Optimal Minimization of the Covariance Loss

Vishesh Jain, Ashwin Sah, and Mehtaab Sawhney

Abstract—Let $X$ be a random vector valued in $\mathbb{R}^m$ such that $\|X\|_2 \leq 1$ almost surely. For every $k \geq 3$, we show that there exists a sigma algebra $F$ generated by a partition of $\mathbb{R}^m$ into $k$ sets such that $\| \text{Cov}(X) - \text{Cov}(E[X \mid F]) \|_F \leq \frac{1}{\sqrt{k}}$. This is optimal up to the implicit constant and improves on a previous bound due to Boedihardjo, Strohmer, and Vershynin. Our proof provides an efficient algorithm for constructing $F$ and leads to improved accuracy guarantees for $k$-anonymous or differentially private synthetic data. We also establish a connection between the above problem of minimizing the covariance loss and the pinning lemma from statistical physics, providing an alternate (and much simpler) algorithmic proof in the important case when $X \in \{\pm 1\}^m / \sqrt{m}$ almost surely.

Index Terms—Covariance loss, pinning, randomized rounding, synthetic data, differential privacy.

I. INTRODUCTION

Let $X$ be a random vector valued in $\mathbb{R}^m$. By slightly abusing notation, we identify $X$ with its law, which is a probability measure on $(\mathbb{R}^m, \mathcal{G})$, where $\mathcal{G}$ is a sigma-algebra on $\mathbb{R}^m$. Let $F$ be a sigma sub-algebra of $\mathcal{G}$ and let $Y = E[X \mid F]$ denote the corresponding conditional expectation. In particular, $E[X] = E[Y]$. Let

$$\Sigma_X := E[(X - E[X])(X - E[X])^T]$$

denote the covariance matrix of $X$ and let $\Sigma_Y$ denote the covariance matrix of $Y$. When $m = 1$, $\Sigma_X$ is precisely the variance of $X$, which we denote by $\text{Var}(X)$, and similarly for $\Sigma_Y$. The familiar law of total variance asserts that

$$\text{Var}(X) - \text{Var}(Y) = E(X - Y)^2 \geq 0,$$

so that taking a conditional expectation results in a loss of variance. This phenomenon extends to higher dimensions as the law of total covariance:

$$\Sigma_X - \Sigma_Y = E(X - Y)(X - Y)^T \succeq 0,$$

where $\succeq$ denotes the usual Loewner order on positive semi-definite matrices.

Recently, motivated by the design of privacy-preserving synthetic data (see the discussion in Section I-A), Boedihardjo, Strohmer, and Vershynin [1] asked the following fundamental question: how much covariance is lost upon taking a conditional expectation? The answer to this clearly depends on how much covariance is lost upon taking a conditional expectation with respect to a sigma sub-algebra $F$ with a given complexity. Moreover, for applications, one would like to be able to find the best possible (at least asymptotically) sigma sub-algebra with a given complexity in an efficient manner.

Since every finitely generated sigma-algebra $F$ may be viewed as the sigma-algebra generated by a partition of $\mathbb{R}^m$ into $k$ sets (for some finite $k$), a natural and useful measure of complexity of $F$ is the number of sets in the underlying partition, $k$. With this notion of complexity, and measuring covariance loss in the Frobenius norm, Boedihardjo, Strohmer, and Vershynin [1, Th. 1.2] showed that there exists an absolute constant $C > 0$ such that for any random vector $X$ valued in $\mathbb{R}^m$ for which $\|X\|_2 \leq 1$ almost surely, and for every $k \geq 3$, there exists a partition of $\mathbb{R}^m$ into at most $k$ sets such that for the sigma-algebra $F$ generated by this partition, $Y = E[X \mid F]$ satisfies the dimension-independent bound

$$\|\Sigma_X - \Sigma_Y\|_F \leq C \frac{\sqrt{\log \log k}}{\log k},$$

(2)

where for $A \in \mathbb{R}^{m \times m}$, $\|A\|_F = \sqrt{\sum_{i,j} A_{ij}^2}$ denotes its Frobenius norm. They noted [1, Proposition 3.14] that the upper bound is optimal up to the factor of $\sqrt{\log \log k}$.

To see the strength of the dimension-independence of the bound in (2), consider the case when $X$ is the uniform distribution over $x_1, \ldots, x_n \in \mathbb{R}^m$ with $\max_{i} \|x_i\|_2 \leq 1$, and let $\mathcal{F}_k$ denote the collection of sigma-algebras of $\mathbb{R}^m$ generated by a partition of $\mathbb{R}^m$ into at most $k$ parts. Using (1) and Jensen’s inequality,

$$\inf_{F \in \mathcal{F}_k} \|\Sigma_X - \Sigma_{E[X \mid F]}\|_F \leq \inf_{F \in \mathcal{F}_k} \mathbb{E}(\|X - E[X \mid F]\|_F)(X - E[X \mid F])^T \|_F$$

$$= \inf_{y_1, \ldots, y_k \in \mathbb{R}^m: I_1 \cup \cdots \cup I_k = [n]} \sum_{i=1}^k \sum_{j \in I_i} \|x_j - y_i\|_2.$$

The last quantity is simply (a variation of) the $k$-means objective, and can decay as slowly as $\Omega(k^{1-1/m})$, which is...
significant worse in the high-dimensional regime of interest.

