A Fast and Efficient Algorithm for Low-rank Approximation of a Matrix

Nam H. Nguyen
The Johns Hopkins University
nam@jhu.edu

Thong T. Do
The Johns Hopkins University
thongdo@jhu.edu

Trac D. Tran
The Johns Hopkins University
trac@jhu.edu

ABSTRACT

The low-rank matrix approximation problem involves finding of a rank k version of a $m \times n$ matrix $\boldsymbol{A}$, labeled $\boldsymbol{A}_k$, such that $\boldsymbol{A}_k$ is as "close" as possible to the best SVD approximation version of $\boldsymbol{A}$ at the same rank level. Previous approaches approximate matrix $\boldsymbol{A}$ by non-uniformly adaptive sampling some columns (or rows) of $\boldsymbol{A}$, hoping that this subset of columns contain enough information about $\boldsymbol{A}$. The sub-matrix is then used for the approximation process. However, these approaches are often computationally intensive due to the complexity in the adaptive sampling. In this paper, we propose a fast and efficient algorithm which at first pre-processes matrix $\boldsymbol{A}$ in order to spread out information (energy) of every columns (or rows) of $\boldsymbol{A}$, then randomly selects some of its columns (or rows). Finally, a rank-k approximation is generated from the row space of these selected sets. The preprocessing step is performed by uniformly randomizing signs of entries of $\boldsymbol{A}$ and transforming all columns of $\boldsymbol{A}$ by an orthonormal matrix $\boldsymbol{F}$ with existing fast implementation (e.g. Hadamard, FFT, DCT...). Our main contribution is summarized as follows.

1) We show that by uniformly selecting at random d rows of the preprocessed matrix with $d = \mathcal{O}\left(\frac{1}{\eta} k \max\{\log k, \log \frac{1}{\beta}\}\right)$, we guarantee the relative Frobenius norm error approximation: $(1+\eta)\left\|A - A_k\right\|_F$ with probability at least $1 - 5\beta$.

2) With d above, we establish a spectral norm error approximation: $\left(2 + \sqrt{\frac{2m}{d}}\right)\left\|A - A_k\right\|_2$ with probability at least $1 - 2\beta$.

3) The algorithm requires 2 passes over the data and runs in time $\mathcal{O}\left(mn \log d + (m+n)d^2\right)$ which, as far as the best of our knowledge, is the fastest algorithm when the matrix $\boldsymbol{A}$ is dense.

4) As a bonus, applying this framework to the well-known least square approximation problem $\min \|\boldsymbol{Ax} - \boldsymbol{b}\|$ where $\boldsymbol{A} \in \mathbb{R}^{m \times r}$, we show that by randomly choosing $d = \mathcal{O}\left(\frac{1}{\eta}\gamma r \log m\right)$, the approximation solution is proportional to the optimal one with a factor of η and with extremely high probability, $(1 - 6m^{-\gamma})$, say.

STOC'09, May 31–June 2, 2009, Bethesda, Maryland, USA.

Categories and Subject Descriptors

F.2.1 [**Numerical Algorithms and Problems**]: Computations on matrices

General Terms

Algorithms, Theory

1. INTRODUCTION

Low-rank matrix approximation has been widely used in many applications involving latent semantic indexing, DNA microarray data, facial recognition, web search, clustering, just to name a few (see [1] for a detailed explanation of these applications). The Singular Value Decomposition (SVD) [2] gives the optimal rank-k approximation of a matrix $\boldsymbol{A}$ in the sense of both error bound in Frobenius and spectral norm. However, computing SVD requires the amount of memory and time which are superlinear in the size of $\boldsymbol{A}$, hence the true SVD becomes prohibitive in many applications. Recently, several developments showed that a subset of rows (or columns) which is obtained by adaptively sampling a few rows (or columns) of $\boldsymbol{A}$ is sufficient for the approximation process, particularly the work of Frieze et al. [3], Drineas et al. [1], [4], Har-Peled [5], Deshpande et al. [6], [7] and Sarlós [8].

