
Communication-efficient Algorithms for Distributed Stochastic Principal Component Analysis

Dan Garber¹ Ohad Shamir² Nathan Srebro³

Abstract

We study the fundamental problem of *Principal Component Analysis* in a statistical distributed setting in which each machine out of m stores a sample of n points sampled i.i.d. from a single unknown distribution. We study algorithms for estimating the leading principal component of the population covariance matrix that are both communication-efficient and achieve estimation error of the order of the centralized ERM solution that uses all mn samples. On the negative side, we show that in contrast to results obtained for distributed estimation under convexity assumptions, for the PCA objective, simply averaging the local ERM solutions cannot guarantee error that is consistent with the centralized ERM. We show that this unfortunate phenomena can be remedied by performing a simple correction step which correlates between the individual solutions, and provides an estimator that is consistent with the centralized ERM for sufficiently-large n . We also introduce an iterative distributed algorithm that is applicable in any regime of n , which is based on distributed matrix-vector products. The algorithm gives significant acceleration in terms of communication rounds over previous distributed algorithms, in a wide regime of parameters.

1. Introduction

Principal Component Analysis (PCA) (Pearson, 1901; Hotelling, 1933; Jolliffe, 2002) is one of the most celebrated and popular techniques in data analysis and ma-

¹Technion - Israel Institute of Technology, Haifa, Israel ²Weizmann Institute of Science, Rehovot, Israel ³Toyota Technological Institute, Illinois, USA. Correspondence to: Dan Garber <dangar@technion.ac.il>, Ohad Shamir <ohad.Shamir@weizmann.ac.il>, Nathan Srebro <nati@ttic.edu>.

chine learning. For data that consists of N vectors in \mathbb{R}^d , $\mathbf{x}_1, \dots, \mathbf{x}_N$, with normalized covariance matrix $\hat{\mathbf{X}} = \frac{1}{N} \sum_{i=1}^N \mathbf{x}_i \mathbf{x}_i^\top$, The PCA method finds the k -dimensional subspace (which corresponds to the span of the top k principal components) such that the projection of the data onto the subspace has largest variance, i.e., it is the solution to the optimization problem:

$$\max_{\mathbf{W} \in \mathbb{R}^{d \times k}, \mathbf{W}^\top \mathbf{W} = \mathbf{I}} \|\hat{\mathbf{X}} \mathbf{W}\|_F^2. \quad (1)$$

PCA is often considered in a statistical setting in which the assumption is that the input vectors are not arbitrary but sampled i.i.d. from some fixed but unknown distribution with certain general characteristics \mathcal{D} . Then, it is often of interest to use the observed sample to estimate the top k principal components of the population covariance matrix, rather than that of the sample, which leads to the modified optimization problem:

$$\max_{\mathbf{W} \in \mathbb{R}^{d \times k}, \mathbf{W}^\top \mathbf{W} = \mathbf{I}} \|\mathbb{E}_{\mathbf{x} \sim \mathcal{D}} [\mathbf{x} \mathbf{x}^\top] \mathbf{W}\|_F^2. \quad (2)$$

Of course the empirical estimation problem (1) and the population estimation problem (2) are well connected, and it is well-known that under mild assumptions on the distribution \mathcal{D} and given a sufficiently large sample, we can guarantee small estimation error in (2) by solving optimization problem (1).

In this work we consider the problem of estimating the first principal component (i.e., $k = 1$) in a statistical and distributed setting. We assume the availability of m machines, each of which stores a sample of n vectors sampled i.i.d from a fixed distribution \mathcal{D} over \mathbb{R}^d , and we are interested in algorithms that can be applied efficiently to solve Problem (2) for $k = 1$, with estimation error that approaches that of a *centralized* algorithm, which has access to all mn samples and does not pay for communication between machines. Indeed, when considering the efficiency of algorithms, we will mainly focus on the amount of communication between machines they require, since this is often the most expensive resource in distributed computing. We note that the i.i.d. assumption is standard in many applications of PCA, and can be leveraged to get more efficient algorithms than when the data partition is arbitrary. Also, we will make a standard assumption that the population covariance matrix has a non-zero additive gap between the

first and second eigenvalues, which makes the problem of estimating the leading principal component meaningful.

A main challenge that often arises in many computational settings of principal components is that it leads to inherently non-convex optimization problems. While many times these problems turn out to admit efficient algorithms, the rich toolbox of optimization and statistical estimation procedures developed for *convex* problems often cannot be directly applied to problems such as (1) and (2). Instead, one often needs to consider a specialized and more involved analysis, to get analogous convergence results for the PCA problem. This for instance was the case in a recent wave of results that applied concepts such as stochastic gradient updates (Balsubramani et al., 2013; Shamir, 2016a; Jain et al., 2016b; Allen Zhu & Li, 2016b) and variance reduction (Shamir, 2015; 2016c; Garber & Hazan, 2015; Garber et al., 2016; Allen Zhu & Li, 2016a) to the PCA problem. This is also the case in our distributed setting. For instance, (Zhang et al., 2013) proposed communication-efficient algorithms for a distributed statistical estimation settings, similar to ours, but under convexity assumptions. The authors show that under their assumptions, in a wide regime of parameters (namely when the per-machine sample size n is large enough), then a simple averaging of the *empirical risk minimizers* (ERM), computed locally on each machine, leads to estimation error of the population parameters of the order the centralized ERM solution. While averaging makes perfect sense in a convex setting, it is clear that it can completely fail in a non-convex setting. Indeed, we show that already for the PCA problem with $k = 1$, simply averaging the local ERM solutions (and normalizing to obtain a unit vector as required), cannot improve significantly over the estimation error of any single machine. We then show that a simple fix to the above scheme, namely correlating the directions of individual ERM solutions, remedies this phenomena and results in estimation error similar to that of the centralized ERM solution. Much like the results of (Zhang et al., 2013), this result only holds in the regime when the per-machine sample size n is sufficiently large. As discussed, due to the inherent non-convexity of the PCA objective, this approach requires a novel analysis tailored to the PCA problem. In this context, we view this work as an initiation of a research effort to understand how to efficiently aggregate statistical estimators in a distributed non-convex setting.

A second line of results for distributed estimation under convexity assumptions consider iterative algorithms that perform multiple communication rounds and are based on distributed gradient computations (some examples include (Shamir et al., 2014; Zhang & Lin, 2015; Lee et al., 2015; Shamir, 2016b; Jaggi et al., 2014; Reddi et al., 2016)). The benefit of these methods is that (a) they provide meaningful estimation error guarantees in a much wider regime of pa-

rameters than the “one-shot” aggregation methods (namely in terms of the number of samples per machine), and (b), due to their iterative nature, they allow to approximate the centralized ERM solution arbitrary well. Unfortunately, these methods, all of which rely heavily on convexity assumption, cannot be directly applied to the PCA problem. Towards designing efficient distributed iterative methods for our PCA setting, we consider the application of the recently proposed method of *Shift-and-Invert power iterations* (S&I) for PCA (Garber & Hazan, 2015; Garber et al., 2016). The S&I method reduces the problem of computing the leading eigenvector of a real positive semidefinite matrix to that of approximately solving a small number (i.e. poly-logarithmic in the problem parameters) of systems of linear equations. These in turn, could be efficiently solved by arbitrary distributed convex solvers. We show that coupling the S&I method with the stochastic pre-conditioning technique for linear systems proposed in (Zhang & Lin, 2015) and well known fast gradient methods such as the conjugate gradient method, gives state-of-the-art guarantees in terms of communication costs, and provides a significant improvement over distributed variants of classical fast eigenvector algorithms such as power iterations and the faster Lanczos algorithm. Much like its convex counterparts, which only rely on distributed gradient computations and simple vector aggregations, our iterative method only relies on distributed matrix-vector products, i.e., it requires each machine to only send products of its local empirical covariance matrix with some input vector.

Beyond the results described so far, (Liang et al., 2014; Boutsidis et al., 2016) studied distributed algorithms for PCA in a *deterministic* setting in which the partition of the data across machines is arbitrary and communication is measured in terms of number of transmitted bits. The approximation guarantees provided in these works are in terms of the projection of the data onto the leading principal components (instead of alignment between the estimate and the optimal solution, studied in this paper). Applying these results to our setting will give a number of communication rounds that scales like $\text{poly}(\epsilon^{-1}\delta^{-1})$, where ϵ is the desired error and δ is the population eigengap. In our setting, ϵ will scale with the inverse of the size of the sample, i.e., $\epsilon \approx (mn)^{-1}$, which for these algorithms will result in amount of communication that is polynomial in the size of the data. In contrast, we will be interested in algorithms whose communication costs does not scale with n at all. In this context we note that, by focusing on algorithms that either perform simple aggregation of local ERM solutions, or perform only distributed matrix-vector products with the empirical covariance matrix, we can circumvent the need to measure communication explicitly in terms of the number of bits transmitted, which often burdens the analysis of natural algorithms, such as those proposed here.

2. Preliminaries

2.1. Notation and problem setting

We write vectors in \mathbb{R}^d in boldface lower-case letters (e.g., \mathbf{v}), matrices in boldface upper-case letters (e.g., \mathbf{X}), and scalars are written as lightface letters (e.g., c). We let $\|\cdot\|$ denote the standard Euclidean norm for vectors and the spectral norm for matrices.

We consider the following statistical distributed setting. Let \mathcal{D} be a distribution over vectors in \mathbb{R}^d with squared ℓ_2 norm at most b , for some $b > 0$. We consider a setting in which m machines, numbered $1 \dots m$, are each given a dataset of n samples drawn i.i.d. from \mathcal{D} . We let \mathbf{v}_1 denote a leading eigenvector of the population covariance matrix $\mathbf{X} = \mathbb{E}_{\mathbf{x} \sim \mathcal{D}}[\mathbf{x}\mathbf{x}^\top]$. Our goal is to efficiently (mainly in terms of communication) find an estimate \mathbf{w} for \mathbf{v}_1 , i.e., a unit vector that maximizes the product $(\mathbf{v}_1^\top \mathbf{w})^2$ with high probability. Towards this end, we assume that the population covariance matrix \mathbf{X} has a non-zero eigengap δ , i.e., $\delta := \lambda_1(\mathbf{X}) - \lambda_2(\mathbf{X}) > 0$, where $\lambda_i(\cdot)$ denotes the i th largest eigenvalue of a symmetric real matrix. Note that $\delta > 0$ is necessary for \mathbf{v}_1 to be uniquely defined (up to sign).

In addition, we let $\hat{\mathbf{X}}_i$ denote the empirical covariance matrix of the sample stored on machine i for every $i \in [m]$, i.e., $\hat{\mathbf{X}}_i = \frac{1}{n} \sum_{j=1}^n \mathbf{x}_j^{(i)} \mathbf{x}_j^{(i)\top}$, where $\mathbf{x}_1^{(i)} \dots \mathbf{x}_n^{(i)}$ are the samples stored on machine i . We let $\hat{\mathbf{X}}$ denote the empirical covariance matrix of the union of points across all machines i.e., $\hat{\mathbf{X}} = \frac{1}{m} \sum_{i=1}^m \hat{\mathbf{X}}_i$.

Our model of communication assumes that the m machines work in rounds during which a central machine (w.l.o.g. machine 1) can send a single vector in \mathbb{R}^d to all other machines, or every machine can send either the leading eigenvector of its local empirical covariance matrix, or the product of a single input vector with its local covariance, to machine 1. We will measure communication complexity in terms of number of such rounds required to achieve a certain estimation error.

2.1.1. THE CENTRALIZED SOLUTION

Our primary benchmark for measuring performance will be the *centralized empirical risk minimizer* which is the leading eigenvector of the aggregated empirical covariance matrix $\hat{\mathbf{X}}$.

The following standard result bounds the error of the centralized ERM.

Lemma 1 (Risk of centralized ERM). *Fix $p \in (0, 1)$. Suppose that $\delta > 0$ and let $\hat{\mathbf{v}}_1$ denote the leading eigenvector of $\hat{\mathbf{X}}$, i.e., $\hat{\mathbf{v}}_1 \in \arg \max_{\mathbf{v}: \|\mathbf{v}\|=1} \mathbf{v}^\top \hat{\mathbf{X}} \mathbf{v}$. Then it holds w.p. at least $1 - p$ that*

$$1 - (\mathbf{v}_1^\top \hat{\mathbf{v}}_1)^2 \leq \epsilon_{ERM}(p) := \frac{32b^2 \ln(d/p)}{mn\delta^2}. \quad (3)$$

Lemma 1 is a direct consequence of the following standard concentration argument for random matrices, and the Davis-Kahan $\sin(\theta)$ theorem (whose proof is given in the appendix for completeness):

Theorem 1 (Matrix Hoeffding, see (Tropp, 2012)). *Let \mathcal{D} be a distribution over vectors with squared ℓ_2 norm at most b , and let $\mathbf{X} = \mathbb{E}_{\mathbf{x} \sim \mathcal{D}}[\mathbf{x}\mathbf{x}^\top]$. Let $\hat{\mathbf{X}} = \frac{1}{n} \sum_{i=1}^n \mathbf{x}_i \mathbf{x}_i^\top$, where $\mathbf{x}_1, \dots, \mathbf{x}_n$ are sampled i.i.d. from \mathcal{D} . Then, it holds that $\forall \epsilon > 0$: $\Pr(\|\hat{\mathbf{X}} - \mathbf{X}\| \geq \epsilon) \leq d \cdot \exp\left(-\frac{\epsilon^2 n}{16b^2}\right)$.*

Theorem 2 (Davis-Kahan $\sin(\theta)$ theorem). *Let \mathbf{X}, \mathbf{Y} be symmetric real $d \times d$ matrices with leading eigenvectors $\mathbf{v}_\mathbf{X}$ and $\mathbf{v}_\mathbf{Y}$ respectively. Also, suppose that $\delta(\mathbf{X}) := \lambda_1(\mathbf{X}) - \lambda_2(\mathbf{X}) > 0$. Then it holds that $1 - (\mathbf{v}_\mathbf{X}^\top \mathbf{v}_\mathbf{Y})^2 \leq 2 \frac{\|\mathbf{X} - \mathbf{Y}\|^2}{\delta(\mathbf{X})^2}$.*

2.2. Informal statement of main results and previous algorithms

We now informally describe our main results, followed by a detailed description of previous approaches that are directly applicable to our setting. The algorithmic results (both new and old) are summarized in Table 1.

2.2.1. MAIN RESULTS

Failure of simple averaging of local ERM solutions We show that a natural approach of simply averaging the individual leading eigenvectors of the empirical covariance matrices $\hat{\mathbf{X}}_i$ (and normalizing the obtain a unit vector) cannot significantly improve (beyond logarithmic factors) over the performance of any of the individual eigenvectors. More concretely, if we let $\hat{\mathbf{v}}_1^{(i)}$ denote the leading eigenvector of $\hat{\mathbf{X}}_i$ for any $i \in [m]$, and we denote their average by $\bar{\mathbf{v}}_1 = \frac{1}{m} \sum_{i=1}^m \hat{\mathbf{v}}_1^{(i)}$, then there exists a distribution \mathcal{D} over vectors with magnitude $O(1)$ and covariance eigengap $\delta = 1$, such that

$$\forall m, n: \quad \mathbb{E}_{\mathcal{D}} \left[1 - \left(\frac{\bar{\mathbf{v}}_1^\top \mathbf{v}_1}{\|\bar{\mathbf{v}}_1\|} \right)^2 \right] = \Omega\left(\frac{1}{n}\right),$$

See Theorem 3 in Section 3 for the complete and formal argument.