As our main result, we remove the gap between the upper bound in Theorem 1 and the lower bound in [1, Proposition 3.14], thereby obtaining an optimal and algorithmic answer to the problem of minimizing covariance loss raised by Boedihardjo, Strohmer, and Vershynin.

Theorem 1: Let $X$ be a random vector valued in $\mathbb{R}^m$ which satisfies $\|X\|_2 \leq 1$ almost surely. Then for every $k \geq 3$, there exists a partition of $\mathbb{R}^m$ into at most $k$ sets such that for the associated $\sigma$-algebra $\mathcal{F}$, the conditional expectation $Y = \mathbb{E}[X | \mathcal{F}]$ satisfies

$$\|\Sigma_X - \Sigma_Y\|_F \leq \frac{C}{\sqrt{\log k}},$$

where $C$ is an absolute constant.

As noted earlier, our bound is optimal up to the value of the absolute constant $C$. We prove Theorem 1 in Section III. Before doing so, in Section II, we provide a completely different proof of Theorem 1 in the case when $X \in \sqrt{m} \cdot \{\pm 1\}^m$ based on the pinning lemma from statistical physics; this case is especially important for applications, since it corresponds to the case of Boolean ‘true’ data in the setting of Section I-A. The proof in Section II is much simpler than the general proof in Section III and provides a significantly faster and simpler algorithm for finding $\mathcal{F}$.

Remark 1: By following exactly the same procedure as in [1, Sec. 3.6], if the probability space has no atoms, then the partition can be made with exactly $k$ sets, all of which have the same probability $1/k$.

Remark 2: By combining Theorem 1 with the tensorization principle [1, Th. 3.10], we immediately obtain an analog of Theorem 1 for higher moments, which improves [1, Corollary 3.12] by a factor of $\sqrt{\log k}$: for all $d \geq 2$,

$$\|\mathbb{E}X^{\otimes d} - \mathbb{E}Y^{\otimes d}\|_F \leq 4^d \cdot \frac{C}{\sqrt{\log k}},$$

where $C$ is the absolute constant appearing in Theorem 1. Here, $X^{\otimes d} \in \mathbb{R}^{m \times m \times \cdots \times m}$ is defined by $X^{\otimes d}(i_1, \ldots, i_d) := X(i_1) \cdots X(i_d)$, where $i_1, \ldots, i_d \in [m]$ (and similarly for $Y^{\otimes d}$), and for $A \in \mathbb{R}^{m 	imes \cdots \times m}$, $\|A\|_F := \sqrt{\sum_{1 \leq i_1, \ldots, i_d \leq m} A(i_1, \ldots, i_d)^2}$.

A. Applications to the Design of Privacy-Preserving Synthetic Data

As mentioned earlier, the problem of minimizing covariance loss was studied in [1] with a view towards designing privacy-preserving synthetic data. Here, one is given ‘true’ data points $x_1, \ldots, x_n \in \mathbb{R}^m$ and would like to construct a map $A : \{x_1, \ldots, x_n\} \to \mathbb{R}^m$ such that the set of ‘synthetic’ data $\{A(x_1), \ldots, A(x_n)\}$ is both ‘private’ and ‘accurate’. We refer the reader to [1] for a much more detailed discussion of these notions and further references, limiting ourselves here to the most basic application of Theorem 1.

A popular notion of preserving privacy is $k$-anonymity [2]; for synthetic data, this is the requirement that for any $y \in \{A(x_1), \ldots, A(x_n)\}$, the preimage $A^{-1}(y)$ has cardinality at least $k$. In words, the true data is transformed into synthetic data in such a manner that the information of each person in the dataset cannot be distinguished from that of at least $k - 1$ other individuals in the dataset.

Let us quickly discuss how Theorem 1 may be used to obtain accurate $[n/k]$-anonymous synthetic data. Given true data $x_1, \ldots, x_n \in \mathbb{R}^m$, we consider the random vector $X$ which takes on each value $x_i$ with probability $1/n$ each. Given $k \geq 3$, Theorem 1 gives a partition of $\mathbb{R}^m$ into $k$ sets, which induces a partition $\mathbb{R}^m$ into $k$ sets, respectively.