The first adaptive-sampling algorithm was originated from Frieze et al. [3] which shows how to sample rows of $\boldsymbol{A}$. Drineas et al. [1] then proposes a simpler algorithm to compute an approximation of the SVD. Both methods claim an additive Frobenius norm error which depends on the Frobenius norm of the input matrix $\boldsymbol{A}$. This approach is undesirable as this norm of $\boldsymbol{A}$ is often large. Also built on Frieze et al.'s idea, more recently Har-Peled [5] and Deshpande et al. [7] propose more intriguing sampling techniques, one employs geometric ideas while the other pioneers the concept of volume sampling. They both showed that the Frobenius norm approximation error is relative, implying that the error is $(1+\eta)$ proportional to the best rank-k approximation and the technique is far better than additive one. However, the amount of time for constructing sampling distribution seems to be costly. Most recently, Sarlós [8] proposes a different approach based on results from fast Johnson-Lindenstrauss transform (FJLT) [9]. The paper shows that if a $d = \mathcal{O}(k/\eta + k \log k)$ random linear combination $\boldsymbol{C}$ of rows of $\boldsymbol{A}$ is constructed, then the rank-k approximation generated from row space of $\boldsymbol{C}$ achieves a relative error with constant probability (at least 1/2, say). This algorithm is the best so far in the sense of the least number of passes over the input data $\boldsymbol{A}$ (only two), as well as the running time $\mathcal{O}(Md + (n+m)d^2)$ where M denotes the number of non-zero elements of $\boldsymbol{A}$.

With a similar flavor but from a different perspective, we propose a new fast and efficient algorithm, demonstrating that by uniformly sampling $d = \mathcal{O}\left(\frac{1}{\eta} k \max\{\log k, \log \frac{1}{\beta}\}\right)$ rows of $\boldsymbol{A}$ after preprocessing, the rank-k approximation also guarantees the relative error with probability at least $(1 - 5\beta)$. Moreover, the algorithm only needs two passes over the input data and the running time is $\mathcal{O}\left(mn \log d + (m+n)d^2\right)$ which, as far as the best of our knowledge, is the fastest algorithms when the matrix $\boldsymbol{A}$ is dense. Our algorithm also produces a low-rank approximation whose spectral norm error is $\sqrt{2m/d}$, proportional to the best rank-k version.

Our approach is motivated from remarkable results in the compressed sensing (CS) community. The CS problem states that one can perfectly recover a k-sparse signal $\boldsymbol{x} \in \mathbb{R}^m$ which has at most k-nonzero coefficients from an observation $\boldsymbol{y} \in \mathbb{R}^d$, which is a random projector of x onto a much lower dimensional space: $d = \mathcal{O}(k \log m)$. To intuitively explain this magical phenomenon, it can be observed that $\boldsymbol{x}$ is a low dimensional signal embedded into a high dimensional space. Hence, under some good linear transforms, $\boldsymbol{y}$ will preserve enough information of $\boldsymbol{x}$ such that the critical information can be efficiently extracted by a good reconstruction algorithm. In a recent paper [10], we show that a structurally random matrix (SRM) is a promising candidate for compressed sensing. Mathematically, SRM $\boldsymbol{\Phi}$ of size $d \times m$ is a product of three matrices

$$\boldsymbol{\Phi} = \sqrt{\frac{m}{d}} \boldsymbol{SFD} \tag{1}$$

where

- $\boldsymbol{D}$, the local randomizer, is a diagonal matrix whose diagonal entries are i.i.d Rademacher random variables: $\mathbb{P}(D_{ii} = \pm 1) = 1/2$.
- $\boldsymbol{F}$ is any $m \times m$ orthonormal matrix. In practice, one can choose $\boldsymbol{F}$ among many with efficient fast-computable algorithms, for instance, Hadamard transform, FFT, DCT, and DWT.
- $\boldsymbol{S}$, the uniformly random downsampler, is an $d \times m$ matrix whose d rows are randomly selected from rows of an $m \times m$ identity matrix.

