{m} \lambda_i u_i u_i^\top \text{ with } \lambda_1 \geq \lambda_2 \ldots \geq \lambda_m > 0$$

and

$$\tau^* = \max_{\tau \geq 0} \left\{ \frac{\tau^*}{\sum_{i=1}^{m} \min(\tau, \lambda_i)} = \frac{1}{\ell} \right\}.$$

Then, we have:

$$P_t = \arg \max_{tX \in \mathcal{F}_t} f(X)$$

$$= \frac{1}{\sum_{i=1}^{m} \min(\lambda_i, \tau^*)} \sum_{i=1}^{m} \min(\lambda_i, \tau^*) u_i u_i^\top.$$

While the matrix, $P_t$, can be efficiently estimated by Taylor series expansion of the exponential function (see [40]), we need to estimate $P_t$ which is given by a careful truncation operation on $\exp(F)$. Note that given access to the exact
top-$\ell$ eigenvectors and eigenvalues of $\exp(F)$, one can efficiently obtain a good estimate of $P_\ell$. However, the main technical challenge is establishing such good estimates given access only to approximate eigenvectors and eigenvalues of a truncated Taylor series approximation of $H$.

One of the main insights of our approach is that instead of analyzing the truncation operator directly, we instead view $P_\ell$ as being the maximizer of $g(X, F) = \langle F, X \rangle - \langle X, \log X \rangle$ with respect to $X$. We then subsequently show that maximizer of $g(X, \tilde{F})$ is close to $P_\ell$ for some $\tilde{F}$ close to $F$ which makes crucial use of the fact that $\log X$ is operator monotone. Our second main piece of insight is that if our approximate eigenvectors and eigenvalues, denoted by $(\hat{\lambda}_i, v_i)_{i=1}^\ell$, satisfy:

\[
(1 - \varepsilon) \sum_{i=1}^\ell \hat{\lambda}_i v_i v_i^\top + \mathcal{P}_V^\perp H \mathcal{P}_V^\perp \preceq H \\
\preceq (1 + \varepsilon) \sum_{i=1}^\ell \hat{\lambda}_i v_i v_i^\top + \mathcal{P}_V^\perp H \mathcal{P}_V^\perp,
\]

where $V$ is the subspace spanned by the $v_i$ and $\mathcal{P}_V^\perp$ is the projection onto the orthogonal subspace of $V$, then our approximate truncation operator can be viewed as the exact maximizer of $g(X, \tilde{F})$ for some $\tilde{F}$ close to $F$. From the previous discussion, this means that our truncation operator operating on the approximate eigenvectors $v_i$ is a good estimate of $P_\ell$. However, standard analysis of methods for the computation of eigenvalues and eigenvectors do not yield such strong guarantees [42], [43]. The final contribution of our work is a refined analysis of the power method that yields the required stronger guarantees which is formally stated in Theorem 6.1 of the full version.2

ACKNOWLEDGEMENTS

We would like to thank Sam Hopkins and Prasad Raghavendra for helpful conversations. We would also like to thank Bryan Chen for pointing out errors in an earlier version of this manuscript.

REFERENCES

[1] M. Charikar, J. Steinhardt, and G. Valiant, “Learning from untrusted data,” in Proceedings of the 49th Annual ACM SIGACT Symposium on Theory of Computing, 2017, pp. 47–60.

[2] Y. Cherapanamjeri, S. Mohanty, and M. Yau, “List decodable mean estimation in nearly linear time,” 2020.

[3] J. Tukey, “A survey of sampling from contaminated distributions,” 1960.

[4] P. J. Huber, “Robust estimation of a location parameter,” Ann. Math. Statist., vol. 35, no. 1, pp. 73–101, 03 1964.

[5] ——, Robust Statistics. Berlin, Heidelberg: Springer Berlin Heidelberg, 2011, pp. 1248–1251.

[6] F. R. Hampel, E. M. Ronchetti, P. J. Rousseuw, and W. A. Stahel, Robust statistics. The approach based on influence functions. Wiley New York, 1986.

[7] M.-F. Balcan, A. Blum, and S. Vempala, “A discriminative framework for clustering via similarity functions,” in Proceedings of the Fortieth Annual ACM Symposium on Theory of Computing, ser. STOC ’08. New York, NY, USA: Association for Computing Machinery, 2008, p. 671–680.

[8] I. Diakonikolas, D. M. Kane, and A. Stewart, “List-decodable robust mean estimation and learning mixtures of spherical gaussians,” in Proceedings of the 50th Annual ACM SIGACT Symposium on Theory of Computing, ser. STOC 2018. New York, NY, USA: Association for Computing Machinery, 2018, p. 1047–1060.

[9] S. Arora, E. Hazan, and S. Kale, “The multiplicative weights update method: a meta-algorithm and applications,” Theory of Computing, vol. 8, no. 1, pp. 121–164, 2012.

[10] Z. Allen Zhu, Y. T. Lee, and L. Orecchia, “Using optimization to obtain a width-independent, parallel, simpler, and faster positive SDP solver,” in Proceedings of the Twenty-Seventh Annual ACM-SIAM Symposium on Discrete Algorithms, SODA 2016, Arlington, VA, USA, January 10-12, 2016, R. Krauthgamer, Ed. SIAM, 2016, pp. 1824–1831.

[11] A. Jambulapati, Y. T. Lee, J. Li, S. Padmanabhan, and K. Tian, “Positive semidefinite programming: Mixed, parallel, and width-independent,” CoRR, vol. abs/2002.04830, 2020.

[12] J. W. Tukey, “Mathematics and the picturing of data,” 1975.

[13] F. R. Hampel, “A general qualitative definition of robustness,” The Annals of Mathematical Statistics, vol. 42, no. 6, pp. 1887–1896, 1971.

[14] I. Diakonikolas, G. Kamath, D. M. Kane, J. Li, A. Moitra, and A. Stewart, “Robust estimators in high dimensions without the computational intractability,” in 2016 IEEE 57th Annual Symposium on Foundations of Computer Science (FOCS), IEEE, 2016, pp. 655–664.

[15] K. A. Lai, A. B. Rao, and S. Vempala, “Agnostic estimation of mean and covariance,” in 2016 IEEE 57th Annual Symposium on Foundations of Computer Science (FOCS). IEEE, 2016, pp. 665–674.

[16] A. Klivans, P. K. Kothari, and R. Meka, “Efficient algorithms for outlier-robust regression,” arXiv preprint arXiv:1803.03241, 2018.

[17] I. Diakonikolas, W. Kong, and A. Stewart, “Efficient algorithms and lower bounds for robust linear regression,” in Proceedings of the Thirtieth Annual ACM-SIAM Symposium on Discrete Algorithms, ser. SODA ‘19. USA: Society for Industrial and Applied Mathematics, 2019, p. 2745–2754.