To quantify this, we consider the expected covariance loss of synthetic data as

$$\mathbb{E}(X - Y)^2 = \mathbb{E}(X - \mathbb{E}[X | \mathcal{F}])^2 = \mathbb{E} \Sigma_X^2 - \mathbb{E} \Sigma_Y^2,$$

where $\Sigma_X$ and $\Sigma_Y$ are the covariance matrices of $X$ and synthetic data $Y$, respectively. Using Theorem 1, we can bound this as

$$\|\Sigma_X - \Sigma_Y\|_F \leq \frac{C}{\sqrt{\log k}}.$$

This means that the synthetic data is accurate in the sense that it approximately preserves, on average, the second order marginals of the true data. This can be extended to higher-order marginals using (3).

The above idea is adapted in [1] to extract additional guarantees for anonymous, synthetic data (see [1, Ths. 4.4, 4.6]). In both cases, replacing (2) with our Theorem 1 leads to quantitative improvements by a factor of $\log \log k$.

Finally, we remark that in [1, Ths. 5.9-5.11], a generalization of (2) is used with additional arguments to design differentially-private synthetic data. Our proof of Theorem 1 in Section III can also be generalized using similar arguments as in [1] to yield versions of [1, Ths. 5.9-5.11] without the $\log \log n$ factor there; we leave the details to the interested reader.

II. PROOF OF THEOREM 1 FOR BOOLEAN DATA

In this section, we provide a proof of Theorem 1 in the case when $X$ is valued in $\{\pm 1\}^m/\sqrt{m}$ almost surely. In the setting of Section I-A, this corresponds to the case when the true data is Boolean and hence is particularly relevant for applications. Our proof relies on the so-called pinning lemma from statistical physics, discovered independently by Montanari [3] and by Raghavendra and Tan [4]. The statement below follows by combining [4, Lemma 4.5] with Pinsker’s inequality (cf. the proofs of [5, Lemmas 4.2, A.2]).
Lemma 2: Let \( X_1, \ldots, X_m \) be a collection of \( \{ \pm 1 \} \)-valued random variables. Then, for any \( \ell \in [m] \), we have that

\[
\mathbb{E}_{t \sim \{ 0, \ldots, \ell \}} \mathbb{E}_{S \sim \binom{[m]}{\ell}} \left[ \mathbb{E}_{S} \left( \sum_{i \neq j \in [m]} \text{Cov}(X_i, X_j \mid X_S)^2 \right) \right] \leq \frac{8m^2 \log 2}{\ell}.
\]

Roughly speaking, the intuition behind the pinning lemma is the following: either the average (pairwise) covariance between the random variables \( X_1, \ldots, X_m \) is already small (in which case, we’re done) or the average covariance is not small. In the latter case, we expect a random coordinate \( X_i \) to contain substantial information about many of the other coordinates \( X_1, \ldots, X_m \), so that conditioning on a small random subset of the coordinates makes the average conditional covariance sufficiently small.

Given Lemma 2, we can quickly deduce Theorem 1 for Boolean data.

Proof: [Proof of Theorem 1 for Boolean data] Recall that \( X \) is valued in \( \{ \pm 1 \}^m / \sqrt{m} \) almost surely. Note that we may assume that \( m \geq \log_2 k \); otherwise \( X \) takes on at most \( 2^m \leq k \) values, so that the sigma algebra \( \mathcal{F} \) generated by the partition of \( \{ \pm 1 \}^m / \sqrt{m} \) which assigns each point to its own part has at most \( k \) parts and satisfies \( \mathcal{Y} := \mathbb{E}[X \mid \mathcal{F}] = X \).

Now, let \( t \) be chosen uniformly from \( \{ 0, 1, \ldots, \log_2 k \} \) and let \( S \) be chosen uniformly from \( \binom{[m]}{t} \). This provides a decomposition of \( \{ \pm 1 \}^m / \sqrt{m} \) into at most \( 2^t \leq k \) clusters, where each cluster consists of all points of \( \{ \pm 1 \}^m / \sqrt{m} \) which agree on the coordinates in \( S \). In other words, each cluster corresponds to a setting of \( X_S := (X_i)_{i \in S} \in \{ \pm 1 \}^S / \sqrt{m} \). Let \( \mathcal{F} \) denote the sigma algebra generated by these clusters and let \( Y = \mathbb{E}[X \mid \mathcal{F}] = \mathbb{E}[X \mid X_S] \). Let \( \Sigma_X \) and \( \Sigma_Y \) denote the covariance matrices of \( X \) and \( Y \) respectively. Then,

\[
\mathbb{E}_S \| \Sigma_X - \Sigma_Y \|_F \leq \mathbb{E}_S \mathbb{E}_{X_S} \left( \mathbb{E}_{X \mid X_S} (X - \mathbb{E}[X \mid X_S]) (X - \mathbb{E}[X \mid X_S])^T \right) \|_F \leq \mathbb{E}_S \mathbb{E}_{X_S} \left( \sum_{i \neq j \in [m]} \text{Cov}(X_i, X_j \mid X_S)^2 + \sum_{i \in [m]} \text{Var}(X_i \mid X_S)^2 \right) \leq \frac{8m^2 \log 2}{\log_2 k}, \frac{1}{m^2} + \frac{1}{m^2} \leq \frac{3}{\log_2 k}.
\]