A successful single communication round algorithm via correlation of individual ERM solutions We show that if prior to averaging the local ERM solutions, as suggested above, we correlate their directions by aligning them according to any single machine (say machine number 1), i.e., we let $\bar{\mathbf{v}}_1 = \frac{1}{m} \sum_{i=1}^m \text{sign}(\hat{\mathbf{v}}_1^{(i)\top} \hat{\mathbf{v}}_1^{(1)}) \hat{\mathbf{v}}_1^{(i)}$, then this guarantees that for any $p \in (0, 1)$, w.p. at least $1 - p$,

$$1 - \left(\frac{\bar{\mathbf{v}}_1^\top \mathbf{v}_1}{\|\bar{\mathbf{v}}_1\|} \right)^2 = O\left(\frac{b^2 \ln\left(\frac{dm}{p}\right)}{\delta^2 mn} + \frac{b^4 \ln^2\left(\frac{dm}{p}\right)}{\delta^4 n^2} \right). \quad (4)$$

Method	$1 - (\mathbf{w}^\top \mathbf{v}_1)^2$ w.p. $3/4$	# communication rounds
Centralized ERM	$\epsilon_{\text{ERM}} = \Theta\left(\frac{b^2 \ln d}{\delta^2 mn}\right)$	-
Distributed Power Method	$\epsilon_{\text{ERM}} \cdot (1 + o(1))$	$\tilde{O}(\lambda_1/\delta)$
Distributed Lanczos	$\epsilon_{\text{ERM}} \cdot (1 + o(1))$	$\tilde{O}(\sqrt{\lambda_1/\delta})$
“Hot-potato” SGD	$O(\epsilon_{\text{ERM}})$	m
Average of ERMs with sign-fixing (Theorem 4)	$O(\epsilon_{\text{ERM}}) + O\left(\frac{b^4 \ln^2 d}{\delta^4 n^2}\right)$	1
Distributed Shift&Invert + preconditioned linear systems (Theorem 6)	$\epsilon_{\text{ERM}} \cdot (1 + o(1))$	$\tilde{O}(\min\{(b/\delta)^{1/2} n^{-1/4}, m^{1/4}\})$

Table 1. Comparison of estimation error and number of communication rounds. For simplicity we fix the failure probability to $p = 1/4$ and assume mn is in the regime in which Lemma 1 is meaningful, i.e., $mn = \Omega(b^2 \delta^{-2} \ln d)$. The $\tilde{O}(\cdot)$ suppresses logarithmic factors in $b, d, 1/p, 1/\epsilon_{\text{ERM}}$. For the result of Theorem 4 we assume the regime $m = O(d)$. The sub-constant $o(1)$ factors could be made, in principle, arbitrary small in all relevant results by trading approximation with communication.

See Theorem 4 in Section 3 for the complete and formal result.

In particular, in the likely scenario when $m = O(d/p)$ we have that w.p. at least $1 - p$, $1 - (\tilde{\mathbf{v}}_1^\top \mathbf{v}_1 / \|\tilde{\mathbf{v}}_1\|)^2 = \epsilon_{\text{ERM}}(p) \cdot O(1 + m^2 \cdot \epsilon_{\text{ERM}}(p))$, where $\epsilon_{\text{ERM}}(p)$ is defined in Eq. (3). Another related interpretation of the results is that the bound in Eq. (4) is comparable with ϵ_{ERM} (up to poly-log factors) when $n = \Omega(\delta^{-2} b^2 m \ln(dm/p))$.

We also show a matching lower bound that the bound in Eq. (4) is tight (up to poly-log factors) for this aggregation method.

A multi communication round algorithm We present a distributed algorithm based on the *Shift-and-Invert* framework for leading eigenvector computation (Garber & Hazan, 2015; Garber et al., 2016) which is applied to explicitly solving the centralized ERM problem. We show that for any $p \in (0, 1)$, when $mn = \Omega(b^2 \ln(d/p)/\delta^2)$ (i.e., when Lemma 3 is meaningful), the algorithm produces a solution \mathbf{w} such that w.p. at least $1 - p$,

$$1 - (\mathbf{v}_1^\top \mathbf{w})^2 \leq \epsilon_{\text{ERM}}(p) \cdot (1 + o(1)), \quad (5)$$

where $\epsilon_{\text{ERM}}(p)$ is defined in Eq. (3). The algorithm performs overall $\tilde{O}(\sqrt{b} \delta^{-1/2} n^{-1/4})$ distributed matrix-vector products with the centralized empirical covariance matrix $\tilde{\mathbf{X}}^{-1}$. The $\tilde{O}(\cdot)$ notation hides poly-logarithmic factors in $1/p, 1/\delta, d, 1/\epsilon_{\text{ERM}}(p)$. See Theorem 6 in Section 4 for the complete and formal result.

We note that in particular, under our assumption that $mn = \tilde{\Omega}(b^2/\delta^2)$, it holds that the number of distributed matrix-vector products is upper bounded by $\tilde{O}(m^{1/4})$. Moreover, in the regime $n = \Omega(b^2 \delta^{-2})$, we can see that the number of distributed matrix-vector products depends only poly-logarithmically on the problem parameters.

In general, the sub-constant $o(1)$ factor in (5) could be made arbitrarily small by trading the approximation error

¹i.e., on each round, each machine i sends the product of an input vector in \mathbb{R}^d with its local covariance matrix $\tilde{\mathbf{X}}_i$.

with the number of distributed matrix-vector products.

2.2.2. PREVIOUS ALGORITHMS

Distributed versions of classical iterative algorithms: Classical fast iterative algorithms for computing the leading eigenvector of a positive semidefinite matrix, such as the well-known Power Method and the Lanczos Algorithm, require iterative multiplications of the input matrix ($\tilde{\mathbf{X}}$ in our case) with the current estimate. It is thus straightforward to implement these algorithms in our distributed setting, by multiplying the same vector with the covariance matrices at each machine, and averaging the result. Thus, by well-known convergence guarantees of these two methods, we will have that for a fixed $\epsilon > 0$, these methods produce a unit vector \mathbf{w} such that, for any $p \in (0, 1)$, $1 - (\mathbf{w}^\top \hat{\mathbf{v}}_1)^2 \leq \epsilon$ w.p. at least $1 - p$, after $O(\hat{\lambda}_1 \hat{\delta}^{-1} \ln(d/p\epsilon))$ rounds for the Power Method and $O(\sqrt{\hat{\lambda}_1 \hat{\delta}^{-1}} \ln(d/p\epsilon))$ for the Lanczos Algorithm, where $\hat{\lambda}_1, \hat{\delta}$ denote the leading eigenvalue and eigengap of $\tilde{\mathbf{X}}$, respectively. Moreover, in the regime of mn in which Lemma 1 is meaningful, we can replace $\hat{\lambda}_1, \hat{\delta}$ with λ_1, δ in the above bounds, and the result will still hold with high probability.

Simple calculations show that in the regime of mn in which Lemma 1 is meaningful, it holds that our Shift-and-Invert-based algorithm outperforms distributed Lanczos (in terms of worst-case guarantees) whenever $n = \tilde{\Omega}(b^2/\lambda_1^2)$.

“Hot potato” SGD: Another straightforward approach is to apply a sequential algorithm for direct risk minimization that can process the data-points one by one, such as stochastic gradient descent (SGD), by passing its state from one machine to the next, after completing a full pass over the machine’s data. Clearly, this process of making a full pass over the data of a certain machine before sending the final estimate to the next one, requires overall m communication rounds in order to make a full pass over all mn points. SGD for PCA was studied in several results in recent years (Balsubramani et al., 2013; Shamir, 2016a;c;

Jain et al., 2016a; Allen Zhu & Li, 2016b). For instance applying the result of (Jain et al., 2016a) in this way will result in a final estimate \mathbf{w} satisfying

$$1 - (\mathbf{w}^\top \mathbf{v}_1)^2 = O\left(\frac{b^2 \ln d}{\delta^2 mn}\right) \quad \text{w.p. at least } 3/4. \quad (6)$$

We note that in the regime in which the bound in (6) is meaningful it holds that the number of communication rounds of our Shift-and-Invert-based algorithm is upper-bounded by $\tilde{O}(m^{1/4})$ which for sufficiently large m dominates the communication complexity of SGD.

3. Single Communication Round Algorithms via ERM on Each Machine

In this section we consider distributed algorithms that require only a single round of communication. Naturally for this regime, all algorithms will be based on aggregating the ERM solutions of the individual machines, i.e., each machine i only sends the leading eigenvector of its empirical covariance matrix $\hat{\mathbf{X}}_i$ to a centralized machine (without loss of generality, machine 1) which it then combines them to a single unit vector in some manner.

3.1. Simple averaging of eigenvectors fail

Perhaps the simplest method to aggregate the individual eigenvectors of each machine is to average them, and then normalize to obtain a unit vector. For instance, in the distributed statistical setting considered in (Zhang et al., 2013), in which the objective is *strongly convex*, it was shown that simply averaging the individual ERM solutions leads, in a meaningful regime of parameters, to estimation error of the order of the centralized ERM solution. However, here we show that for PCA, in which the objective is certainly not convex, this approach fails practically in any regime, in the sense that the error of the returned aggregated solution can be no better than that returned by any single machine.

Theorem 3. *There exists a distribution over vectors in \mathbb{R}^2 with ℓ_2 norm bounded by a universal constant for which the eigengap in the covariance matrix is 1 (i.e., $\delta = 1$), such that if each machine i returns an estimate $\hat{\mathbf{v}}_1^{(i)}$ which is an unbiased leading eigenvector of $\hat{\mathbf{X}}_i$ (i.e., both outcomes $-\hat{\mathbf{v}}_1^{(i)}$, $+\hat{\mathbf{v}}_1^{(i)}$ are equally likely), then the aggregated vector $\bar{\mathbf{v}}_1 = \frac{1}{m} \sum_{i=1}^m \hat{\mathbf{v}}_1^{(i)}$ satisfies*

$$\forall m, n : \quad \mathbb{E} \left[1 - \left\langle \frac{\bar{\mathbf{v}}_1}{\|\bar{\mathbf{v}}_1\|}, \mathbf{v}_1 \right\rangle^2 \right] = \Omega(1/n).$$

The proof is given in the appendix.

3.2. Averaging with Sign Fixing

As evident from the statement of Theorem 3, an important assumption is that each machine produces an unbiased estimate, in the sense that the sign of the outcome is uniform and independent of the other machines. This hints that correlating the signs of the different estimates can circumvent the lower bound result in Theorem 3. It turns out that this is indeed the case, as captured by the following theorem:

Theorem 4. *Let $\tilde{\mathbf{w}}_i$ be the leading eigenvector of $\hat{\mathbf{X}}_i$ for any $i \in [m]$, and consider the unit vector*

$$\mathbf{w} = \frac{\sum_{i=1}^m \text{sign}(\tilde{\mathbf{w}}_i^\top \tilde{\mathbf{w}}_1) \tilde{\mathbf{w}}_i}{\left\| \sum_{i=1}^m \text{sign}(\tilde{\mathbf{w}}_i^\top \tilde{\mathbf{w}}_1) \tilde{\mathbf{w}}_i \right\|}. \quad (7)$$

Then, for any $p \in (0, 1)$, it holds w.p. at least $1 - p$ that

$$1 - (\mathbf{v}_1^\top \mathbf{w})^2 = O\left(\frac{b^2 \log\left(\frac{dm}{p}\right)}{\delta^2 mn} + \frac{b^4 \log^2\left(\frac{dm}{p}\right)}{\delta^4 n^2}\right).$$

For ease of presentation, throughout the rest of this section we denote the correlated vector $\hat{\mathbf{w}}_i = \text{sign}(\tilde{\mathbf{w}}_i^\top \tilde{\mathbf{w}}_1) \tilde{\mathbf{w}}_i$ for any $i \in [m]$.

The main step towards proving Theorem 4 is to consider each $\hat{\mathbf{w}}_i$ as an approximately unbiased perturbation of the true leading eigenvector \mathbf{v}_1 and to upper bound the magnitude of this perturbation. This is carried out in the following much more general and self-contained lemma, which might be of independent interest. The proof is given in the appendix.

Lemma 2. *Let \mathbf{A} be a positive semidefinite matrix with some fixed leading eigenvector \mathbf{v}_1 , a leading eigenvalue λ_1 and an eigengap $\delta := \lambda_1(\mathbf{A}) - \lambda_2(\mathbf{A}) > 0$. Let $\hat{\mathbf{A}}$ be some positive semidefinite matrix such that $\|\hat{\mathbf{A}} - \mathbf{A}\| \leq \delta/4$. Then there is a unique leading eigenvector $\hat{\mathbf{v}}_1$ of $\hat{\mathbf{A}}$ such that $\langle \hat{\mathbf{v}}_1, \mathbf{v}_1 \rangle \geq 0$, and*

$$\left\| \hat{\mathbf{v}}_1 - \mathbf{v}_1 - (\lambda_1 \mathbf{I} - \mathbf{A})^\dagger (\hat{\mathbf{A}} - \mathbf{A}) \mathbf{v}_1 \right\| \leq \frac{c \|\hat{\mathbf{A}} - \mathbf{A}\|^2}{\delta^2},$$

where \dagger denotes the pseudo-inverse, and c is a positive numerical constant.

Lemma 2 is central to the proof of the following Lemma, of which the proof of Theorem 4 is an easy consequence. We defer the proof of both the Lemma and that of Theorem 4 to the appendix.

Lemma 3. *The following two conditions hold with probability at least $1 - p - d \exp(-\delta^2 n / cb^2)$, for some numerical constants $c, c' > 0$:*

- *The leading eigenvalue of every $\hat{\mathbf{X}}_i$ is simple, i.e., $\lambda_1(\hat{\mathbf{X}}_i) - \lambda_2(\hat{\mathbf{X}}_i) > 0$.*
- *Fixing \mathbf{v}_1 , there exist unique leading eigenvectors $\hat{\mathbf{v}}_1^i, \dots, \hat{\mathbf{v}}_m^i$ of $\hat{\mathbf{X}}_1, \dots, \hat{\mathbf{X}}_m$, such that $\max_i \|\hat{\mathbf{v}}_1^i - \mathbf{v}_1\| \leq \frac{1}{4}$, and $\left\| \frac{1}{m} \sum_{i=1}^m \hat{\mathbf{v}}_1^i - \mathbf{v}_1 \right\| \leq c' \left(\frac{b^2 \log(2dm/p)}{\delta^2 n} + \sqrt{\frac{b^2 \log(2dm/p)}{\delta^2 mn}} \right)$.*

3.3. Lower Bound for Sign Fixing

We now show that the result of Theorem 4 is tight up to poly-logarithmic factors and cannot be improved in general:

Theorem 5. *For any $\delta \in (0, 1)$ and $d > 1$, there exist a distribution over vectors in \mathbb{R}^d (of norm at most a universal constant) with eigengap δ in the covariance matrix, such that for any number of machines m and for per-machine sample size any n sufficiently larger than $1/\delta^2$, the aggregated vector $\bar{\mathbf{v}}_1 = \frac{1}{m} \sum_{i=1}^m \hat{\mathbf{v}}_1^{(i)}$ (even after sign fixing with the population eigenvector \mathbf{v}_1) satisfies*

$$\mathbb{E} \left[1 - \left\langle \frac{\bar{\mathbf{v}}_1}{\|\bar{\mathbf{v}}_1\|}, \mathbf{e}_1 \right\rangle^2 \right] = \Omega \left(\frac{1}{\delta^2 m n} + \frac{1}{\delta^4 n^2} \right)$$

The proof is given in the appendix.

4. A Multi-round Algorithm based on Shift-and-Invert Iterations

In this section we move on to consider distributed algorithms that perform multiple communication rounds. The main motivation, beyond improving some poly-logarithmic factors in the estimation error, is to obtain a result that does not require the per-machine sample size n to grow with the number of machines m , as in the result of Theorem 4.

Towards this end we consider the use of the Shift-and-Invert meta-algorithm, originally described in (Garber & Hazan, 2015; Garber et al., 2016), to explicitly solve the centralized ERM objective, i.e., find a unit vector that is an approximate solution to $\max_{\mathbf{v}: \|\mathbf{v}\|=1} \mathbf{v}^\top \hat{\mathbf{X}} \mathbf{v}$.

Throughout this section we let $\hat{\lambda}_1, \hat{\delta}$ denote the leading eigenvalue and eigengap of $\hat{\mathbf{X}}$, respectively. Also, we assume without loss of generality that $b = 1$ (i.e., all data points lie in the unit Euclidean ball).

Since our approach is to approximate the population risk by approximating the empirical risk, we state the following simple lemma for completeness (a proof is given in the appendix).