The intuition behind SRM is the Uncertainty Principle which states that a signal whose energy is spread out in time/spacial domain is concentrated in frequency domain and vice versa. From this observation, it is necessary to randomize all entries of $\boldsymbol{x}$ to produce a noise-like signal before applying a fast transform to it.

In our proposed algorithm, we utilize SRM $\boldsymbol{\Phi}$ as a preprocessor. By projecting columns of $\boldsymbol{A}$ onto $\boldsymbol{\Phi}$, we hope that the row space of $\boldsymbol{\Phi A}$ will contain a good approximation of the row space of the entire matrix $\boldsymbol{A}$. In a later section of the paper, we will show that a sufficient selection of rows of $\boldsymbol{FDA}$ will produce a fast approximation matrix and with a relative error in the Frobenius norm as well as small error in the spectral norm.

It is necessary to note that our algorithm is different from the one of Sarlós [8] in terms of the last pre-processing step. The later uses the so-called FJLT which is basically a combination of three matrices: $\boldsymbol{\Phi} = \boldsymbol{PFD}$ where $\boldsymbol{F}$ and $\boldsymbol{D}$ are both defined above, and $\boldsymbol{P}$ is a sparse matrix whose entries are chosen with distribution specified in [9]. Hence, the projections of columns of $\boldsymbol{A}$ on $\boldsymbol{\Phi}$ are obtained by multiplication operators on $\boldsymbol{P}$. In our algorithm, however, instead of using matrix multiplication, d rows of matrix $\boldsymbol{FDA}$ are uniformly selected in a random manner. Hence, if $\boldsymbol{F}$ is a fast transform like Hadamard or FFT, the computational time can be reduced from $\mathcal{O}(mnd)$ to $\mathcal{O}(mn \log d)$[11] with a dense input matrix $\boldsymbol{A}$. Our proofs are also significantly different: we use remarkable results in Banach space to claim for our results, while Sarlós arguments based on Johnson-Lindenstrauss lemma. In addition, unlike previously adaptively sampling techniques [3], [1], [4], [5], [7] whose sampling distributions base mostly on the characteristics of rows (columns) of $\boldsymbol{A}$, our algorithm sample rows of $\boldsymbol{FDA}$ uniformly at random which is superior in the simplicity sense.

While preparing this paper, we are awared of two closely-related efforts on constructing a similar preprocess as SRM [11], [12]. However, there are still several significant differences from our approach. In the first effort [11], entries of the diagonal matrix $\boldsymbol{D}$ are complex and distributed uniformly on the unit circle. However, they were only able to prove approximation bound if the matrix $\boldsymbol{S}$ is sampled with an order of k^2 coordinates ($d = \mathcal{O}(k^2)$) which is far over $k \log k$. Not only the techniques are different, our resulting spectral norm bound is also better by a factor of $\sqrt{d}$. Moreover, our approach is more general in the choice of the fast transform $\boldsymbol{F}$. In the second effort [12], the problem is different: the authors apply a pre-processing step to improve the least square approximation. Actually, by applying our technique, the number of samples here can be decreased by a factor of $\log(r \log m)$ and the probability of success is extremely higher. We will present this result in another version in the near future.

The paper is organized as follows. The next section covers critical background materials on matrix norms and linear algebra. In section III, we introduce the algorithm and present our main results for matrix approximation. We devote the last sections for our arguments and concluding remarks.

2. NOTATIONS AND REVIEW OF LINEAR ALGEBRA

Here are some notations used throughout the paper. Matrices are represented by bold capital letters while vectors are bold lower-case. Matrix and vector entries are not bold, just like any scalar. For instance, $\boldsymbol{A}$ is a matrix, and its entry at row i^{th} and column j^{th} is A_{ij}. Similarly, $\boldsymbol{a}$ is a vector, and a_i is its i^{th} entry. When we mention about a vector $\boldsymbol{a}$, we assume that it is the row vector while $\boldsymbol{a}^*$ is its transpose. In a matrix $\boldsymbol{A}$, $\boldsymbol{a}_i$ is defined as the i^{th}-row of the matrix $\boldsymbol{A}$.