The second line follows from (1), the third line follows from norm convexity, the fifth line follows from Jensen’s inequality, the first term in the sixth line follows by applying Lemma 2 with \( \ell = \log_2 k \) and rescaling by a factor of \( m^{-2} \) (since each \( X_i \) is valued in \( \{ \pm 1 \} / \sqrt{m} \)) and the second term in the sixth line follows by noting that \( \text{Var}(X_i \mid X_S) \leq 1/m \) (again, since \( X_i \in \{ \pm 1 \} / \sqrt{m} \)).

Finally, by Markov’s inequality,

\[
\mathbb{P}_S \left[ \| \Sigma_X - \Sigma_Y \|_F \geq \frac{9}{\sqrt{\log_2 k}} \right] \leq \frac{1}{3},
\]

so we have a very simple randomized algorithm for finding (with probability at least 2/3) a sigma algebra \( \mathcal{F} \) obtaining the desired guarantee: first choose \( t \) uniformly from \( \{ 0, 1, \ldots, \log_2 k \} \), then choose \( S \) uniformly from \( \binom{[m]}{t} \), and finally decompose \( \{ \pm 1 \}^m / \sqrt{m} \) based on the values of the coordinates in \( S \).

III. PROOF OF THEOREM 1

In this section, we prove Theorem 1 for general random vectors \( X \in \mathbb{R}^m \) satisfying \( \|X\|_2 \leq 1 \) almost surely. As in [1], we use principal component analysis to reduce to the case where \( m = c \log k \), for a sufficiently small absolute constant \( c > 0 \). However, our treatment of the dimension-reduced problem is rather different from [1]. Indeed, whereas [1] partitions the dimension-reduced random vector according to the closest point in a volumetric epsilon-net (thereby, only exploiting the information that \( \|X\|_2 \leq 1 \) almost surely), our clustering scheme also takes into account the distributional profile of the dimension-reduced random vector; briefly, we place each ‘heavy’ point into its own cluster, place nearby points, which are ‘collectively light’ into a single cluster, and for the intermediate case, adopt a randomized rounding scheme to cluster the points. In particular, our proof provides another instance where nets based on randomized rounding provide better control than volumetric nets (see [6], [7], [8] for some other recent examples).

This section is organized as follows: in Section III-A, we show how to appropriately cluster points in the most challenging ‘intermediate’ case, mentioned above (Proposition 4). Given this, the proof of Theorem 1 is completed in Section III-B by following the aforementioned decomposition into heavy, collectively light, and intermediate cases.

A. Key Estimate

As alluded to above, the most challenging case in our analysis is that of a random vector with no ‘heavy’ atoms. The main result of this section, Proposition 4, shows how to construct a suitable sigma-algebra in this case. Briefly, by using a randomized rounding procedure, we construct a distribution over decompositions of the support of the random vector into \( k \) parts, and show that with high-probability, the sigma algebra generated by a random decomposition sampled from this distribution incurs sufficiently small covariance loss.

More precisely, let \( p = c \log k \), where \( c \) is a sufficiently small positive universal constant (for instance, \( c \in (0, 1/120) \) is certainly sufficient). Let

\[
\gamma := \frac{e^{-(\log k)/(4p)}}{\sqrt{p}} = \frac{e^{-1/(4c)}}{\sqrt{c \log k}}.
\]

Let \( X \) be a random vector valued in \( x_0 + [-\gamma/2, \gamma/2]^p \), supported on finitely many points, such that for any \( x \in \text{supp}(X) =: \mathcal{X} \), we have \( \mathbb{P}[X = x] \leq k^{-1/3} \); we note that
this is not the same random vector as the one appearing in the statement of Theorem 1. Let \( \mathcal{W} := x_0 + \{ \pm 3\gamma/2 \}_p \). For each \( x \in \mathcal{X} \), let \( w_x \in \mathcal{W} \) be a random vector defined as follows: \( \mathbb{E}[(w_x)_i] = x_i \), and the random variables \( (w_x)_i \) are independent. In words, the vector \( w_x \) is obtained by randomly rounding \( x \) to a point in \( \mathcal{W} \) so that \( w_x \) has mean \( x \); it is easily seen that such a distribution \( w_x \) is unique. Moreover, for distinct \( x \in \mathcal{X} \), the random vectors \( w_x \) are independent.