Lemma 4 (Risk of approximated-ERM for PCA). *Let \mathbf{w} be a unit vector such that $(\mathbf{w}^\top \hat{\mathbf{v}}_1)^2 \geq 1 - \epsilon$, for some fixed $\epsilon > 0$, where $\hat{\mathbf{v}}_1$ is the leading eigenvector of $\hat{\mathbf{X}}$. Then it holds that $1 - (\mathbf{w}^\top \mathbf{v}_1)^2 \leq 1 - (\mathbf{w}^\top \hat{\mathbf{v}}_1)^2 + \sqrt{2\epsilon}$.*

4.1. The Shift-and-Invert meta-algorithm

The Shift-and-Invert algorithm (Garber & Hazan, 2015; Garber et al., 2016) efficiently reduces the problem of computing the leading eigenvector of a positive semidefinite matrix $\hat{\mathbf{X}}$ to that of approximately-solving a poly-logarithmic number of linear systems, i.e., finding approximate minimizers of convex quadratic optimization problems of the form

$$\min_{\mathbf{z} \in \mathbb{R}^d} \{F_{\lambda, \mathbf{w}}(\mathbf{z}) := \frac{1}{2} \mathbf{z}^\top (\lambda \mathbf{I} - \hat{\mathbf{X}}) \mathbf{z} - \mathbf{z}^\top \mathbf{w}\}, \quad (8)$$

where $\lambda > \lambda_1(\hat{\mathbf{X}})$ is a shifting parameter. The algorithm is essentially based on applying *power iterations* to a shifted and inverted matrix $(\lambda \mathbf{I} - \hat{\mathbf{X}})^{-1}$, where the shifting parameter λ is carefully chosen. The algorithm that implements this reduction, originally described in (Garber & Hazan, 2015), is given below (see Algorithm 1).

Algorithm 1 SHIFT-AND-INVERT POWER METHOD

- 1: Input: estimate $\tilde{\delta}$ for the gap $\hat{\delta}$, accuracy $\epsilon \in (0, 1)$, failure probability p
 - 2: Set: $m_1 \leftarrow \lceil 8 \ln(144d/p^2) \rceil, m_2 \leftarrow \lceil \frac{3}{2} \ln\left(\frac{18d}{p^2\epsilon}\right) \rceil$
 - 3: Set: $\tilde{\epsilon} \leftarrow \min \left\{ \frac{1}{16} \left(\tilde{\delta}/8\right)^{m_1+1}, \frac{\epsilon}{4} \left(\tilde{\delta}/8\right)^{m_2+1} \right\}$
 - 4: Set: $\lambda_{(0)} \leftarrow 1 + \tilde{\delta}, \hat{\mathbf{w}}_0 \leftarrow$ random unit vector, $s \leftarrow 0$
 - 5: **repeat**
 - 6: $s \leftarrow s + 1, \mathbf{M}_s \leftarrow (\lambda_{(s-1)} \mathbf{I} - \hat{\mathbf{X}})$
 - 7: **for** $t = 1 \dots m_1$ **do**
 - 8: Find approx. minimizer - $\hat{\mathbf{w}}_t$ of $F_{\lambda_{(s-1)}, \hat{\mathbf{w}}_{t-1}}(\mathbf{z})$ such that $\|\hat{\mathbf{w}}_t - \mathbf{M}_s^{-1} \hat{\mathbf{w}}_{t-1}\| \leq \tilde{\epsilon}$
 - 9: **end for**
 - 10: $\mathbf{w}_s \leftarrow \hat{\mathbf{w}}_{m_1} / \|\hat{\mathbf{w}}_{m_1}\|$
 - 11: Find approx. minimizer - \mathbf{v}_s of $F_{\lambda_{(s-1)}, \mathbf{w}_s}(\mathbf{z})$ such that $\|\mathbf{v}_s - \mathbf{M}_s^{-1} \mathbf{w}_s\| \leq \tilde{\epsilon}$
 - 12: $\Delta_s \leftarrow \frac{1}{2} \cdot \frac{1}{\mathbf{w}_s^\top \mathbf{v}_s - \tilde{\epsilon}}, \lambda_{(s)} \leftarrow \lambda_{(s-1)} - \frac{\Delta_s}{2}$
 - 13: **until** $\Delta_s \leq \tilde{\delta}$
 - 14: $\lambda_{(f)} \leftarrow \lambda_{(s)}, \mathbf{M}_f \leftarrow (\lambda_{(f)} \mathbf{I} - \hat{\mathbf{X}})$
 - 15: **for** $t = 1 \dots m_2$ **do**
 - 16: Find approx. minimizer - $\hat{\mathbf{w}}_t$ of $F_{\lambda_{(f)}, \hat{\mathbf{w}}_{t-1}}(\mathbf{z})$ such that $\|\hat{\mathbf{w}}_t - \mathbf{M}_f^{-1} \hat{\mathbf{w}}_{t-1}\| \leq \tilde{\epsilon}$
 - 17: **end for**
 - 18: Return: $\mathbf{w}_f \leftarrow \hat{\mathbf{w}}_{m_2} / \|\hat{\mathbf{w}}_{m_2}\|$
-

Lemma 5 (Efficient reduction of top eigenvector to convex optimization; originally Theorem 4.2 in (Garber & Hazan, 2015)). *Suppose that $\hat{\delta} := \lambda_1(\hat{\mathbf{X}}) - \lambda_2(\hat{\mathbf{X}}) > 0$ and suppose that the estimate $\tilde{\delta}$ in Algorithm 1 satisfies $\tilde{\delta} \in [\hat{\delta}/2, 3\hat{\delta}/4]$. Then, with probability at least $1 - p$, Algorithm 1 finds a unit vector \mathbf{w}_f such that $(\mathbf{w}_f^\top \hat{\mathbf{v}}_1)^2 \geq 1 - \epsilon$, and the total number of optimization problems of the form (8) solved during the run of the algorithm, is upper bounded by $O\left(\ln(d/p) \ln(\hat{\delta}^{-1}) + \ln\left(\frac{d}{p\epsilon}\right)\right)$. Moreover, throughout the run of the algorithm it holds that $1 + \hat{\delta} \geq \lambda_{(s)} - \hat{\lambda}_1 = \Omega(\hat{\delta})$.*

Remark: the purpose of the *repeat-until* loop in Algorithm 1 is to efficiently find a shifting parameter $\lambda_{(f)}$ such that $c_1 \hat{\delta} \leq \lambda_{(f)} - \hat{\lambda}_1 \leq c_2 \hat{\delta}$ for some universal constants $c_2 > c_1 > 0$. When n satisfies $n = \Omega(\delta^{-2} \ln(d/p))$, we can directly find (w.h.p) such a shifting parameter, by

simply estimating $\hat{\lambda}_1, \hat{\delta}$ from the data of a *single machine*. Also, we can take $\hat{\mathbf{w}}_0$ to be the leading eigenvector of any single machine, since this will already have a constant correlation with $\hat{\mathbf{v}}_1$. Thus, for such n , the total number of optimization problems can be reduced to $O(\ln(p^{-1}\epsilon^{-1}))$.

Algorithm 1 is a meta-algorithm in the sense that the choice of solver for the optimization problems $\min F_{\lambda, \mathbf{w}}$ is unspecified, and any solver will do. A simple calculation shows that a naive application of either the conjugate gradient method or Nesterov's accelerated gradient method to solve these optimization problems in a distributed manner, i.e., the computation of the gradient vector is distributed across machines, will require overall $\tilde{O}(\sqrt{\hat{\lambda}_1/\hat{\delta}})$ communication rounds, which does not give any improvement over the distributed Lanczos approach, described in Subsection 2.2.2. However, this can be substantially improved by taking advantage of the fact that the data on all machines is sampled i.i.d. from the same distribution. In particular, we present below an approach based on applying a preconditioner to the optimization Problem (8), in the spirit of the one described in (Zhang & Lin, 2015).

4.2. Faster Distributed Approximation of Linear Systems via Local Preconditioning

Let $\mathbf{M} = \lambda \mathbf{I} - \hat{\mathbf{X}}$, for some shift parameter $\lambda > \hat{\lambda}_1$, and define the pre-conditioning matrix $\mathbf{C} = (\lambda + \mu) \mathbf{I} - \hat{\mathbf{X}}_1$, where μ is required so \mathbf{C} is invertible. Consider now solving the following modified quadratic problem:

$$\tilde{F}_{\lambda, \mathbf{w}}(\mathbf{y}) := \frac{1}{2} \mathbf{y}^\top \mathbf{C}^{-1/2} \mathbf{M} \mathbf{C}^{-1/2} \mathbf{y} - \mathbf{y}^\top \mathbf{C}^{-1/2} \mathbf{w}. \quad (9)$$

Note that if \mathbf{y}^* is the optimal solution to Problem (9), i.e.,

$$\mathbf{y}^* = \mathbf{C}^{1/2} \mathbf{M}^{-1} \mathbf{C}^{1/2} \mathbf{C}^{-1/2} \mathbf{w} = \mathbf{C}^{1/2} \mathbf{M}^{-1} \mathbf{w},$$

then $\mathbf{z}^* := \mathbf{C}^{-1/2} \mathbf{y}^*$ is the optimal solution to Problem (8).

The idea behind choosing \mathbf{C} this way is very intuitive. Ideally we could have chosen $\mathbf{C} = \mathbf{M}$, making the condition number of $\tilde{F}_{\lambda, \mathbf{w}}$ equal to $\kappa(\tilde{F}_{\lambda, \mathbf{w}}) = 1$, which is the best we can hope for. The problem of course is that this requires us to explicitly compute $\mathbf{M}^{-1/2}$, which is more challenging than just computing the leading eigenvector of $\hat{\mathbf{X}}$. The next best thing is thus to choose \mathbf{C} based only on the data available on any single machine, which allows computing $\mathbf{C}^{-1/2}$ without additional communication overhead, and leads to the choice described above. The following lemma, rephrased from (Zhang & Lin, 2015), quantifies exactly how such a choice of \mathbf{C} helps in improving the condition number of the new optimization problem, Problem (9). The proof is given in the appendix.

Lemma 6. *Suppose that $\mu \geq \|\hat{\mathbf{X}} - \hat{\mathbf{X}}_1\|$. Then, $\tilde{F}_{\lambda, \mathbf{w}}(\mathbf{y})$ is 1-smooth and $\left(\frac{\lambda - \hat{\lambda}_1}{(\lambda - \hat{\lambda}_1) + 2\mu}\right)$ -strongly convex. In particular, $\kappa(\tilde{F}_{\lambda, \mathbf{w}}) \leq 1 + 2\mu/(\lambda - \hat{\lambda}_1)$. Moreover, fixing $\tilde{\mathbf{y}} \in \mathbb{R}^d$,*

if we let $\tilde{\mathbf{z}} := \mathbf{C}^{-1/2} \tilde{\mathbf{y}}$, then it holds that $\|\tilde{\mathbf{z}} - \mathbf{M}^{-1} \mathbf{w}\| \leq (\lambda - \hat{\lambda}_1)^{-1/2} \|\tilde{\mathbf{y}} - \mathbf{C}^{1/2} \mathbf{M}^{-1} \mathbf{w}\|$. In particular, for any $p \in (0, 1)$, if we set $\mu = 4\sqrt{\ln(d/p)/n}$, then the above holds with probability at least $1 - p$, where this probability depends only on the randomness in $\hat{\mathbf{X}}_1$.

4.2.1. SOLVING THE PRE-CONDITIONED LINEAR SYSTEMS

We now discuss the application of gradient-based algorithms for finding an approximate minimizer of the pre-conditioned problem, Problem (9), in our distributed setting. Towards this end we require a *distributed* implementation for the *first-order oracle* of $\tilde{F}_{\lambda, \mathbf{w}}(\mathbf{y})$ (i.e., computation of the value and gradient vector at a queried point).

A straight-forward implementation of the first-order oracle in our distributed setting is given in Algorithm 2.

Algorithm 2 Distributed First-Order Oracle for $\tilde{F}_{\lambda, \mathbf{w}}(\mathbf{y})$

- 1: Input: shift parameter $\lambda > 0$, regularization parameter $\mu > 0$, vector $\mathbf{w} \in \mathbb{R}^d$, query vector $\mathbf{y} \in \mathbb{R}^d$
 - 2: send $\tilde{\mathbf{y}} := \mathbf{C}^{-1/2} \mathbf{y}$ to machines $\{2, \dots, m\}$ for $\mathbf{C} := (\lambda + \mu) \mathbf{I} - \hat{\mathbf{X}}_1$ {executed on machine 1}
 - 3: **for** $i = 1 \dots m$ **do**
 - 4: send $\tilde{\mathbf{v}}_i := \hat{\mathbf{X}}_i \tilde{\mathbf{y}}$ to machine 1 {executed on each machine i }
 - 5: **end for**
 - 6: aggregate $\tilde{\mathbf{V}} := \frac{1}{m} \sum_{i=1}^m \tilde{\mathbf{v}}_i$ {executed on machine 1}
 - 7: compute $\tilde{F}_{\lambda, \mathbf{w}}(\mathbf{y}) = \frac{1}{2} (\lambda \mathbf{y}^\top \mathbf{C}^{-1} \mathbf{y} - \mathbf{y}^\top \mathbf{C}^{-1/2} \tilde{\mathbf{V}}) - \mathbf{y}^\top \mathbf{C}^{-1/2} \mathbf{w}$ {executed on machine 1}
 - 8: compute $\nabla \tilde{F}_{\lambda, \mathbf{w}}(\mathbf{y}) = \lambda \mathbf{C}^{-1} \mathbf{y} - \mathbf{C}^{-1/2} \tilde{\mathbf{V}} - \mathbf{C}^{-1/2} \mathbf{w}$ {executed on machine 1}
 - 9: return: $(\tilde{F}_{\lambda, \mathbf{w}}(\mathbf{y}), \nabla \tilde{F}_{\lambda, \mathbf{w}}(\mathbf{y}))$
-

We have the following lemma, the proof of which is deferred to the appendix.

Lemma 7. *Fix some $\lambda > \lambda_1(\hat{\mathbf{X}})$ and $\mathbf{w} \in \mathbb{R}^d$, and let $1 \geq \mu > 0$ be as in Lemma 6. Fix $\epsilon > 0$. Consider the following two-step algorithm:*

1. *Apply either the conjugate gradient method or Nesterov's accelerated method with the distributed first-order oracle described in Algorithm 2 to find $\tilde{\mathbf{y}} \in \mathbb{R}^d$ such that $\tilde{F}_{\lambda, \mathbf{w}}(\tilde{\mathbf{y}}) - \min_{\mathbf{y} \in \mathbb{R}^d} \tilde{F}_{\lambda, \mathbf{w}}(\mathbf{y}) \leq \epsilon'$*
2. *Return $\tilde{\mathbf{z}} = \mathbf{C}^{-1/2} \tilde{\mathbf{y}}$.*

Then, for $\epsilon' = \frac{\epsilon}{2} \left(1 + \frac{2\mu}{\lambda - \hat{\lambda}_1}\right)^{-1} (\lambda - \hat{\lambda}_1)$ it holds that $\|\tilde{\mathbf{z}} - (\lambda \mathbf{I} - \hat{\mathbf{X}}_1)^{-1} \mathbf{w}\| \leq \epsilon$, and the total number distributed matrix-vector products with the empirical covariance matrix $\hat{\mathbf{X}}$ required to compute $\tilde{\mathbf{z}}$ is upper-bounded by $O\left(\sqrt{1 + 2\mu(\lambda - \hat{\lambda}_1)^{-1}} \ln\left(\left(1 + \frac{2\mu}{\lambda - \hat{\lambda}_1}\right) \|\mathbf{w}\| / [(\lambda - \hat{\lambda}_1)\epsilon]\right)\right)$.

4.3. Putting it all together

We now state our main result for this section, which is a simple consequence of the previous lemmas. The full proof is given in the appendix.