2.1 Matrix and vector norms

Several different matrix norms are used throughout this paper. The spectral norm of a matrix $\boldsymbol{X}$ is denoted by $\|\boldsymbol{X}\|$ whereas the Frobenius norm is represented as $\|\boldsymbol{X}\|_F$. If we denote the Euclidean inner product between two matrices is $\langle \boldsymbol{X}, \boldsymbol{Y} \rangle = \text{trace}(\boldsymbol{X}^* \boldsymbol{Y})$, then $\|\boldsymbol{X}\|_F = \langle \boldsymbol{X}, \boldsymbol{X} \rangle$. It can be easily verified that: $\|\boldsymbol{X}\|_F = \sup_{\|\boldsymbol{Y}\|_F = 1} \langle \boldsymbol{X}, \boldsymbol{Y} \rangle$.

1: **Input:** Matrix $\boldsymbol{A} \in \mathbb{R}^{m\times n}$, error parameter η and probability success β

2: **Output:** Matrix $\tilde{\boldsymbol{A}}_k \in \mathbb{R}^{m\times n}$ of rank at most k

1. Set $d = \mathcal{O}\left(\frac{1}{\eta}\mu^2 m^2 \max\left\{k, \sqrt{k}\log\frac{m}{\beta}\right\}\max\left\{\log k, \log\frac{1}{\beta}\right\}\right)$ where $\mu = \max_{i,j}|F_{ij}|^2$
2. Randomly pick up a subset Ω of d entries from a set $\{1, 2, ..., m\}$ with probability of each entry selection is d/m
3. Compute $\boldsymbol{C} = \sqrt{\frac{m}{d}}\boldsymbol{F}_\Omega \boldsymbol{D}\boldsymbol{A} = \boldsymbol{\Phi}\boldsymbol{A}$.
4. Project rows of $\boldsymbol{A}$ onto $\boldsymbol{C}$ to obtain $\mathcal{P}_{\boldsymbol{C}}(\boldsymbol{A})$
5. Compute the best rank-k approximation of $\mathcal{P}_{\boldsymbol{C}}(\boldsymbol{A})$, $\tilde{\boldsymbol{A}}_k = \mathcal{P}_{\boldsymbol{C},k}(\boldsymbol{A})$

Algorithm 1: Low-rank matrix approximation algorithm

Another useful norm for our purpose is the Schatten norm. Given a parameter $q \geq 1$, the Schatten q-norm of a matrix $\boldsymbol{X}$ is defined as: $\|\boldsymbol{X}\|_{S_q} = \left(\sum_i s_i^q\right)^{1/q}$ where s_i's are singular values of the matrix $\boldsymbol{X}$.

Note that when $q = \infty$, the Schatten q-norm is the spectral norm: $\|\boldsymbol{X}\|_{S_\infty} = \|\boldsymbol{X}\|$. Schatten 2-norm is the Frobenius norm: $\|\boldsymbol{X}\|_{S_2} = \|\boldsymbol{X}\|_F$. The following properties of Schatten p-norm are used in the paper:

1) When $p \leq q$, the inequality occurs: $\|\boldsymbol{X}\|_{S_q} \leq \|\boldsymbol{X}\|_{S_p}$.

2) If r is a rank of $\boldsymbol{X}$, then with $q \geq \log(r)$, it holds that $\|\boldsymbol{X}\| \leq \|\boldsymbol{X}\|_{S_q} \leq e\|\boldsymbol{X}\|$.

With vectors, the only norm we consider is the l^2-norm, so we simple denote l^2-norm of a vector by $\|\boldsymbol{x}\|$ which is equal to $\sqrt{\langle \boldsymbol{x}, \boldsymbol{x}\rangle}$, where $\langle \boldsymbol{x}, \boldsymbol{y}\rangle$ is the Euclidean inner product between two vectors. Like matrices, we can straightforwardly establish: $\|\boldsymbol{x}\| = \sup_{\|\boldsymbol{y}\|=1}\langle \boldsymbol{x}, \boldsymbol{y}\rangle$.