Now, given a realisation of the random vectors \( w_x \), for each \( w \in \mathcal{W} \), let

\[
C_w := \{ x \in \mathcal{X} : w_x = w \},
\]

so that \( C_w \) consists of those points in \( \mathcal{X} \) which are rounded to \( w \). Let \( \mathcal{F} \) denote the sigma-algebra corresponding to the partition \( (C_w)_{w \in \mathcal{W}} \). Note that \( \mathcal{F} \) is random, depending on the realisation of \( w_x \).

In our analysis, we will also require the following random vector, which should be viewed as an idealised version of \( \mathbb{E}[X | \mathcal{F}] \); this random vector, which we denote by \( Z \), takes on the value

\[
z_w := \frac{\sum_{x \in \mathcal{X}} x \mathbb{P}[w_x = w] \mathbb{P}[X = x]}{\sum_{x \in \mathcal{X}} \mathbb{P}[w_x = w] \mathbb{P}[X = x]}
\]

with probability

\[
q_w := \mathbb{P}[w_x = w] \mathbb{P}[X = x]
\]

each \( w \in \mathcal{W} \). We begin with the following preliminary, but key, lemma.

**Lemma 3:** With notation as above,

\[
\|\Sigma_X - \Sigma_Z\|_F = \|\mathbb{E}[XX^T] - \mathbb{E}[ZZ^T]\|_F \leq \frac{36e^{-1/2\epsilon}}{c \log k}.
\]

**Proof:** The first equality follows from the observation that \( \mathbb{E}[Z] = \mathbb{E}[X] \). We proceed to prove the inequality. For convenience of notation, let

\[
\mu_{x,w} := \mathbb{P}[X = x] \mathbb{P}(w_x = w).
\]

First, note that, using the definitions of \( z_w \) and \( q_w \),

\[
\begin{align*}
\sum_{x,w} \mu_{x,w} (x z_w)^T &= \sum_{w} q_w \left( q_w^{-1} \sum_x x \mathbb{P}[X = x] \mathbb{P}[w_x = w] \right) z_w^T \\
&= \sum_{w} q_w z_w z_w^T \\
&= \sum_{w} x \sum_{x,w} \mu_{x,w} z_w z_w^T,
\end{align*}
\]

and therefore, by transposition, \( \sum_{x,w} \mu_{x,w} z_w x^T = \sum_{x,w} \mu_{x,w} z_w z_w^T \). Therefore, we have

\[
\begin{align*}
\|\mathbb{E}[XX^T] - \mathbb{E}[ZZ^T]\|_F &= \|\sum_{x,w} \mu_{x,w} (x x^T - z_w z_w^T)\|_F \\
&= \|\sum_{x,w} \mu_{x,w} (x x^T - z_w z_w^T + z_w x^T - z_w x^T + z_w z_w^T)\|_F \\
&= \|\sum_{x,w} \mu_{x,w} (x x^T - z_w z_w^T + z_w x^T - z_w x^T + z_w z_w^T)\|_F
\end{align*}
\]

as desired.

Inequality (1) follows since \( (x+y)(x+y) \leq 2xx^T + 2yy^T \) for any vectors \( x, y \) and \( 0 \leq A \leq B \) for symmetric matrices \( A, B \) implies that \( \|A\|_F \leq \|B\|_F \). (To see this inequality note that \( \|B\|_F^2 - \|A\|_F^2 = \text{tr}(B^2 - A^2) = \text{tr}((B-A)(B+A)) = \text{tr}((B + A)^1/2(B-A)(B+A)^1/2) \geq 0 \).) Inequality (2) follows since for any collection of vectors \( y_1, \ldots, y_m \) and for any \( p_1 \geq 0, \ldots, p_m \geq 0 \) such that \( \sum_i p_i = 1 \), we have

\[
\begin{align*}
\sum_i p_i y_i (\sum_i p_i y_i)^T u &= \left( \sum_i p_i (u^T y_i)^2 \right) u \\
&\leq \left( \sum_i p_i \right) \left( \sum_i p_i (u^T y_i)^2 \right) u \\
&= u^T \left( \sum_i p_i y_i y_i^T u \\
&
\end{align*}
\]

where the second line uses Cauchy-Schwarz. Finally, inequality (3) uses that \( \mathbb{E}[(w_x)_i] = x_i \), the independence of \( (w_x)_i \) and \( (w_x)_j \), and the crude estimate \( \|x - w_x\|_2 \leq 3\gamma \). \( \square \)

The following is the main result of this subsection.

**Proposition 4:** There exists an absolute constant \( K > 0 \) such that for all \( k \geq K \), and with \( Y = \mathbb{E}[X | \mathcal{F}] \) (notation as above), we have

\[
\|\Sigma_X - \Sigma_Y\|_F = \|\mathbb{E}[XX^T] - \mathbb{E}[YY^T]\|_F \\
\leq \frac{36e^{-1/2\epsilon}}{c \log k} + K^{-1/48},
\]

with probability (over the realisation of \( \mathcal{F} \)) at least \( 1 - \exp(-k^{1/7}) \).