Theorem 6. Fix $\epsilon \in (0, 1)$ and $p \in (0, 1)$. Suppose that $mn = \Omega(\delta^{-2} \ln(d/p))$. Set $\mu = 4\sqrt{\ln(3d/p)/n}$. Applying the Shift-and-Invert algorithm, Algorithm 1, with the parameters $\epsilon, p/3$, and applying the algorithm in Lemma 7 with the parameter μ , to approximately solve the linear systems, yields with probability at least $1 - p$ a unit vector \mathbf{w}_f such that $(\mathbf{w}_f^\top \hat{\mathbf{v}}_1)^2 \geq 1 - \epsilon$, after executing at most

$$O\left(\sqrt{\frac{\sqrt{\ln(d/p)}}{\delta\sqrt{n}}}\left[\ln\left(\frac{d}{p\epsilon^2}\right)\ln\left(\frac{\sqrt{\ln(d/p)}}{\delta^2\sqrt{n}}\right) + \ln^2\left(\frac{d}{p\epsilon^2}\right)\ln\left(\frac{1}{\delta}\right)\right]\right) = \tilde{O}\left(\sqrt{\frac{1}{\delta\sqrt{n}}}\right)$$

distributed matrix-vector products with the empirical covariance matrix $\hat{\mathbf{X}}$.

5. Experiments

To validate some of our theoretical findings we conducted experiments with single-round algorithms on synthetic data. We generated synthetic datasets using two distributions. For both distributions we used the covariance matrix $\mathbf{X} = \mathbf{U}\Sigma\mathbf{U}^\top$ with \mathbf{U} being a random $d \times d$ orthonormal matrix and Σ is diagonal satisfying: $\Sigma(1, 1) = 1$, $\Sigma(2, 2) = 0.8$, $\forall j \geq 3 : \Sigma(j, j) = 0.9 \cdot \Sigma(j-1, j-1)$, i.e., $\delta = 0.2$. One dataset was generated according to the normal distributions $\mathcal{N}(0, \mathbf{X})$, and for the second datasets we generated samples by taking $\mathbf{x} = \sqrt{3/2}\mathbf{X}^{1/2}\mathbf{y}$ where $\mathbf{y} \sim U[-1, 1]$. In both cases we set $d = 300$.

Beyond the single-round algorithms that are based on aggregating the individual ERM solutions described so far, we propose an additional natural aggregation approach, based on aggregating the individual projection matrices. More concretely, letting $\{\hat{\mathbf{v}}_1^{(i)}\}_{i=1}^m$ denote the leading eigenvectors of the individual machines, let $\bar{\mathbf{P}}_1 := \frac{1}{m} \sum_{i=1}^m \hat{\mathbf{v}}_1^{(i)} \hat{\mathbf{v}}_1^{(i)\top}$. We then take the final estimate \mathbf{w} to be the leading eigenvector of the aggregated matrix $\bar{\mathbf{P}}_1$. Note that as with the sign-fixing based aggregation, this approach also resolves the sign-ambiguity in the estimates produced by the different machines, which circumvents the lower bound result of Theorem 3.

For both datasets we fixed the number of machines to $m = 25$. We tested the estimation error (i.e., the value $1 - (\mathbf{w}^\top \mathbf{v}_1)^2$ where \mathbf{v}_1 is the leading eigenvector of \mathbf{X} and \mathbf{w} is the estimator) of five benchmarks vs. the per-machine sample size n : the centralized solution $\hat{\mathbf{v}}_1$, the average of the individual (unbiased) ERM solutions (normalized to unit norm), the average of ERM solutions with sign-fixing, and the leading eigenvector of the averaged projection ma-

trix. We also plotted the average loss of the individual ERM solutions. Results are averaged over 400 independent runs.

The results for the normal distribution appear in Figure 1. The results for the uniform-based distribution are very similar and are deferred to the appendix. We can see that, as our lower bound in Theorem 3 suggests, simply averaging and normalizing the individual ERM solutions has significantly worse performance than the centralized ERM solution. Perhaps surprisingly, the performance of this estimator is even worse than the average error of an estimate computed using only a single machine. We see that both aggregation methods that are based on correlating the individual ERM solutions, namely the sign-fixing-based estimator, and the proposed averaging-of-projections heuristic, are asymptotically consistent with the centralized ERM. In particular, the averaging-of-projections scheme, at least empirically, significantly outperforms the sign-fixing approach, which justifies further theoretical investigation of this heuristic. For the sign fixing approach, we can see that as suggested by our bounds, the estimator is not consistent with the centralized ERM solution for small values of n .

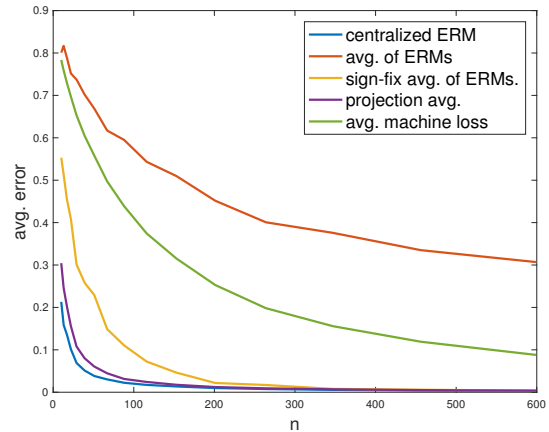


Figure 1. Estimation error vs. the per-machine sample size n for a normal distribution.

6. Discussion

We presented communication-efficient algorithms for distributed statistical estimation of principal components. Focusing on our results for methods based on a single communication round, we initiated a study of how to correctly aggregate distributed ERM solutions in a non-convex setting. An important take-home message of our work is that in a non-convex setting, simply averaging the local solutions is not a good idea. On the positive side, we show that a very simple correction (i.e., sign-fixing) is possible by leveraging the specific structure of the problem at hand. It is thus interesting to develop a richer theory of how to perform such aggregations in more involved non-convex problems.

References

- Eigenvalues and eigenvectors of 2x2 matrices. http://www.math.harvard.edu/archive/21b_fall_04/exhibits/2dmatrices/.
- Allen Zhu, Zeyuan and Li, Yuanzhi. Even faster SVD decomposition yet without agonizing pain. In *Advances in Neural Information Processing Systems 29: Annual Conference on Neural Information Processing Systems 2016, December 5-10, 2016, Barcelona, Spain*, pp. 974–982, 2016a.
- Allen Zhu, Zeyuan and Li, Yuanzhi. Fast global convergence of online PCA. *CoRR*, abs/1607.07837, 2016b.
- Balsubramani, Akshay, Dasgupta, Sanjoy, and Freund, Yoav. The fast convergence of incremental PCA. In *Advances in Neural Information Processing Systems 26: 27th Annual Conference on Neural Information Processing Systems 2013*, pp. 3174–3182, 2013.
- Boutsidis, Christos, Woodruff, David P, and Zhong, Peilin. Optimal principal component analysis in distributed and streaming models. In *Proceedings of the 48th Annual ACM SIGACT Symposium on Theory of Computing*, pp. 236–249. ACM, 2016.
- Garber, Dan and Hazan, Elad. Fast and simple pca via convex optimization. *arXiv preprint arXiv:1509.05647*, 2015.
- Garber, Dan, Hazan, Elad, Jin, Chi, Kakade, Sham M., Musco, Cameron, Netrapalli, Praneeth, and Sidford, Aaron. Faster eigenvector computation via shift-and-invert preconditioning. *CoRR*, abs/1605.08754, 2016.
- Golub, Gene H and Pereyra, Victor. The differentiation of pseudo-inverses and nonlinear least squares problems whose variables separate. *SIAM Journal on numerical analysis*, 10(2):413–432, 1973.
- Hotelling, H. Analysis of a complex of statistical variables into principal components. *J. Educ. Psych.*, 24, 1933.
- Jaggi, Martin, Smith, Virginia, Takác, Martin, Terhorst, Jonathan, Krishnan, Sanjay, Hofmann, Thomas, and Jordan, Michael I. Communication-efficient distributed dual coordinate ascent. In *Advances in Neural Information Processing Systems*, pp. 3068–3076, 2014.
- Jain, Prateek, Jin, Chi, Kakade, Sham M, Netrapalli, Praneeth, and Sidford, Aaron. Matching matrix bernstein with little memory: Near-optimal finite sample guarantees for oja’s algorithm. *arXiv preprint arXiv:1602.06929*, 2016a.
- Jain, Prateek, Jin, Chi, Kakade, Sham M, Netrapalli, Praneeth, and Sidford, Aaron. Matching matrix bernstein with little memory: Near-optimal finite sample guarantees for oja’s algorithm. *arXiv preprint arXiv:1602.06929*, 2016b.
- Jolliffe, IT. Principal component analysis. 2002. *Springer-Verlag, New York*, 2002.
- Lee, Jason D., Ma, Tengyu, and Lin, Qihang. Distributed stochastic variance reduced gradient methods. *CoRR*, abs/1507.07595, 2015.
- Liang, Yingyu, Balcan, Maria-Florina F, Kanchanapally, Vandana, and Woodruff, David. Improved distributed principal component analysis. In *NIPS*, 2014.
- Magnus, Jan R. On differentiating eigenvalues and eigenvectors. *Econometric Theory*, 1(02):179–191, 1985.
- Pearson, K. On lines and planes of closest fit to systems of points in space. *Philosophical Magazine*, 2(6):559–572, 1901.
- Reddi, Sashank J., Konečný, Jakub, Richtárik, Peter, Póczos, Barnabás, and Smola, Alexander J. AIDE: fast and communication efficient distributed optimization. *CoRR*, abs/1608.06879, 2016.
- Shamir, Ohad. A stochastic PCA and SVD algorithm with an exponential convergence rate. In *Proceedings of the 32nd International Conference on Machine Learning, ICML 2015, Lille, France, 6-11 July 2015*, pp. 144–152, 2015.
- Shamir, Ohad. Convergence of stochastic gradient descent for PCA. In *Proceedings of the 33rd International Conference on Machine Learning, ICML 2016, New York City, NY, USA, June 19-24, 2016*, pp. 257–265, 2016a.
- Shamir, Ohad. Without-replacement sampling for stochastic gradient methods. In *Advances in Neural Information Processing Systems 29: Annual Conference on Neural Information Processing Systems 2016, December 5-10, 2016, Barcelona, Spain*, pp. 46–54, 2016b.
- Shamir, Ohad. Fast stochastic algorithms for svd and pca: Convergence properties and convexity. In *Proceedings of The 33rd International Conference on Machine Learning*, pp. 248–256, 2016c.
- Shamir, Ohad, Srebro, Nathan, and Zhang, Tong. Communication-efficient distributed optimization using an approximate newton-type method. In *Proceedings of the 31th International Conference on Machine Learning, ICML 2014, Beijing, China, 21-26 June 2014*, pp. 1000–1008, 2014.

Tropp, Joel A. User-friendly tail bounds for sums of random matrices. *Foundations of Computational Mathematics*, 12(4):389–434, 2012.

Yu, Yi, Wang, Tengyao, and Samworth, Richard J. A useful variant of the davis–kahan theorem for statisticians. *Biometrika*, 102(2):315–323, 2015.

Zhang, Yuchen and Lin, Xiao. Disco: Distributed optimization for self-concordant empirical loss. In *Proceedings of the 32nd International Conference on Machine Learning (ICML-15)*, pp. 362–370, 2015.

Zhang, Yuchen, Duchi, John C, and Wainwright, Martin J. Communication-efficient algorithms for statistical optimization. *Journal of Machine Learning Research*, 14: 3321–3363, 2013.

A. Proofs Omitted from Section 3

A.1. Proof of Theorem 3

Proof. Consider the following distribution over \mathbb{R}^2 .

$$\mathbf{x} = \mathbf{e}_1 + \begin{pmatrix} \epsilon_1 \\ \epsilon_2 \end{pmatrix}, \quad \epsilon_1, \epsilon_2 \sim U\{-1, +1\},$$

where \mathbf{e}_1 is the first standard basis vector in \mathbb{R}^2 .

The population covariance matrix and the empirical covariance matrix of a sample of size n are clearly given by

$$\mathbf{X} = \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}, \quad \hat{\mathbf{X}}_{(n)} = \begin{pmatrix} 2 & y_n \\ y_n & 1 \end{pmatrix},$$

where y_n is a random variable which is the average of n $U\{-1, +1\}$ random variables. By elementary calculations we have that the leading eigenvector of $\hat{\mathbf{X}}_{(n)}$ is given by

$$\hat{\mathbf{v}}_1 = \sigma \cdot C(y_n) \cdot \left(1, \frac{2y_n}{1 + \sqrt{1 + 4y_n^2}} \right),$$

where

$$C(y_n) := \left(1 + \left(\frac{2y_n}{1 + \sqrt{1 + 4y_n^2}} \right)^2 \right)^{-1/2}$$

is the normalization factor that guarantees that $\hat{\mathbf{v}}_1$ is a unit vector. In particular, it holds that $1/\sqrt{2} \leq C(y_n) \leq 1$. The random variable $\sigma \sim U\{-1, +1\}$ is independent of y_n and determines the sign of $\hat{\mathbf{v}}_1$, which follows from our assumption that $\hat{\mathbf{v}}_1$ is generated by unbiased ERM.

Consider now the average of m such unit vectors $\hat{\mathbf{v}}_1^{(1)} \dots \hat{\mathbf{v}}_1^{(m)}$ given by $\bar{\mathbf{v}} = \frac{1}{m} \sum_{i=1}^m \hat{\mathbf{v}}_1^{(i)}$ and the normalized estimate $\bar{\mathbf{v}}_1 / \|\bar{\mathbf{v}}_1\|$, and recall that the leading eigenvector of the population covariance matrix is \mathbf{e}_1 . It holds that

$$\left\langle \frac{\bar{\mathbf{v}}_1}{\|\bar{\mathbf{v}}_1\|}, \mathbf{e}_1 \right\rangle^2 = \frac{\bar{\mathbf{v}}_1(1)^2}{\bar{\mathbf{v}}_1(1)^2 + \bar{\mathbf{v}}_1(2)^2} = 1 - \frac{\bar{\mathbf{v}}_1(2)^2}{\bar{\mathbf{v}}_1(1)^2 + \bar{\mathbf{v}}_1(2)^2}. \quad (10)$$

Towards upper-bounding the RHS of (10) in expectation, the main step is to lower bound the random variable $|\bar{\mathbf{v}}_1(2)|$ using Chebyshev's inequality.

It holds that

$$\begin{aligned} \mathbb{E}[|\bar{\mathbf{v}}_1(2)|] &= \mathbb{E} \left[\left| \frac{1}{m} \hat{\mathbf{v}}_1^{(i)}(2) \right| \right] = \mathbb{E} \left[\left| \frac{1}{m} \sum_{i=1}^m \sigma^{(i)} \frac{2C(y_n^{(i)})y_n^{(i)}}{1 + \sqrt{1 + 4y_n^{(i)2}}} \right| \right] \\ &\stackrel{(a)}{=} \mathbb{E} \left[\left| \frac{1}{m} \sum_{i=1}^m \sigma^{(i)} \frac{2C(y_n^{(i)})|y_n^{(i)}|}{1 + \sqrt{1 + 4y_n^{(i)2}}} \right| \right] \\ &= \mathbb{E}_{\{\sigma^{(i)}\}} \left[\mathbb{E}_{\{y_n^{(i)}\}} \left[\left| \frac{1}{m} \sum_{i=1}^m \sigma^{(i)} \frac{2C(y_n^{(i)})|y_n^{(i)}|}{1 + \sqrt{1 + 4y_n^{(i)2}}} \right| \mid \{\sigma^{(i)}\} \right] \right] \\ &\stackrel{(b)}{\geq} \mathbb{E}_{\{\sigma^{(i)}\}} \left[\mathbb{E}_{\{y_n^{(i)}\}} \left[\frac{1}{m} \sum_{i=1}^m \sigma^{(i)} \frac{2C(y_n^{(i)})|y_n^{(i)}|}{1 + \sqrt{1 + 4y_n^{(i)2}}} \mid \{\sigma^{(i)}\} \right] \right] \\ &\stackrel{(c)}{=} \mathbb{E}_{\{\sigma^{(i)}\}} \left[\left| \frac{1}{m} \sum_{i=1}^m \sigma^{(i)} \right| \right] \cdot \mathbb{E}_{y_n} \left[\frac{2C(y_n)|y_n|}{1 + \sqrt{1 + 4y_n^2}} \right] \stackrel{(d)}{=} \Theta \left(\frac{1}{\sqrt{mn}} \right), \quad (11) \end{aligned}$$

where (a) follows since $\sigma^{(i)}y_n^{(i)} \sim \sigma^{(i)}|y_n^{(i)}|$ and $C(y_n^{(i)})/(1 + \sqrt{1 + 4y_n^{(i)2}})$ depends only on $|y_n^{(i)}|$, (b) follows from the triangle inequality, and (c) follows since $\{\sigma^{(i)}\}_{i \in [m]}$ and $\{y_n^{(i)}\}_{i \in [m]}$ are independent random variables. Finally, it is easy to verify that (d) follows since $\sum_{i=1}^m \sigma^{(i)}/m$ is the average of m $U\{-1, +1\}$ random variables and hence its expected absolute value is $\Theta(1/\sqrt{m})$. Similarly the expected absolute value of y_n is $\Theta(1/\sqrt{n})$ and $C(y_n)/(1 + \sqrt{1 + 4y_n^2})$ is lower bounded by a positive constant.