2.2 Singular value decomposition

The Singular Value Decomposition (SVD) of a matrix $\boldsymbol{A} \in \mathbb{R}^{m\times n}$ is denoted by $\boldsymbol{A} = \boldsymbol{U}\boldsymbol{\Sigma}\boldsymbol{V}^*$ where $\boldsymbol{U} \in \mathbb{R}^{m\times\rho}$, $\boldsymbol{\Sigma} \in \mathbb{R}^{\rho\times\rho}$, $\boldsymbol{V} \in \mathbb{R}^{\rho\times n}$ with ρ being the rank of $\boldsymbol{A}$. The best rank-k approximation with respect to spectral and Frobenius norm of $\boldsymbol{A}$ turns out to be $\boldsymbol{A}_k = \boldsymbol{U}_k\boldsymbol{\Sigma}_k\boldsymbol{V}_k^*$, where $\boldsymbol{U}_k$ is the first k columns of $\boldsymbol{U}$.

The orthogonal projector of rows of a matrix $\boldsymbol{A}$ onto a matrix $\boldsymbol{C}$ is denoted by $\mathcal{P}_{\boldsymbol{C}}(\boldsymbol{A}) = \boldsymbol{A}\boldsymbol{C}^\dagger\boldsymbol{C}$ where $\boldsymbol{C}^\dagger$ is the Moore-Penrose pseudoinverse of $\boldsymbol{C}$. A best rank-k approximation of $\mathcal{P}_{\boldsymbol{C}}(\boldsymbol{A})$ is defined by $\mathcal{P}_{\boldsymbol{C},k}(\boldsymbol{A})$.

3. OUR ALGORITHM AND MAIN RESULTS

Our Algorithm 1 takes matrix $\boldsymbol{A} \in \mathbb{R}^{m\times n}$, an error parameter η and a probability success β as inputs. At first the $\boldsymbol{A}$ is preprocessed by randomizing signs its columns and passing through a fast linear transform, for instance, Hadamard, FFT, DCT, Wavelet, to name a few. A matrix $\boldsymbol{C}$ is then constructed by uniformly randomly sampling a subset of rows from the $\boldsymbol{FDA}$ matrix. Next steps are followed similarly as the algorithms of A. Deshpande et al. [7] and T. Sarlós [8]. The low-rank approximation matrix is constructed by projecting $\boldsymbol{A}$ onto $\boldsymbol{C}$ and computing the best rank-k approximation of this projector.

Remark 1. It is important to understand the significance of the parameter μ here. μ can be seen as a measure of how concentrated and expanded magnitude of rows of the transform $\boldsymbol{F}$ are. The value of μ ranges from $1/m$ to 1. In the worse case when $\mu = 1$ and $\boldsymbol{F}$ is a diagonal matrix with $|F_{ii}| = 1$, it implies that most of the entries of $\boldsymbol{A}$ are totally lost in the random selection process, except when $d = m$. Hence, the matrix $\boldsymbol{C}$ is certainly not able to represent a good approximation of $\boldsymbol{A}$ at small d. On the other hand when $\mu = 1/m$, $\boldsymbol{F}$ is a Hadamard or Fourier matrix, entries of $\boldsymbol{F}$ are spread out uniformly and number of rows to select is optimal: $d = \mathcal{O}\left(\frac{1}{\eta}\max\left\{k, \sqrt{k}\log\frac{2m}{\beta}\right\}\max\left\{\log k, \log\frac{3}{\beta}\right\}\right)$.

Our main result for the Algorithm 1 is presented in the following theorem. Its proof is delayed to the next section.