**Proof:** Without loss of generality we may assume that \( x_0 = 0 \). By Lemma 3 and the triangle inequality, it suffices to
show that for all sufficiently large $k$, except with probability at most $\exp(-k^{1/7})$,
\[ \|E[ZZ^T] - E[YY^T]\|_F \leq k^{-1/48}. \]
For convenience of notation, for $w \in \mathcal{W}$ let
\[ p_w := \sum_{x \in X} P(X = x) I[w_x = w] \]
and for $w \in \mathcal{W}$, $i \in [p]$, let
\[ (y_{w,i}) := \sum_{x \in X} x_i P(X = x) I[w_x = w]. \]
By Hoeffding’s inequality, for a given $w \in \mathcal{W}$,
\[ \mathbb{P}\left[ p_w - q_w \geq k^{-1/12}\right] \leq \exp\left(-2k^{-1/6}/\sum_x P[X = x]^2\right) \leq (1) \exp\left(-2k^{-1/6}/k^{-1/3}\right) = \exp(-2k^{1/6}), \]
where inequality (1) uses $\sum_x P[X = x]^2 \leq \max_x P[X = x] \leq k^{-1/3}$, by assumption. Similarly, for a given $w \in \mathcal{W}$ and $i \in [p]$, we have
\[ \mathbb{P}\left[ (y_{w,i}) - q_w \cdot (z_{w,i}) \geq \gamma \cdot k^{-1/12}\right] \leq \exp(-2\gamma^2k^{-1/6}/\sum_x x_i^2 P[X = x]^2) \leq \exp(-2k^{1/6}). \]
Let $E$ denote the event that $\sum_{x \in X} P[X = x] I[w_x = w] - q_w \leq k^{-1/12}$ and $\|y_{w,i} - q_w \cdot (z_{w,i})\| \leq \gamma \cdot k^{-1/12}$ for all $w \in \mathcal{W}$, $i \in [p]$. By the preceding discussion,
\[ \mathbb{P}[E^c] \leq 2 \cdot 2^p \cdot p \cdot \exp(-2k^{1/6}) \leq \exp(-k^{1/7}) \]
for all sufficiently large $k$. Moreover, for every $i \in [p]$ and $x \in \mathcal{X}$, since $x_i \in [-\gamma/2, \gamma/2]$ and $(z_{w,i}) \in \{\pm \gamma/2\}$, we must have $P[(w_x)_i = \epsilon \cdot \gamma/2] \geq 1/3$ for $\epsilon \in \{\pm 1\}$. Indeed, if this failed for, say, $\epsilon = 1$, then we would have $x_i = E[(w_x)_i] < (1/3) \cdot \gamma/2 + (2/3) \cdot (-\gamma/2) = -\gamma/2$, a contradiction. So, for every $w \in \mathcal{W}$,
\[ q_w \geq 3^{-p} \geq k^{-3c/2}, \]
and hence, on the event $E$, we have for all $w \in \mathcal{W}$ that
\[ p_w = q_w \pm k^{-1/12} \approx q_w (1 \pm k^{-1/24}), \]
assuming that $c < 1/36$. Finally, we see that on the event $E$,
\[ \|E[ZZ^T] - E[YY^T]\|_F = \left\| \sum_{w \in \mathcal{W}} (q_w z_{w}^T - y_w y_w^T/p_w) \right\|_F \leq \left\| \sum_{w} (q_w z_{w}^T - y_w y_w^T/p_w) \right\|_F \leq 2^p \max_w \|q_w z_{w} - y_w y_w/p_w\|_F \leq 2^p \gamma k^{1/2} \cdot k^{-1/12} + \gamma^2 k^{-1/2}, \]
\[ \leq \gamma^2 k^{-1/2} \leq \gamma \cdot k^{-1/12} + k^{1/2} \cdot \gamma^2 k^{-1/12} + k^{1/2} \cdot \gamma^2 k^{-1/12} + k^{1/2} \cdot \gamma^2 \leq \gamma \cdot k^{-1/24} \leq k^{-1/48}, \]
provided that $c < 1/120$.

### B. Finishing the Proof

With Proposition 4, we are ready to prove Theorem 1 through a sequence of reductions. Recall that in the statement of Theorem 1, $X$ is a random vector valued in $\mathbb{R}^m$ which satisfies $\|X\|_2 \leq 1$ almost surely. Without loss of generality, we may assume that $X$ is finitely supported, by rounding the points in the support to a sufficiently fine $\varepsilon$-net with respect to the Euclidean metric (see, e.g., [1, Lemma 3.6]).

Next, we show that it suffices to assume that $X$ is valued in $\mathbb{R}^p$, for $p = c \log k$, where $c$ is as in Section III-A. The following lemma is a slight modification of [1, Lemmas 3.2, 3.3].