Also, observe that

$$\begin{aligned} \mathbb{E}[\bar{\mathbf{v}}_1(2)^2] &= \mathbb{E}\left[\left(\frac{1}{m}\hat{\mathbf{v}}_1^{(i)}(2)\right)^2\right] = \frac{1}{m}\mathbb{E}[\hat{\mathbf{v}}_1(2)^2] = \frac{1}{m}\mathbb{E}\left[\left(\frac{2C(y_n)y_n}{1 + \sqrt{1 + 4y_n^2}}\right)^2\right] \\ &\geq \frac{1}{2m}\mathbb{E}[y_n^2] = \Theta\left(\frac{1}{mn}\right), \end{aligned} \quad (12)$$

where the inequality follows since $|y_n| \leq 1$ and $1/\sqrt{2} \leq C(y_n) \leq 1$.

Combining Eq. (11) and Eq. (12), we have by an application of Chebyshev's inequality to the random variable $|\bar{\mathbf{v}}_1(2)|$ that there exists universal constants $c_1 > 0$ such that

$$\Pr\left(|\bar{\mathbf{v}}_1(2)| \leq \frac{1}{c_1\sqrt{mn}}\right) \leq \frac{1}{4}. \quad (13)$$

Also, it is easy to verify that

$$\mathbb{E}[\bar{\mathbf{v}}_1(1)^2] = O(1/m), \quad \mathbb{E}[\bar{\mathbf{v}}_1(2)^2] = O(1/m).$$

Thus, by a simple application of Markov's inequality we have that there exists a universal constant $c_2 > 0$ such that

$$\Pr\left(\max\{\bar{\mathbf{v}}_1(1)^2, \bar{\mathbf{v}}_1(2)^2\} \geq \frac{1}{c_3m}\right) \leq \frac{1}{4}. \quad (14)$$

Using Eq. (10), (13) and (14) we finally have that

$$\mathbb{E}\left[\left\langle \frac{\bar{\mathbf{v}}_1}{\|\bar{\mathbf{v}}_1\|}, \mathbf{e}_1 \right\rangle^2\right] = 1 - \mathbb{E}\left[\frac{\bar{\mathbf{v}}_1(2)^2}{\bar{\mathbf{v}}_1(1)^2 + \bar{\mathbf{v}}_1(2)^2}\right] = 1 - \Omega\left(\frac{1}{n}\right).$$

□

A.2. Proof of Lemma 2

Proof. The proof is based on viewing $\hat{\mathbf{A}}$ as an unbiased perturbation of the matrix \mathbf{A} , and computing a Taylor expansion of $\hat{\mathbf{v}}_1$ around \mathbf{v}_1 . For notational convenience, let $\mathbf{E} = \hat{\mathbf{A}} - \mathbf{A}$, and define $\mathbf{A}(t) = \mathbf{A} + t\mathbf{E}$ for $t \in [0, 1]$. Also, define $\lambda(t)$ to be the leading eigenvalue of $\mathbf{A}(t)$.

First, we note that for any $t \in [0, 1]$, $\mathbf{A}(t)$ has an eigengap of at least $\delta/2$ between its first two eigenvalues (since by Weyl's inequality, its eigenvalues are at most $\|t\mathbf{E}\| \leq \|\mathbf{E}\| \leq \delta/4$ different than \mathbf{A} , and we know that \mathbf{A} has an eigengap of δ). Therefore, the leading eigenvalue of $\mathbf{A}(t)$ is simple. This means that the function $\mathbf{v}(t)$, which equals the leading eigenvector of $\mathbf{A}(t)$, is uniquely defined up to a sign. This sign will be chosen so that $\langle \mathbf{v}(t), \mathbf{v}_1 \rangle \geq 0$, which makes $\mathbf{v}(t)$ unique and well-defined². By Theorem 1 in (Magnus, 1985), we have that both $\lambda(t)$ and $\mathbf{v}(t)$ are infinitely differentiable at any $t \in [0, 1]$, and satisfy³

$$\lambda'(t) = \mathbf{v}(t)^\top \mathbf{E} \mathbf{v}(t), \quad \mathbf{v}'(t) = (\lambda(t)\mathbf{I} - \mathbf{A}(t))^\dagger \mathbf{E} \mathbf{v}(t).$$

²Note that ties are impossible, since that can only happen if $\langle \mathbf{v}(t), \mathbf{v}_1 \rangle = 0$, yet by applying the Davis-Kahan $\sin(\theta)$ theorem (Theorem 2), $\sqrt{1 - \langle \mathbf{v}(t), \mathbf{v}_1 \rangle^2} \leq \frac{2\|\mathbf{A}(t) - \mathbf{A}\|}{\delta} \leq \frac{2\|\mathbf{E}\|}{\delta} \leq \frac{1}{2}$.

³Formally speaking, the theorem only ensures $\mathbf{v}(t), \lambda(t)$ exist and are infinitely differentiable in some open neighborhood of t . However, since the result holds for any $t \in [0, 1]$, and the proof implies that these functions are unique in each such neighborhood (where the uniqueness of $\mathbf{v}(t)$ holds once we fixed the sign as above), it follows that the same holds in all of $t \in [0, 1]$.

We will also need to bound the second derivative of $\mathbf{v}(t)$. By the product rule and the equations above, this derivative equals

$$\begin{aligned}\mathbf{v}''(t) &= \frac{\partial}{\partial t} ((\lambda(t)\mathbf{I} - \mathbf{A}(t))^\dagger) \mathbf{E}\mathbf{v}(t) + (\lambda(t)\mathbf{I} - \mathbf{A}(t))^\dagger \mathbf{E} \frac{\partial}{\partial t} \mathbf{v}(t) \\ &= \frac{\partial}{\partial t} ((\lambda(t)\mathbf{I} - \mathbf{A}(t))^\dagger) \mathbf{E}\mathbf{v}(t) + (\lambda(t)\mathbf{I} - \mathbf{A}(t))^\dagger \mathbf{E} (\lambda(t)\mathbf{I} - \mathbf{A}(t))^\dagger \mathbf{E}\mathbf{v}(t).\end{aligned}\quad (15)$$

To compute the derivative above, we apply the chain rule. The derivative of a pseudo-inverse \mathbf{B}^\dagger of a matrix-valued function $\mathbf{B} = \mathbf{B}(t)$ with respect to t (assuming \mathbf{B} and hence its pseudo-inverse is symmetric for all t) is given by (see Theorem 4.3 in (Golub & Pereyra, 1973))

$$-\mathbf{B}^\dagger \left(\frac{\partial}{\partial t} \mathbf{B} \right) \mathbf{B}^\dagger + (\mathbf{B}^\dagger)^2 \left(\frac{\partial}{\partial t} \mathbf{B} \right) (\mathbf{I} - \mathbf{B}\mathbf{B}^\dagger) + (\mathbf{I} - \mathbf{B}^\dagger\mathbf{B}) \left(\frac{\partial}{\partial t} \mathbf{B} \right) (\mathbf{B}^\dagger)^2.$$

This formula is true assuming the rank of \mathbf{B} is constant in some open neighborhood of t . Applying this for $\mathbf{B} = \lambda(t)\mathbf{I} - \mathbf{A}(t)$ (which indeed has a fixed rank of $d - 1$ by the eigengap assumption), noting that $\left\| \frac{\partial}{\partial t} (\lambda(t)\mathbf{I} - \mathbf{A}(t)) \right\| = \left\| \mathbf{v}(t)^\top \mathbf{E}\mathbf{v}(t)\mathbf{I} - \mathbf{E} \right\| \leq 2\|\mathbf{E}\|$, and using the facts that $\|\mathbf{v}(t)\| = 1$, $\|\mathbf{I} - \mathbf{B}^\dagger\mathbf{B}\| \leq 1$, $\|\mathbf{I} - \mathbf{B}\mathbf{B}^\dagger\| \leq 1$ and $\|(\lambda(t)\mathbf{I} - \mathbf{A}(t))^\dagger\| \leq 2/\delta$ (since the smallest non-zero eigenvalue of $\lambda(t)\mathbf{I} - \mathbf{A}(t)$ is at least $\delta/2$), we have that

$$\left\| \frac{\partial}{\partial t} ((\lambda(t)\mathbf{I} - \mathbf{A}(t))^\dagger) \right\| \leq \frac{24 \cdot \|\mathbf{E}\|}{\delta^2}.$$

Plugging this into (15), and again using the fact that $\|(\lambda(t)\mathbf{I} - \mathbf{A}(t))^\dagger\| \leq 2/\delta$, we get that

$$\|\mathbf{v}''(t)\| \leq \frac{c\|\mathbf{E}\|^2}{\delta^2}$$

for some numerical constant c .

By a first-order Taylor expansion of $\mathbf{v}(t)$ with an explicit remainder term⁴,

$$\mathbf{v}(1) = \mathbf{v}(0) + \mathbf{v}'(0) + \frac{1}{2} \int_{t=0}^1 (1-t)^2 \mathbf{v}''(t) dt,$$

which by the equations above and the definition of $\mathbf{v}(t)$ implies that

$$\hat{\mathbf{v}}_1 = \mathbf{v}_1 + (\lambda_1\mathbf{I} - \mathbf{A})^\dagger \mathbf{E}\mathbf{v}_1 + \frac{1}{2} \int_{t=0}^1 (1-t)^2 \mathbf{v}''(t) dt.$$

This implies

$$\|\hat{\mathbf{v}}_1 - \mathbf{v}_1 - (\lambda_1\mathbf{I} - \mathbf{A})^\dagger \mathbf{E}\mathbf{v}_1\| \leq \frac{1}{2} \int_{t=0}^1 (1-t)^2 \|\mathbf{v}''(t)\| dt \leq \frac{c\|\mathbf{E}\|^2}{2\lambda^2} \int_{t=0}^1 (1-t)^2 dt,$$

which is at most $c'\|\mathbf{E}\|^2/\lambda^2$ for some appropriate numerical constant c' . Plugging back $\mathbf{E} = \hat{\mathbf{A}} - \mathbf{A}$, the result follows. \square

A.3. Proof of Lemma 3

Proof. Using the matrix Hoeffding inequality (Theorem 1) and a union bound, we that

$$\Pr \left(\exists i, \|\hat{\mathbf{X}}_i - \mathbf{X}\| > \frac{\delta}{12} \right) \leq md \exp \left(-\frac{\delta^2 n}{c'b^2} \right) \quad (16)$$

for some constant $c' > 0$. Thus, with high probability, $\max_i \|\hat{\mathbf{X}}_i - \mathbf{X}\| \leq \delta/12$. By Weyl's inequality, it follows that the eigenvalues of \mathbf{X} and $\hat{\mathbf{X}}_i$ are at most $\delta/12$ apart, and since \mathbf{X} has an eigengap of δ between its two leading eigenvalues,

⁴Since $\mathbf{v}(t)$, $\mathbf{v}'(t)$, $\mathbf{v}''(t)$ are all vectors, this is a direct consequence of the standard Taylor expansion of the scalar function $t \mapsto \mathbf{v}(t)_j$, mapping t to the j -th coordinate of $\mathbf{v}(t)$, using the fact that this mapping is differentiable to any order (see Theorem 1 in (Magnus, 1985), and in particular twice continuously differentiable).

it follows that $\hat{\mathbf{X}}_i$ has an eigengap of at least $\delta - \delta/12 - \delta/12 > 0$, which proves the first part of the lemma. To handle the second part, note that by a variant of the Davis-Kahan $\sin\theta$ theorem (see Corollary 1 in (Yu et al., 2015)), if $\max_i \|\hat{\mathbf{X}}_i - \mathbf{X}\| \leq \delta/12$, then the leading eigenvectors $\hat{\mathbf{v}}_1^i$ of $\hat{\mathbf{X}}_i$ (after choosing the sign appropriately, i.e. $\langle \hat{\mathbf{v}}_1^i, \mathbf{v}_1 \rangle \geq 0$) are all at a distance of at most $1/4$ from \mathbf{v}_1 . Moreover, by Lemma 2,

$$\frac{1}{m} \sum_{i=1}^m \left\| \hat{\mathbf{v}}_1^i - \mathbf{v}_1 - (\lambda_1 \mathbf{I} - \mathbf{X})^\dagger (\hat{\mathbf{X}}_i - \mathbf{X}) \mathbf{v}_1 \right\| \leq \frac{c}{\delta^2} \cdot \frac{1}{m} \sum_{i=1}^m \|\hat{\mathbf{X}}_i - \mathbf{X}\|^2.$$

By the triangle inequality, this implies

$$\left\| \frac{1}{m} \sum_{i=1}^m \hat{\mathbf{v}}_1^i - \mathbf{v}_1 - (\lambda_1 \mathbf{I} - \mathbf{X})^\dagger \left(\frac{1}{m} \sum_{i=1}^m (\hat{\mathbf{X}}_i - \mathbf{X}) \right) \mathbf{v}_1 \right\| \leq \frac{c}{\delta^2} \cdot \frac{1}{m} \sum_{i=1}^m \|\hat{\mathbf{X}}_i - \mathbf{X}\|^2,$$

and therefore (as $\|\mathbf{v}_1\| = 1$),

$$\left\| \frac{1}{m} \sum_{i=1}^m \hat{\mathbf{v}}_1^i - \mathbf{v}_1 \right\| \leq \frac{c}{\delta^2} \cdot \frac{1}{m} \sum_{i=1}^m \|\hat{\mathbf{X}}_i - \mathbf{X}\|^2 + \|(\lambda_1 \mathbf{I} - \mathbf{X})^\dagger\| \cdot \left\| \frac{1}{m} \sum_{i=1}^m \hat{\mathbf{X}}_i - \mathbf{X} \right\|. \quad (17)$$

Since \mathbf{X} has an eigengap of δ , it follows that the minimal non-zero eigenvalue of $\lambda_1 \mathbf{I} - \mathbf{X}$ is at least δ , and therefore $\|(\lambda_1 \mathbf{I} - \mathbf{X})^\dagger\| \leq 1/\delta$. As to the other terms, recall that $\hat{\mathbf{X}}_i$ is the average of n i.i.d. matrices with mean \mathbf{X} , and $\frac{1}{m} \sum_{i=1}^m \hat{\mathbf{X}}_i$ is the average of mn such i.i.d. matrices. Thus, by a matrix Hoeffding inequality (Theorem 1) and a union bound, it holds with probability at least $1 - p$ that

$$\forall i, \|\hat{\mathbf{X}}_i - \mathbf{X}\| \leq c_1 \sqrt{\frac{b^2 \log(2dm/p)}{n}}$$

as well as

$$\left\| \frac{1}{m} \sum_{i=1}^m \hat{\mathbf{X}}_i - \mathbf{X} \right\| \leq c_1 \sqrt{\frac{b^2 \log(2dm/p)}{mn}}$$

for some constant c_1 . Combining this with (16) using a union bound, and plugging into (17), it follows that with probability at least $1 - p - d \exp\left(-\frac{\delta^2 n}{c'b^2}\right)$,

$$\left\| \frac{1}{m} \sum_{i=1}^m \hat{\mathbf{v}}_1^i - \mathbf{v}_1 \right\| \leq \frac{cc_1^2 b^2 \log(2dm/p)}{\delta^2 n} + c_1 \sqrt{\frac{b^2 \log(2dm/p)}{\delta^2 mn}}.$$

Slightly simplifying, the result follows. \square

A.4. Proof of Theorem 4

Proof of Thm. 4. The proof is an easy consequence of Lemma 3. Assuming the events in the lemma occur, we have that the leading eigenvalues of \mathbf{X} as well as $\hat{\mathbf{X}}_i$ for all i are simple, hence the leading eigenvectors are all unique up to a sign. In particular, let \mathbf{v}_1 be the eigenvector closest to $\hat{\mathbf{w}}_1 = \hat{\mathbf{w}}_1$, with ties broken arbitrarily, so that $\|\hat{\mathbf{w}}_1 - \mathbf{v}_1\| \leq \|\hat{\mathbf{w}}_1 + \mathbf{v}_1\|$. This implies that $\hat{\mathbf{w}}_1 = \hat{\mathbf{v}}_1^1$ (where $\hat{\mathbf{v}}_1^1$ is as defined in Lemma 3), since otherwise, by the inequality above, we would get $\|-\hat{\mathbf{v}}_1^1 - \mathbf{v}_1\| \leq \|-\hat{\mathbf{v}}_1^1 + \mathbf{v}_1\|$, which implies in turn $\langle \hat{\mathbf{v}}_1^1, \mathbf{v}_1 \rangle \leq 0$, contradicting the fact that $\|\hat{\mathbf{v}}_1^1 - \mathbf{v}_1\| = \sqrt{2 - 2\langle \hat{\mathbf{v}}_1^1, \mathbf{v}_1 \rangle}$ is at most $1/4$ by Lemma 3.

Having established that $\hat{\mathbf{w}}_1 = \hat{\mathbf{v}}_1^1$, we note that by Lemma 3 and the triangle inequality, for any $i > 1$,

$$\|\hat{\mathbf{v}}_1^i - \hat{\mathbf{v}}_1^1\| \leq \frac{1}{2} \quad \text{and therefore} \quad \|\hat{\mathbf{v}}_1^i - \hat{\mathbf{w}}_1\| \leq \frac{1}{2}.$$

As $\hat{\mathbf{v}}_1^i, \hat{\mathbf{w}}_1$ are unit vectors, this implies that $\|\hat{\mathbf{v}}_1^i - \hat{\mathbf{w}}_1\| < \|-\hat{\mathbf{v}}_1^i - \hat{\mathbf{w}}_1\|$. Since for any i , we have $\hat{\mathbf{w}}_i \in \{-\hat{\mathbf{v}}_1^i, \hat{\mathbf{v}}_1^i\}$, with the sign chosen based on which vector is closest to $\hat{\mathbf{w}}_1$, it follows that $\hat{\mathbf{w}}_i = \hat{\mathbf{v}}_1^i$ for all i . Applying Lemma 3 with $\hat{\mathbf{w}}_i = \hat{\mathbf{v}}_1^i$, we get that with probability at least $1 - p - d \exp(-\delta^2 n/cb^2)$,

$$\begin{aligned} \left\| \frac{1}{m} \sum_{i=1}^m \hat{\mathbf{w}}_i - \mathbf{v}_1 \right\| &\leq c' \left(\frac{b^2 \log(2dm/p)}{\delta^2 n} \right. \\ &\quad \left. + \sqrt{\frac{b^2 \log(2dm/p)}{\delta^2 mn}} \right). \end{aligned}$$

Squaring both sides and using the fact that $(x + y)^2 \leq 2x^2 + 2y^2$, we get that

$$\begin{aligned} \left\| \frac{1}{m} \sum_{i=1}^m \hat{\mathbf{w}}_i - \mathbf{v}_1 \right\|^2 &\leq 2(c')^2 \left(\frac{b^4 \log^2(2dm/p)}{\delta^4 n^2} \right. \\ &\quad \left. + \frac{b^2 \log(2dm/p)}{\delta^2 mn} \right). \end{aligned} \quad (18)$$

This holds with probability at least $1 - p - d \exp(-\delta^2 n / cb^2)$. To simplify things a bit, note that we can assume $d \exp(-\delta^2 n / cb^2) \leq p$ without loss of generality, since otherwise the bound in the displayed equation above is at least a constant and therefore trivially true (holds with probability 1) if we make the constant c' sufficiently large. Therefore, we can argue that (18) (with an appropriate c') holds with probability at least $1 - 2p$. Absorbing the 2 factor into the p term, slightly increasing c' appropriately, and simplifying a bit, the result finally follows from the simple observation that

$$\begin{aligned} (\mathbf{v}_1^\top \mathbf{w})^2 &= \frac{1}{2} (2 - \|\mathbf{w} - \mathbf{v}_1\|^2) \geq \\ &\frac{1}{2} \left(2 - 2 \left\| \mathbf{w} - \frac{1}{m} \sum_{i=1}^m \hat{\mathbf{w}}_i \right\|^2 - 2 \left\| \frac{1}{m} \sum_{i=1}^m \hat{\mathbf{w}}_i - \mathbf{v}_1 \right\|^2 \right) \\ &\geq 1 - 2 \left\| \frac{1}{m} \sum_{i=1}^m \hat{\mathbf{w}}_i - \mathbf{v}_1 \right\|^2, \end{aligned}$$

where the first inequality follows from the triangle inequality and the inequality $(a + b)^2 \leq 2a^2 + 2b^2$, and the second inequality follows since \mathbf{v}_1 is a unit vector, and by definition, \mathbf{w} is the unit vector closest to $\frac{1}{m} \sum_{i=1}^m \hat{\mathbf{w}}_i$. \square

A.5. Proofs of Theorem 5

The proof is a combination of the following two lemmas, each proves one of the lower bounds. We first state the two lemmas and then prove them.

Lemma 8. *For any $\delta \in (0, 1)$ and $d > 1$, there exist a distribution over vectors in \mathbb{R}^d (of norm at most 2) such that the covariance matrix has eigengap δ , and for any number of machines m and per-machine sample size n , the aggregated vector $\bar{\mathbf{v}}_1 = \frac{1}{m} \sum_{i=1}^m \hat{\mathbf{v}}_1^{(i)}$ (even after sign fixing) satisfies*

$$\mathbb{E} \left[1 - \left\langle \frac{\bar{\mathbf{v}}_1}{\|\bar{\mathbf{v}}_1\|}, \mathbf{e}_1 \right\rangle^2 \right] = \Omega \left(\min \left\{ \frac{1}{m}, \frac{1}{\delta^2 mn} \right\} \right).$$

Lemma 9. *For any $\delta \in (0, 1)$ and $d > 1$, there exist a distribution over vectors in \mathbb{R}^d (of norm at most 2) with eigengap δ in the covariance matrix, such that for any number of machines m and for per-machine sample size any n sufficiently larger than $1/\delta^2$, the aggregated vector $\bar{\mathbf{v}}_1 = \frac{1}{m} \sum_{i=1}^m \hat{\mathbf{v}}_1^{(i)}$ (even after sign fixing with the population eigenvector \mathbf{v}_1) satisfies*

$$\mathbb{E} \left[1 - \left\langle \frac{\bar{\mathbf{v}}_1}{\|\bar{\mathbf{v}}_1\|}, \mathbf{e}_1 \right\rangle^2 \right] = \Omega \left(\frac{1}{\delta^4 n^2} \right).$$

proof of Lemma 8. We will prove the result for $d = 2$ (i.e. a distribution in \mathbb{R}^2). This is without loss of generality, since we can always embed the distribution below in \mathbb{R}^d for any $d > 2$ (say, by having all coordinates other than the first two identically zero).

Consider the distribution defined by the random vector $\mathbf{x} = \sqrt{1 + \delta} \mathbf{e}_1 + \sigma \mathbf{e}_2$, where σ is uniformly distributed on $\{-1, +1\}$, and $\mathbf{e}_1 = (1, 0)$, $\mathbf{e}_2 = (0, 1)$ are the standard basis vectors. Clearly, the population covariance matrix is

$$\mathbf{X} := \mathbb{E}[\mathbf{x}\mathbf{x}^\top] = \begin{pmatrix} 1 + \delta & 0 \\ 0 & 1 \end{pmatrix},$$

with a leading eigenvector $(1, 0)$. Let us now consider the distribution of the output of a machine i . Given n samples, the empirical covariance matrix is

$$\hat{\mathbf{X}}_{(n)} = \begin{pmatrix} 1 + \delta & y_n \\ y_n & 1 \end{pmatrix}, \quad y_n := \sqrt{1 + \delta} \cdot \frac{1}{n} \sum_{i=1}^n \epsilon_i,$$

where ϵ_i are i.i.d. and uniformly distributed on $\{-1, +1\}$. Using a standard formula for the leading eigenvector of a 2×2 matrix (eig), we have that the leading eigenvector (and hence the output of any machine i) is of the form

$$\hat{\mathbf{v}}_1 = \frac{1}{\|\hat{\mathbf{u}}\|} \hat{\mathbf{u}} \quad \text{where} \quad \hat{\mathbf{u}} := \left(\frac{\delta}{2} + \sqrt{\frac{\delta^2}{4} + y_n^2}, y_n \right). \quad (19)$$

Note that with this formula, the leading eigenvector is always closer to $(1, 0)$ than $(-1, 0)$, and converges to $(1, 0)$ as $n \rightarrow \infty$. Thus, we can view the random variable $\hat{\mathbf{v}}^{(i)}$ as the output of any machine i , given n samples and after fixing the sign.

Consider now the average of m such vectors given by $\bar{\mathbf{v}} = \frac{1}{m} \sum_{i=1}^m \hat{\mathbf{v}}_1^{(i)}$. Using (19), we have that

$$\begin{aligned} \mathbb{E}[\bar{\mathbf{v}}_1(2)^2] &= \mathbb{E} \left[\left(\frac{1}{m} \sum_{i=1}^m \hat{\mathbf{v}}_2^{(i)} \right)^2 \right] = \frac{1}{m^2} \sum_{i=1}^m \mathbb{E}[(\hat{\mathbf{v}}_2^{(i)})^2] = \frac{1}{m} \mathbb{E}[(\hat{\mathbf{v}}(2))^2] \\ &= \frac{1}{m} \mathbb{E} \left[\frac{y_n^2}{\frac{\delta^2}{2} + 2y_n^2 + \delta \sqrt{\frac{\delta^2}{4} + y_n^2}} \right]. \end{aligned} \quad (20)$$

By definition of y_n and recalling that $\delta \in [0, 1]$, we have that there exist universal constants $c_1, c_2 > 0$ such that with constant probability it holds that $c_1/n \geq y_n^2 \geq c_2/n$. Using this fact and considering the two cases $1/n \geq \delta^2$ and $1/n < \delta^2$ in the RHS of Eq. (20) separately, we can see that

$$\mathbb{E}[\bar{\mathbf{v}}_1(2)^2] = \Omega \left(\frac{1}{m} \min\{1, \frac{1}{\delta^2 n}\} \right). \quad (21)$$

Using Eq. (21) we have that

$$\begin{aligned} \mathbb{E} \left[\left\langle \frac{\bar{\mathbf{v}}_1}{\|\bar{\mathbf{v}}_1\|}, \mathbf{e}_1 \right\rangle^2 \right] &= \mathbb{E} \left[\frac{\bar{\mathbf{v}}_1(1)^2}{\bar{\mathbf{v}}_1(1)^2 + \bar{\mathbf{v}}_1(2)^2} \right] = 1 - \mathbb{E} \left[\frac{\bar{\mathbf{v}}_1(2)^2}{\bar{\mathbf{v}}_1(1)^2 + \bar{\mathbf{v}}_1(2)^2} \right] \\ &\leq 1 - \mathbb{E}[\bar{\mathbf{v}}_1(2)^2] = 1 - \Omega \left(\min \left\{ \frac{1}{m}, \frac{1}{\delta^2 m n} \right\} \right), \end{aligned}$$

where the inequality follows since $\|\bar{\mathbf{v}}_1\| \leq 1$. □

proof of Lemma 9. As in Lemma 8, we prove the result for $d = 2$, however, using a different construction. Consider the defined by the random vector

$$\mathbf{x} = \sqrt{1 + \delta} \cdot \mathbf{e}_1 + \xi \cdot \mathbf{e}_2,$$

where ξ is an independent random variable defined as:

$$\xi = \begin{cases} \sqrt{2} & \text{w.p. } 1/3 \\ -1/\sqrt{2} & \text{w.p. } 2/3 \end{cases}$$

It is easy to verify that $\mathbb{E}[\xi] = 0$, $\mathbb{E}[\xi^2] = 1$, $\mathbb{E}[\xi^3] = 1/\sqrt{2}$. As we shall see, choosing ξ to be asymmetric (as opposed to ϵ in the proof of Lemma 9) will be key to our construction. Clearly, the population covariance and the empirical covariance of a sample of size n are given by we have

$$\mathbf{X} = \mathbb{E}[\mathbf{x}\mathbf{x}^\top] = \begin{pmatrix} 1 + \delta & 0 \\ 0 & 1 \end{pmatrix}, \quad \hat{\mathbf{X}}_{(n)} = \begin{pmatrix} 1 + \delta & y_n \\ y_n & z_n \end{pmatrix},$$

where

$$y_n := \sqrt{1 + \delta} \cdot \frac{1}{n} \sum_{i=1}^n \xi_i, \quad z_n := \frac{1}{n} \sum_{i=1}^n \xi_i^2,$$

with ξ_1, \dots, ξ_n being i.i.d. copies of the random variable ξ .

Clearly the leading eigenvector of \mathbf{X} is $\mathbf{e}_1 = (1, 0)$. Consider now $\hat{\mathbf{v}}_1^{(1)}, \dots, \hat{\mathbf{v}}_1^{(m)}$ to be the leading eigenvectors of m i.i.d. empirical covariance matrices of n samples, $\hat{\mathbf{X}}_{(n)}^{(1)}, \dots, \hat{\mathbf{X}}_{(n)}^{(m)}$, and let $\bar{\mathbf{v}}_1$ denote their average after sign-fixings according to the leading eigenvector of the population covariance \mathbf{e}_1 . In the following, we let \hat{v}_j^i denote the j th coordinate in the eigenvector $\hat{\mathbf{v}}_1^{(i)}$.

It holds that

$$\begin{aligned} \mathbb{E} \left[\left\langle \frac{\bar{\mathbf{v}}_1}{\|\bar{\mathbf{v}}_1\|}, \mathbf{e}_1 \right\rangle^2 \right] &= \mathbb{E} \left[\frac{\bar{\mathbf{v}}_1(1)^2}{\bar{\mathbf{v}}_1(1)^2 + \bar{\mathbf{v}}_1(2)^2} \right] = 1 - \mathbb{E} \left[\frac{\bar{\mathbf{v}}_1(2)^2}{\bar{\mathbf{v}}_1(1)^2 + \bar{\mathbf{v}}_1(2)^2} \right] \\ &\leq 1 - \mathbb{E} [\bar{\mathbf{v}}_1(2)^2] = 1 - \mathbb{E} \left[\left(\frac{1}{m} \sum_{i=1}^m \text{sign}(\hat{v}_1^i) \hat{v}_2^i \right)^2 \right] \\ &\leq 1 - \left(\frac{1}{m} \sum_{i=1}^m \mathbb{E} [\text{sign}(\hat{v}_1^i) \hat{v}_2^i] \right)^2 \\ &= 1 - (\mathbb{E}[\text{sign}(\hat{v}_1^1) \hat{v}_2^1])^2, \end{aligned} \quad (22)$$

where the first inequality follows since $\|\bar{\mathbf{v}}_1\| \leq 1$, the second inequality follows from Jensen's inequality, and the last equality follows from the fact that $\hat{\mathbf{v}}_1^{(1)}, \dots, \hat{\mathbf{v}}_1^{(m)}$ are i.i.d. random variables. From this chain of inequalities, it follows that it is enough to lower bound $(\mathbb{E}[\text{sign}(\hat{v}_1^1) \hat{v}_2^1])^2$, where $\hat{\mathbf{v}}^1$ is the leading eigenvector computed by machine 1.