**Lemma 5.** Suppose that $X$ is a random vector with $\|X\|_2 \leq 1$ almost surely. Let $S = E[XX^T]$ and let $P$ the projection onto the subspace corresponding to the largest $t \geq 1$ eigenvectors of $S$. Let $Y = E[X | PX]$. Then,
\[ \|\Sigma_X - \Sigma_Y\|_F = \|E[XX^T] - E[YY^T]\|_F \leq \frac{1}{\sqrt{t}}. \]

**Proof:** The equality holds since $E[X] = E[Y]$. For the inequality, we note that, with $A := E[XX^T] - E[YY^T]$,
\[ \|A\|_F \leq \|P A P\|_F + \|(I - P) E[XX^T](I - P)\|_F \leq \|P A P\|_F + \frac{1}{\sqrt{t}} \]
\[ = \|E(PX - PY)(PX - PY)^T\|_F + \frac{1}{\sqrt{t}} \]
\[ \leq \frac{1}{\sqrt{t}} \]
where (1) follows from the proof of [1, Lemma 3.2], (2) follows from [1, Lemma 3.3], and (3) follows since $PY = P E[X | PX] = PX$. □

By taking $t = c \log k$ in Lemma 5 and using the triangle inequality, we see that it suffices to prove Theorem 1 for $X$ in $\mathbb{R}^p$, with $p = c \log k$ (the clustering in the original problem corresponds to applying the map $P^{-1}$ to the clustering in the dimension-reduced problem). Therefore, consider such an $X$, and recall that we may assume that $X$ is finitely supported, denoting the support by $\mathcal{X}$. Let
\[ \mathcal{X}^{(1)} = \{x \in \mathcal{X} : P[X = x] \geq k/3\} \]
Note that $|\mathcal{X}^{(1)}| \leq k/3$. By assigning each point in $\mathcal{X}^{(1)}$ to its own cluster, it suffices to find a clustering of the points in $\mathcal{X} \setminus \mathcal{X}^{(1)}$ into fewer than $2k/3$ clusters.

For this, we begin by covering $\mathcal{B} := \{x \in \mathbb{R}^p : \|x\|_2 \leq 1\}$ by a disjoint union of cubes, denoted by $\mathcal{C}$, each with side length $\gamma = e^{-\log k/(4p)}/\sqrt{p}$. Since the Euclidean diameter of such a cube is at most $1$, this can be done in a manner such that all of the cubes in $\mathcal{C}$ are contained in $\mathcal{B} := \{x \in \mathbb{R}^p : \|x\|_2 \leq 2\}$. Moreover, since the volume of each cube in $\mathcal{C}$ is $(1/\sqrt{p})^p \cdot e^{-\log k/4}$ and the volume of $\mathcal{B}$ is well-known to be at most $\left(10/\sqrt{p}\right)^p$ (see, e.g., the proof of [1, Proposition 3.7]), it follows that the number of cubes in $\mathcal{C}$ is at most
\[ \left(\frac{10/\sqrt{p}}{1/\sqrt{p}}\right)^p \cdot e^{-\log k/4} = k^{1/4} \cdot 10^c \log k \leq k^{1/3}, \]
if $c < 1/50$, say. Therefore, it suffices to cluster the points in each cube into at most $(2/3)k^{2/3}$ clusters. We have two cases:
Case I: $\mathcal{C} \in \mathbb{C}$ satisfies $\mathbb{P}[X \in \mathcal{C} \setminus \mathcal{X}(1)] \leq k^{-1/2}$. Let us denote all such cubes by $\mathcal{C}_1$. In this case, we assign all the points in $\mathcal{C} \setminus \mathcal{X}(1)$ to a single cluster (say, corresponding to the midpoint of $\mathcal{C}$).

Case II: $\mathcal{C} \in \mathbb{C}$ satisfies $\mathbb{P}[X \in \mathcal{C} \setminus \mathcal{X}(1)] \geq k^{-1/2}$. Let us denote all such cubes by $\mathcal{C}_2$. In this case, consider the random vector $X_C$, which takes on each value $x \in \mathcal{C} \setminus \mathcal{X}(1)$ with probability $\mathbb{P}[X = x]/\mathbb{P}[X \in \mathcal{C} \setminus \mathcal{X}(1)]$.

Note that $X_C$ is supported on a $p$-dimensional cube of side length $\gamma$, and for any $x \in X_C$, we have that $\mathbb{P}[X_C = x] \leq (3/k)k^{-1/2} \leq 3k^{-1/2} \leq k^{-1/3}$. We partition the points in $\mathcal{C} \setminus \mathcal{X}(1)$ according to the clusters coming from Proposition 4 applied to $X_C$, noting that there are at most $2^p < k^{1/2}$ clusters for each cube $\mathcal{C} \in \mathcal{C}_2$ (provided that $c < 1/2$). Denote the corresponding sigma algebra by $\mathcal{F}_C$.