Let us now consider the distribution of the leading eigenvector of the empirical covariance matrix $\hat{\mathbf{X}}_{(n)}$. Using a standard formula for the leading eigenvector of a 2×2 matrix (eig), we have that this leading eigenvector $\hat{\mathbf{v}}_1$ is proportional to

$$\left(\frac{\delta + 1 - z_n}{2} + \sqrt{\left(\frac{\delta + 1 - z_n}{2} \right)^2 + y_n^2}, y_n \right) \quad (23)$$

Assume for now that $z_n \leq 1 + c\delta$ for some positive constant c to be fixed later (note this happens with arbitrarily high probability as $n \rightarrow \infty$, as z_n converges to 1 in probability). In that case, the sign of the first coordinate in the formula above is positive, and has the same sign as the first coordinate of the leading eigenvector $\mathbf{v}_1 = (1, 0)$. Moreover, we know that $\hat{\mathbf{v}}_1^{(1)}$ must have unit norm, from which follows that

$$\text{sign}(\hat{v}_1^1) \cdot \hat{\mathbf{v}}_1^{(1)} = \frac{\left(\frac{\delta+1-z_n}{2} + \sqrt{\left(\frac{\delta+1-z_n}{2} \right)^2 + y_n^2}, y_n \right)}{\sqrt{y_n^2 + \left(\frac{\delta+1-z_n}{2} + \sqrt{\left(\frac{\delta+1-z_n}{2} \right)^2 + y_n^2} \right)^2}}. \quad (24)$$

In particular, letting $r_n = 1 - z_n$, we have that if $r_n \geq -c\delta$, then

$$\begin{aligned} \text{sign}(\hat{v}_1^1) \cdot \hat{v}_2^1 &= \frac{y_n}{\sqrt{y_n^2 + \left(\frac{\delta+r_n}{2} + \sqrt{\left(\frac{\delta+r_n}{2} \right)^2 + y_n^2} \right)^2}} \\ &= \frac{y_n}{\sqrt{y_n^2 + \left(\frac{\delta+r_n}{2} \right)^2 \left(1 + \sqrt{1 + \left(\frac{2y_n}{\delta+r_n} \right)^2} \right)^2}}. \end{aligned} \quad (25)$$

Towards using Eq. (22) to derive the lower bound, the main step is to bound the expectation of the RHS of Eq.(25) away from zero. To get an intuition why this is possible, observe that when $n \rightarrow \infty$ (in particular, when it is significantly larger than $1/\delta^2$), it holds that

$$\text{RHS of (25)} \approx \frac{y_n}{\sqrt{y_n^2 + \Theta(\delta^2)}},$$

since in this regime, with high probability, $r_n \ll \delta$ and $y_n \ll 1$. Now comes to play our choice of ξ to be an asymmetric random variable. If, just for sake of intuition, we set $n = 1$, it is easy to verify that despite the fact that $\mathbb{E}[y_n] = 0$, it holds that

$$\mathbb{E} \left[\frac{y_n}{\sqrt{y_n^2 + \Theta(\delta^2)}} \right] = \mathbb{E} \left[\frac{\xi}{\sqrt{\xi^2 + \Theta(\delta^2)}} \right] < 0.$$

Note in particular that taking ξ to be uniformly distributed on $\{-1, +1\}$, as in Lemma 8, will still give zero expectation, and hence will not work. We now formalize this intuition. We will use a Taylor expansion of the formula above, in order to bound its expectation (over y_n, r_n), from which a lower bound on $(\mathbb{E}[\text{sign}(\hat{v}_1^1) \cdot \hat{v}_2^1])^2$ would follow. To that end, define the function

$$g(t) = \frac{ty_n}{\sqrt{(ty_n)^2 + \left(\frac{\delta+tr_n}{2}\right)^2 \left(1 + \sqrt{1 + \left(\frac{2ty_n}{\delta+tr_n}\right)^2}\right)^2}}, \quad t \in [0, 1],$$

and note that $g(1)$ equals $\text{sign}(\hat{v}_1^1) \cdot \hat{v}_2^1$ as defined above. By a Taylor expansion, we have

$$\text{sign}(\hat{v}_1^1) \cdot \hat{v}_2^1 = g(1) = g(0) + g'(0) + \frac{1}{2}g''(0) + \frac{s^3}{6}g'''(s)$$

for some $s \in [0, 1]$. A tedious calculation of g 's derivatives⁵ reveals that this implies

$$\text{sign}(\hat{v}_1^1) \cdot \hat{v}_2^1 = \frac{y_n}{\delta} - \frac{r_n y_n}{\delta^2} \pm \mathcal{O} \left(\frac{|y_n|^3 + |r_n|^3}{\delta^3} \right), \quad (26)$$

assuming $\max\{|y_n|, |r_n|\} \leq c\delta$ for some constant c (hence fixing c we used in our earlier assumptions on r_n, z_n). To simplify notation, let $q_n = \text{sign}(\hat{v}_1^1) \cdot \hat{v}_2^1$, let $b_n = \frac{y_n}{\delta} - \frac{r_n y_n}{\delta^2} \pm \mathcal{O} \left(\frac{|y_n|^3 + |r_n|^3}{\delta^3} \right)$ be the expression on the right-hand side of the equation above, and let A be the event that $\max\{|y_n|, |r_n|\} \leq c\delta$ indeed holds. Also, note that with probability 1, $|q_n| \leq 1$ and $|b_n| = \mathcal{O}(1/\delta^3)$. Thus, by Eq. (26), we have that $\mathbb{E}[q_n|A] = \mathbb{E}[b_n|A]$, and therefore

$$\begin{aligned} \mathbb{E}[q_n] &= \Pr(\neg A) \cdot \mathbb{E}[q_n|\neg A] + \Pr(A) \cdot \mathbb{E}[q_n|A] \\ &= \Pr(\neg A) \cdot \mathbb{E}[q_n|\neg A] + \Pr(A) \cdot \mathbb{E}[b_n|A] \\ &= \Pr(\neg A) \cdot \mathbb{E}[q_n|\neg A] + \mathbb{E}[b_n] - \Pr(\neg A) \cdot \mathbb{E}[b_n|\neg A] \\ &= \mathbb{E}[b_n] \pm \mathcal{O}(\Pr(\neg A)/\delta^3). \end{aligned}$$

Plugging back the definitions of q_n, b_n, A , we get that

$$\mathbb{E}[\text{sign}(\hat{v}_1^1) \cdot \hat{v}_2^1] = \mathbb{E} \left[\frac{y_n}{\delta} - \frac{r_n y_n}{\delta^2} \pm \mathcal{O} \left(\frac{|y_n|^3 + |r_n|^3}{\delta^3} \right) \right] \pm \mathcal{O} \left(\frac{1}{\delta^3} \Pr(\max\{|y_n|, |r_n|\} > c\delta) \right).$$

Recalling that $y_n = \sqrt{1+\delta} \cdot \frac{1}{n} \sum_{i=1}^n \xi_i$ and $r_n = 1 - z_n = 1 - \frac{1}{n} \sum_{i=1}^n \xi_i^2$, where ξ_i are i.i.d. copies of a zero-mean, bounded random variable satisfying $\mathbb{E}[\xi^3] = 1/\sqrt{2}$, and using Hoeffding's inequality, it is easily verified that the above equals

$$0 + \sqrt{1+\delta} \frac{1}{\sqrt{2}\delta^2 n} \pm \mathcal{O} \left(\frac{1}{(\delta^2 n)^{3/2}} \right) \pm \mathcal{O} \left(\frac{1}{\delta^3} \exp(-\Omega(n\delta^2)) \right),$$

which is $\Omega\left(\frac{1}{\delta^2 n}\right)$ assuming n is sufficiently larger than $1/\delta^2$. As a result, we get that $(\mathbb{E}[\text{sign}(\hat{v}_1^1) \cdot \hat{v}_2^1])^2 = \Omega\left(\frac{1}{\delta^4 n^2}\right)$ as required. \square

B. Proofs Omitted from Section 4

B.1. Proof of Lemma 4

Proof. Let \bullet denote the standard inner product for matrices, i.e., $\mathbf{A} \bullet \mathbf{B} = \text{Tr}(\mathbf{A}\mathbf{B}^\top)$. It holds that

$$\begin{aligned} (\mathbf{w}^\top \mathbf{v}_1)^2 &= \mathbf{w}\mathbf{w}^\top \bullet \mathbf{v}_1 \mathbf{v}_1^\top \geq \hat{\mathbf{v}}_1 \hat{\mathbf{v}}_1^\top \bullet \mathbf{v}_1 \mathbf{v}_1^\top - \|\mathbf{w}\mathbf{w}^\top - \hat{\mathbf{v}}_1 \hat{\mathbf{v}}_1^\top\|_F \cdot \|\mathbf{v}_1 \mathbf{v}_1^\top\| \\ &= (\mathbf{w}^\top \mathbf{v}_1)^2 - \sqrt{2(1 - (\mathbf{w}^\top \hat{\mathbf{v}}_1)^2)} \geq (\mathbf{w}^\top \mathbf{v}_1)^2 - \sqrt{2\epsilon}. \end{aligned}$$

⁵Using MATLAB's symbolic math toolbox together with some straightforward manual calculations

□

B.2. Proof of Lemma 6

Proof. Observe that $\mathbf{C} = \mathbf{M} + (\hat{\mathbf{X}} - \hat{\mathbf{X}}_1) + \mu\mathbf{I}$. Thus, by our assumption on μ it follows that

$$\mathbf{M} + 2\mu\mathbf{I} \succeq \mathbf{C} \succeq \mathbf{M}. \quad (27)$$

Since $\tilde{F}_{\lambda, \mathbf{w}}(\mathbf{y})$ is twice differentiable, in order to bound its smoothness and strong-convexity parameters, it suffices to upper bound the largest eigenvalue and lower bound the smallest eigenvalue of its Hessian, respectively.

The Hessian of $\tilde{F}_{\lambda, \mathbf{w}}(\mathbf{y})$ is given by $\nabla^2 \tilde{F}_{\lambda, \mathbf{w}}(\mathbf{y}) = \mathbf{C}^{-1/2} \mathbf{M} \mathbf{C}^{-1/2}$.

From Eq. (27) it follows that we can write $\mathbf{M} = \mathbf{C} - \Delta$ where $\Delta \succeq 0$.

Thus we have that

$$\lambda_1(\mathbf{C}^{-1/2} \mathbf{M} \mathbf{C}^{-1/2}) = \lambda_1(\mathbf{C}^{-1/2} (\mathbf{C} - \Delta) \mathbf{C}^{-1/2}) \leq \lambda_1(\mathbf{I}) = 1, \quad (28)$$

where the inequality follows since $\mathbf{C}^{-1/2} \Delta \mathbf{C}^{-1/2}$ is positive semidefinite.

Since \mathbf{M}, \mathbf{C} are invertible and positive definite, Eq. (27) implies that

$$\mathbf{M}^{-1} \succeq \mathbf{C}^{-1} \succeq (\mathbf{M} + 2\mu\mathbf{I})^{-1}. \quad (29)$$

Thus we have that

$$\begin{aligned} \lambda_d(\mathbf{C}^{-1/2} \mathbf{M} \mathbf{C}^{-1/2}) &= \lambda_d(\mathbf{M}^{1/2} \mathbf{C}^{-1/2} \mathbf{C}^{-1/2} \mathbf{M} \mathbf{C}^{-1/2} \mathbf{C}^{1/2} \mathbf{M}^{-1/2}) = \lambda_d(\mathbf{M}^{1/2} \mathbf{C}^{-1} \mathbf{M}^{1/2}) \\ &\geq \lambda_d(\mathbf{M}^{1/2} (\mathbf{M} + 2\mu\mathbf{I})^{-1} \mathbf{M}^{1/2}) = \min_{i \in [d]} \left\{ \frac{\lambda_i(\mathbf{M})}{\lambda_i(\mathbf{M}) + 2\mu} \right\} \\ &= \frac{\lambda_d(\mathbf{M})}{\lambda_d(\mathbf{M}) + 2\mu} = \frac{\lambda - \hat{\lambda}_1}{(\lambda - \hat{\lambda}_1) + 2\mu}, \end{aligned} \quad (30)$$

where the first equality follows from matrix similarity and the fact that \mathbf{M}, \mathbf{C} are invertible, and the first inequality follows from Eq. (29).

To prove the second part of the lemma we observe that

$$\begin{aligned} \|\tilde{\mathbf{z}} - \mathbf{M}^{-1} \mathbf{w}\| &= \|\mathbf{C}^{-1/2} \tilde{\mathbf{y}} - \mathbf{C}^{-1/2} \mathbf{C}^{1/2} \mathbf{M}^{-1} \mathbf{w}\| \leq \|\mathbf{C}^{-1/2}\| \cdot \|\tilde{\mathbf{y}} - \mathbf{C}^{1/2} \mathbf{M}^{-1} \mathbf{w}\| \\ &\leq \frac{1}{\sqrt{\lambda - \lambda_1(\hat{\mathbf{X}})}} \|\tilde{\mathbf{y}} - \mathbf{C}^{1/2} \mathbf{M}^{-1} \mathbf{w}\|, \end{aligned}$$

where the second inequality follows from Eq. (29).

Finally, the last part of the lemma follows from a direct application of Theorem 1 to upper bound $\|\mathbf{X} - \hat{\mathbf{X}}_1\|$. □

B.3. Proof of Lemma 7

Proof. Let $\mathbf{z}^* := (\lambda\mathbf{I} - \hat{\mathbf{X}})^{-1} \mathbf{w}$, $\mathbf{y}^* := \mathbf{C}^{1/2} (\lambda\mathbf{I} - \hat{\mathbf{X}})^{-1} \mathbf{w}$, and recall that \mathbf{z}^* and \mathbf{y}^* are the global minimizers of $F_{\lambda, \mathbf{w}}(\mathbf{z})$ and $\tilde{F}_{\lambda, \mathbf{w}}(\mathbf{y})$, respectively. Using the results of Lemma 6 we have that

$$\|\tilde{\mathbf{z}} - \mathbf{z}^*\| \leq (\lambda - \hat{\lambda}_1)^{-1/2} \|\tilde{\mathbf{y}} - \mathbf{y}^*\| \leq (\lambda - \hat{\lambda}_1)^{-1/2} \sqrt{2 \left(1 + \frac{2\mu}{\lambda - \hat{\lambda}_1} \right)} \epsilon',$$

where the second inequality follows from the strong-convexity of $\tilde{F}_{\lambda, \mathbf{w}}(\mathbf{y})$. Thus, it suffices to set ϵ' as stated in the lemma in order to obtain the approximation guarantee for $\tilde{\mathbf{z}}$.