At this point, we have partitioned the points in $\mathcal{X}$ into at most $k/3 + k^{1/3}/k^{1/2} < k/2$ clusters. To complete the proof, we check that the sigma algebra $\mathcal{F}$ generated by this clustering satisfies the conclusion of Theorem 1. Letting $Y = \mathbb{E}[X | \mathcal{F}]$, we have

$$\|\Sigma_X - \Sigma_Y\|_F = \|\mathbb{E}[XX^T] - \mathbb{E}[YY^T]\|_F$$

$$\leq \sum_{C \in \mathcal{C}_1} \mathbb{P}[X \in C \setminus \mathcal{X}(1)] \cdot \gamma^2 p^+$$

$$+ \sum_{C \in \mathcal{C}_2} \mathbb{P}[X \in \mathcal{C} \setminus \mathcal{X}(1)] \cdot \|\Sigma_{X_C} - \Sigma_{\mathbb{E}[X_C | \mathcal{F}_C]}\|_F$$

$$\leq k^{1/3} \cdot k^{-1/2} +$$

$$+ \sum_{C \in \mathcal{C}_2} \mathbb{P}[X \in \mathcal{C} \setminus \mathcal{X}(1)] \cdot \left(\frac{36e^{-1/(2c)}}{\sqrt{c} \log k} + k^{-1/4k}\right)$$

$$\leq \frac{40}{\sqrt{c} \log k},$$

provided that $c < 1/120$ and $k$ is sufficiently large, where the penultimate inequality uses Proposition 4.

Acknowledgment

The authors would like to thank anonymous reviewers for helpful comments and suggestions, which have improved the presentation.

References

[1] M. Boedihardjo, T. Strohmer, and R. Vershynin, “Covariance’s loss is privacy’s gain: Computationally efficient, private and accurate synthetic data,” 2021, arXiv:2107.05824.

[2] L. Sweeney, “$k$-anonymity: A model for protecting privacy,” Int. J. Uncertainty, Fuzziness Knowl.-Based Syst., vol. 10, no. 5, pp. 557–570, 2002.

[3] M. Andrea, “Estimating random variables from random sparse observations,” Eur. Trans. Telecommun., vol. 19, no. 4, pp. 385–403, 2008.

[4] P. Raghavendra and N. Tan, “Approximating CSPs with global cardinality constraints using SDP hierarchies,” in Proc. 23rd Ann. ACM-SIAM Symp. Discrete Algorithms, New York, NY, USA, 2012, pp. 373–384.

[5] V. Jain, F. Koehler, and A. Risteski, “Mean-field approximation, convex hierarchies, and the optimality of correlation rounding: A unified perspective,” in Proc. 51st Ann. ACM SIGACT Symp. Theory Comput., Jun. 2019, pp. 1226–1236.

[6] K. Tikhomirov, “Singularity of random Bernoulli matrices,” Ann. Math., vol. 191, no. 2, pp. 593–634, 2020. [Online]. Available: https://doi.org//libproxy.mit.edu/10.4007/annals.2020.191.2.6

[7] B. Klartag and G. V. Livshyts, “The lower bound for Koldobsky’s slicing inequality via random rounding,” in Geometric Aspects of Functional Analysis. Cham, Switzerland: Springer, 2020, pp. 43–63.

[8] G. V. Livshyts, K. Tikhomirov, and R. Vershynin, “The smallest singular value of inhomogeneous square random matrices,” Ann. Probab., vol. 49, no. 3, pp. 1286–1309, 2021.

Vishesh Jain received the B.S. degree in mathematics from Stanford University, Stanford, CA, USA, in 2015, and the Ph.D. degree in mathematics from the Massachusetts Institute of Technology, Cambridge, MA, USA, in 2020.

In 2020, he was a Simons-Berkeley Research Fellow at the Simons Institute for the Theory of Computing. From 2021 to 2022, he was a Stein Fellow with the Department of Statistics, Stanford University. Since 2022, he has been an Assistant Professor with the Department of Mathematics, Statistics, and Computer Science, University of Illinois Chicago, Chicago, IL, USA. His research interests include high-dimensional probability, probabilistic combinatorics, and randomized algorithms.

Ashwin Sah received the B.S. degree in mathematics from the Massachusetts Institute of Technology (MIT), Cambridge, MA, USA, in 2020, where he is currently pursuing the graduate degree with the Mathematics Department. His research interests include extremal combinatorics, discrete probability, and random matrices.

Mehtaab Sawhney received the B.S. degree in mathematics from the Massachusetts Institute of Technology (MIT), Cambridge, MA, USA, in 2020, where he is currently pursuing the graduate degree with the Mathematics Department. His research interests include extremal and probabilistic combinatorics, algorithms, and random matrices.