To upper-bound the total number of communication rounds required to obtain $\tilde{\mathbf{y}}$ with the guarantee prescribed in the lemma, we note that both the conjugate gradient method and Nesterov's accelerated gradient method require

$$O\left(\sqrt{\frac{\beta}{\alpha}} \ln(\|\mathbf{y}^*\|/\epsilon')\right) \quad (31)$$

calls to the first-order oracle of $\tilde{F}_{\lambda, \mathbf{w}}(\mathbf{y})$ to obtain $\tilde{\mathbf{y}}$ satisfying $\tilde{F}_{\lambda, \mathbf{w}}(\tilde{\mathbf{y}}) - \min_{\mathbf{y} \in \mathbb{R}^d} \tilde{F}_{\lambda, \mathbf{w}}(\mathbf{y}) \leq \epsilon'$, where α and β are the strong-convexity and smoothness parameters of $\tilde{F}_{\lambda, \mathbf{w}}$, respectively, and assuming w.l.o.g. that the initial iterate is $\mathbf{y}_0 = \mathbf{0}$. Thus, by our construction of a distributed first-order oracle given in Algorithm 2, we have that the total number of communication rounds is upper bounded by (31). The lemma now follows from noticing that by Lemma 6 we have that $\beta/\alpha = 1 + \frac{2\mu}{\lambda - \hat{\lambda}_1}$ and that

$$\|\mathbf{y}^*\| = \|\mathbf{C}^{1/2}(\lambda \mathbf{I} - \hat{\mathbf{X}}_1)\mathbf{w}\| \leq \lambda_1(\mathbf{C}^{1/2})(\lambda - \hat{\lambda}_1)^{-1}\|\mathbf{w}\| = O\left(\|\mathbf{w}\|/(\lambda - \hat{\lambda}_1)\right).$$

□

B.4. Proof of Theorem 6

Proof. Under our assumption that $mn = \Omega(\delta^{-2} \ln(d/p))$, the following three events all hold with probability at least $1 - p$ (each of which holds w.p. at least $1 - p/3$):

1. the output \mathbf{w}_f satisfies $(\mathbf{w}_f^\top \hat{\mathbf{v}}_1)^2 \geq 1 - \epsilon$ (holds w.p. $1 - p/3$ by applying Lemma 5 with our choice of parameters)
2. $\hat{\delta} = \Theta(\delta)$ (by applying Theorem 1)
3. $\|\hat{\mathbf{X}} - \hat{\mathbf{X}}_1\| \leq \mu$, where μ is as prescribed in the Theorem (by applying Theorem 1)

The approximation guarantee of \mathbf{w}_f follows directly from Lemma 5. It thus remains to upper-bound the number of matrix-vector products. Thus, combining Lemmas 5 and 7 we have that when using either the conjugate gradient method or Nesterov's accelerated method to approximately solve the linear systems in Algorithm 1, as prescribed in Lemma 7, the total number of distributed matrix-vector products with $\hat{\mathbf{X}}$ is:

$$\begin{aligned} & O\left(\ln\left(\frac{d}{p\epsilon}\right) \cdot \left(\sqrt{1 + \frac{2\mu}{\delta}} \left(\ln \delta^{-1} \ln\left(\frac{d}{p\epsilon}\right) + \ln\left(\frac{(1 + 2\mu/\delta)}{\delta \bar{\epsilon}}\right)\right)\right)\right) = \\ & O\left(\sqrt{1 + \frac{2\mu}{\delta}} \left(\ln \delta^{-1} \ln^2\left(\frac{d}{p\epsilon}\right) + \ln\left(\frac{d}{p\epsilon}\right) \left(\ln\left(\frac{(1 + 2\mu/\delta)}{\delta}\right) + \ln\left(\frac{1}{\bar{\epsilon}}\right)\right)\right)\right) = \\ & O\left(\sqrt{1 + \frac{2\mu}{\delta}} \left(\ln \delta^{-1} \ln^2\left(\frac{d}{p\epsilon}\right) + \ln\left(\frac{d}{p\epsilon}\right) \ln\left(\frac{(1 + 2\mu/\delta)}{\delta}\right) + \ln^2\left(\frac{d}{p\epsilon}\right) \ln\left(\frac{1}{\bar{\delta}}\right)\right)\right), \end{aligned}$$

where the first term in the $O(\cdot)$ in the first row accounts for the total number of instances of $F_{\lambda, \mathbf{w}}(\mathbf{z})$ needs to be solved, given by the bound in Lemma 5, and the second term in the first row accounts for the communication-complexity of solving each such instance according to Lemma 7. Additionally, we have used Lemma 5 to lower bound $\lambda - \hat{\lambda}_1 = \Omega(\hat{\delta})$, and $\bar{\epsilon}(\epsilon)$ is as prescribed in Algorithm 1. Finally, we have upper-bounded $\ln(\|\mathbf{w}\|)$, in all instances of $F_{\lambda, \mathbf{w}}(\mathbf{z})$ solved throughout the run of the algorithm, by noticing that in all of them it holds that

$$\ln(\|\mathbf{w}\|) = O\left(\ln\left(\lambda_{(s)} - \hat{\lambda}_1\right)^{-\max\{m_1, m_2\}}\right) = O\left(\ln \delta^{-1} \ln\left(\frac{d}{p\epsilon}\right)\right),$$

where m_1, m_2 are as prescribed in Algorithm 1, and we have used Lemma 5 again to lower bound $\lambda_{(s)} - \hat{\lambda}_1 = \Omega(\delta)$.

Finally, using Lemma 6, we can set $\mu = \frac{4\sqrt{\ln(3d/p)}}{\sqrt{n}}$. Thus, the overall number of communication rounds is upper-bound by

$$O\left(\sqrt{\frac{\sqrt{\ln(d/p)}}{\delta \sqrt{n}}} \left(\ln\left(\frac{d}{p\epsilon^2}\right) \ln\left(\frac{\sqrt{\ln(d/p)}}{\delta^2 \sqrt{n}}\right) + \ln^2\left(\frac{d}{p\epsilon^2}\right) \ln\left(\frac{1}{\bar{\delta}}\right)\right)\right).$$

C. Additional Experimental Results

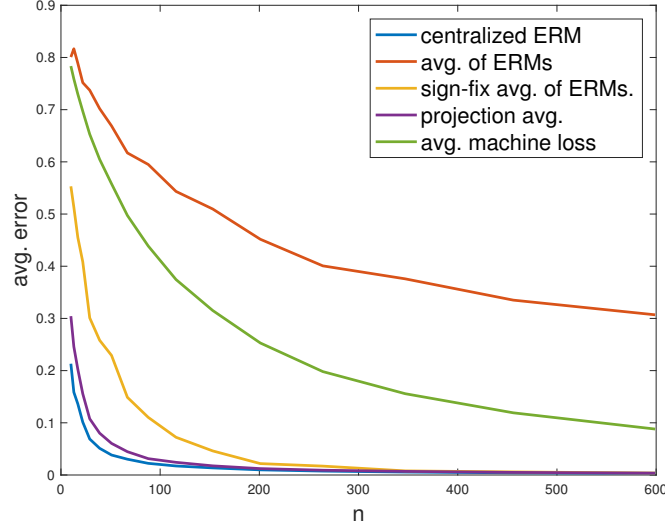


Figure 2. Estimation error vs. the per-machine sample size n for uniform sampling-based distribution.

D. Proof of the Davis-Kahan $\sin\theta$ Theorem

We prove Theorem 2 in greater generality. In particular, Theorem 2 follows from setting $k = 1$ in the next theorem.

Theorem 7 (Davis-Kahan $\sin\theta$ theorem). *Let \mathbf{X}, \mathbf{Y} be symmetric real $d \times d$ matrices and fix $k \in [d]$. Let $\mathbf{V}_\mathbf{X}$ and $\mathbf{V}_\mathbf{Y}$ denote $d \times k$ matrix whose columns are the top k eigenvectors of \mathbf{X} and the matrix whose columns are the top k eigenvectors of \mathbf{Y} , respectively. Also, suppose that $\delta_k(\mathbf{X}) := \lambda_k(\mathbf{X}) - \lambda_{k+1}(\mathbf{X}) > 0$. Then it holds that*

$$\|\mathbf{V}_\mathbf{X}\mathbf{V}_\mathbf{X}^\top - \mathbf{V}_\mathbf{Y}\mathbf{V}_\mathbf{Y}^\top\|_F \leq 2 \frac{\|\mathbf{X} - \mathbf{Y}\|}{\delta_k(\mathbf{X})}.$$

Proof. Throughout the proof we denote the projection matrices:

$$\mathbf{P}_\mathbf{X} := \mathbf{V}_\mathbf{X}\mathbf{V}_\mathbf{X}^\top, \mathbf{P}_\mathbf{X}^\perp := \mathbf{I} - \mathbf{V}_\mathbf{X}\mathbf{V}_\mathbf{X}^\top, \mathbf{P}_\mathbf{Y} := \mathbf{V}_\mathbf{Y}\mathbf{V}_\mathbf{Y}^\top, \mathbf{P}_\mathbf{Y}^\perp := \mathbf{I} - \mathbf{V}_\mathbf{Y}\mathbf{V}_\mathbf{Y}^\top,$$

i.e., $\mathbf{P}_\mathbf{X}$ is the projection matrix onto the top k eigenvectors of \mathbf{X} and $\mathbf{P}_\mathbf{X}^\perp$ is the projection matrix onto the lower $d - k$ eigenvectors, and same goes for $\mathbf{P}_\mathbf{Y}, \mathbf{P}_\mathbf{Y}^\perp$. We also let $\mathbf{A} \bullet \mathbf{B}$ denote the standard inner products between matrices \mathbf{A}, \mathbf{B} .

We can write $\mathbf{P}_\mathbf{Y}$ as

$$\mathbf{P}_\mathbf{Y} = \mathbf{P}_\mathbf{X}\mathbf{P}_\mathbf{Y}\mathbf{P}_\mathbf{X} + \mathbf{P}_\mathbf{X}^\perp\mathbf{P}_\mathbf{Y}\mathbf{P}_\mathbf{X} + \mathbf{P}_\mathbf{X}\mathbf{P}_\mathbf{Y}\mathbf{P}_\mathbf{X}^\perp + \mathbf{P}_\mathbf{X}^\perp\mathbf{P}_\mathbf{Y}\mathbf{P}_\mathbf{X}^\perp. \quad (32)$$

Observe that

$$\mathbf{P}_\mathbf{X}\mathbf{P}_\mathbf{Y}\mathbf{P}_\mathbf{X}^\perp \bullet \mathbf{X} = \text{Tr}(\mathbf{P}_\mathbf{X}\mathbf{P}_\mathbf{Y}\mathbf{P}_\mathbf{X}^\perp \mathbf{X}) = \text{Tr}(\mathbf{P}_\mathbf{Y}\mathbf{P}_\mathbf{X}^\perp \mathbf{X} \mathbf{P}_\mathbf{X}) = 0, \quad (33)$$

where the second equality follows from the cyclic property of the trace, and the last equality follows since $\mathbf{P}_\mathbf{X}^\perp \mathbf{X} \mathbf{P}_\mathbf{X} = \mathbf{0}_{d \times d}$. Using Eq. (32) and (33) we have that

$$\begin{aligned} \mathbf{P}_\mathbf{Y} \bullet \mathbf{X} &= \mathbf{P}_\mathbf{X}\mathbf{P}_\mathbf{Y}\mathbf{P}_\mathbf{X} \bullet \mathbf{X} + \mathbf{P}_\mathbf{X}^\perp\mathbf{P}_\mathbf{Y}\mathbf{P}_\mathbf{X}^\perp \bullet \mathbf{X} = \text{Tr}(\mathbf{P}_\mathbf{X}\mathbf{P}_\mathbf{Y}\mathbf{P}_\mathbf{X} \mathbf{X}) + \text{Tr}(\mathbf{P}_\mathbf{X}^\perp\mathbf{P}_\mathbf{Y}\mathbf{P}_\mathbf{X}^\perp \mathbf{X}) \\ &= \text{Tr}(\mathbf{P}_\mathbf{Y}\mathbf{P}_\mathbf{X} \mathbf{X}) + \text{Tr}(\mathbf{P}_\mathbf{X}^\perp\mathbf{P}_\mathbf{Y}\mathbf{P}_\mathbf{X}^\perp \mathbf{X}) \leq \text{Tr}(\mathbf{P}_\mathbf{Y}\mathbf{P}_\mathbf{X} \mathbf{X}) + \text{Tr}(\mathbf{P}_\mathbf{X}^\perp\mathbf{P}_\mathbf{Y}\mathbf{P}_\mathbf{X}^\perp) \cdot \lambda_1(\mathbf{P}_\mathbf{X}^\perp \mathbf{X}) \\ &= \text{Tr}(\mathbf{P}_\mathbf{Y}\mathbf{P}_\mathbf{X} \mathbf{X}) + \lambda_{k+1}(\mathbf{X}) \cdot \text{Tr}(\mathbf{P}_\mathbf{X}^\perp\mathbf{P}_\mathbf{Y}), \end{aligned} \quad (34)$$

where the inequality follows since for any two positive semidefinite matrices \mathbf{A}, \mathbf{B} it holds that $\text{Tr}(\mathbf{AB}) \leq \text{Tr}(\mathbf{A}) \cdot \lambda_1(\mathbf{B})$ and the fact that $\mathbf{P}_{\bar{\mathbf{X}}}^\perp \mathbf{X}$ is positive semidefinite. The last equality follows since $\lambda_1(\mathbf{P}_{\bar{\mathbf{X}}}^\perp \mathbf{X}) = \lambda_{k+1}(\mathbf{X})$. It further holds that

$$\mathbf{P}_Y \bullet \mathbf{Y} \geq \mathbf{P}_X \bullet \mathbf{Y} = \text{Tr}(\mathbf{P}_X \mathbf{X}) + \mathbf{P}_X \bullet (\mathbf{Y} - \mathbf{X}). \quad (35)$$

Subtracting Eq. (35) from Eq. (34) we have that

$$\text{Tr}(\mathbf{P}_Y \mathbf{P}_X \mathbf{X}) + \lambda_{k+1}(\mathbf{X}) \cdot \text{Tr}(\mathbf{P}_{\bar{\mathbf{X}}}^\perp \mathbf{P}_Y) - \text{Tr}(\mathbf{P}_X \mathbf{X}) - \mathbf{P}_X \bullet (\mathbf{Y} - \mathbf{X}) \geq \mathbf{P}_Y \bullet \mathbf{X} - \mathbf{P}_Y \bullet \mathbf{Y}.$$

Rearranging we have that

$$\begin{aligned} \text{Tr}((\mathbf{I} - \mathbf{P}_Y) \mathbf{P}_X \mathbf{X}) - \lambda_{k+1}(\mathbf{X}) \cdot \text{Tr}(\mathbf{P}_{\bar{\mathbf{X}}}^\perp \mathbf{P}_Y) &\leq (\mathbf{Y} - \mathbf{X}) \bullet (\mathbf{P}_Y - \mathbf{P}_X) \\ &\leq \|\mathbf{X} - \mathbf{Y}\| \cdot \|\mathbf{P}_X - \mathbf{P}_Y\|_F. \end{aligned} \quad (36)$$

It holds that

$$\begin{aligned} \text{Tr}((\mathbf{I} - \mathbf{P}_Y) \mathbf{P}_X \mathbf{X}) &= \text{Tr}(\mathbf{P}_X (\mathbf{I} - \mathbf{P}_Y) \mathbf{P}_X \mathbf{P}_X \mathbf{X}) \\ &\geq \text{Tr}(\mathbf{P}_X (\mathbf{I} - \mathbf{P}_Y) \mathbf{P}_X) \cdot \lambda_k(\mathbf{P}_X \mathbf{X}) \\ &= \text{Tr}(\mathbf{P}_X - \mathbf{P}_Y \mathbf{P}_X) \cdot \lambda_k(\mathbf{X}) \\ &= (k - \mathbf{P}_X \bullet \mathbf{P}_Y) \cdot \lambda_k(\mathbf{X}) \\ &= \frac{\lambda_k(\mathbf{X})}{2} \|\mathbf{P}_X - \mathbf{P}_Y\|_F^2. \end{aligned} \quad (37)$$

Furthermore, it holds that

$$\text{Tr}(\mathbf{P}_{\bar{\mathbf{X}}}^\perp \mathbf{P}_Y) = \text{Tr}((\mathbf{I} - \mathbf{P}_X) \mathbf{P}_Y) = k - \mathbf{P}_X \bullet \mathbf{P}_Y = \frac{1}{2} \|\mathbf{P}_X - \mathbf{P}_Y\|_F^2. \quad (38)$$

Plugging Eq. (37) and (38) into Eq. (36), we have that

$$\frac{1}{2} \|\mathbf{P}_X - \mathbf{P}_Y\|_F^2 \cdot (\lambda_k(\mathbf{X}) - \lambda_{k+1}(\mathbf{X})) \leq \|\mathbf{X} - \mathbf{Y}\| \cdot \|\mathbf{P}_X - \mathbf{P}_Y\|_F, \quad (39)$$

which completes the proof. \square