THEOREM 1. *Suppose $\boldsymbol{A} \in \mathbb{R}^{m\times n}$, let $\eta \in (0,1]$ and $\beta \in (0,1)$. Running the Algorithm 1 will return a rank-k approximation matrix $\tilde{\boldsymbol{A}}_k$. Then the three following claims hold:*

1. $\left\|\boldsymbol{A} - \tilde{\boldsymbol{A}}_k\right\|_F \leq (1+\eta)\|\boldsymbol{A} - \boldsymbol{A}_k\|_F$ *with probability at least* $1 - 5\beta$
2. $\left\|\boldsymbol{A} - \tilde{\boldsymbol{A}}_k\right\| < (2 + \sqrt{\frac{2m}{d}})\|\boldsymbol{A} - \boldsymbol{A}_k\|$ *with probability at least* $1 - 2\beta$,
3. *The algorithm requires two passes over the data and runs in time* $\mathcal{O}\left(mn\log d + (m+n)d^2\right)$

Remark 2. Recently, there appears two inspiring works of N. Ailon and E. Liberty [13] [14] which significantly improve the running time of Johnson-Lindenstrauss (JL) transform. Particularly, they showed that by connecting results in coding theory, a fast linear mapping $\boldsymbol{\Phi} \in \mathbb{R}^{d\times m}$ which guarantees JL Lemma is efficiently designed [13]. The 'efficiency' implies complexity of the projection of $\boldsymbol{A}$ onto $\boldsymbol{\Phi}$ is reduced to $\mathcal{O}(mn\log d)$ (the efford of [14] even archive a more decreasing complexity which is a order $\mathcal{O}(mn)$. Nevertheless, maximum entries of each column of $\boldsymbol{A}$ need to be strictly restricted). These FJLT can be applied directly to Sarlós's algorithm [8] to obtain less running time. Hence, it is now essential to evaluate the proposed algorithm with Sarlós's one. For a fair comparison, we fix the transform matrix to be Hardarmard and set probability of success to $1 - m^{-1}$. Then our algorithm needs $d = \mathcal{O}\left(\frac{1}{\eta}\max\left\{k\log m, \sqrt{k}\log^2 m\right\}\right)$ and $\mathcal{O}\left(mn\log(k\log m) + (m+n)(k\log m)^2\right)$ for computational complexity (when k is less than $\mathcal{O}(\log^2 m)$), while applying the best FJLT so far [13] to Sarlós's algorithm will requires

$$\mathcal{O}\left(\left[mn\log(k\log k) + (m+n)(k\log k)^2\right]\log m\right)$$

complexity which is still higher than that of our by approximately a factor of $\log m$.

4. PROOF OF THEOREM 1

Suppose matrix $\boldsymbol{A}$ has rank ρ. Let $\boldsymbol{A} = \boldsymbol{U}\boldsymbol{\Sigma}\boldsymbol{V}^*$. Denote pairs $\boldsymbol{U}_k$, $\boldsymbol{V}_k$ and $\boldsymbol{U}_{\rho-k}$, $\boldsymbol{V}_{\rho-k}$ the matrices of the first k and last $(\rho - k)$ singular vectors of $\boldsymbol{U}$, $\boldsymbol{V}$, respectively. Also denote $\boldsymbol{\Sigma}_k$ and $\boldsymbol{\Sigma}_{\rho-k}$ diagonal matrices of the first k and last $(\rho - k)$ singular values of $\boldsymbol{\Sigma}$. In order to establish the Theorem 1, we use the two following lemmas and theorems. These lemmas will be proven at the end of the section. We leave the proofs of Theorem 2 and 3 for the next section.

The two following lemmas consider the Frobenius and spectral norm bounds of $(\boldsymbol{A} - \tilde{\boldsymbol{A}}_k)$.

LEMMA 1. *Let $\boldsymbol{H} = \boldsymbol{U}_{\rho-k}\boldsymbol{\Sigma}_{\rho-k}$. If matrix $(\boldsymbol{\Phi}\boldsymbol{U}_k)$ is full column rank, then the following inequality holds*

$$\left\|\boldsymbol{A} - \mathcal{P}_{\boldsymbol{C},k}(\boldsymbol{A})\right\|_F \le \left\|\boldsymbol{A} - \boldsymbol{A}_k\right\|_F + \left\|(\boldsymbol{\Phi}\boldsymbol{U}_k)^\dagger \boldsymbol{\Phi}\boldsymbol{H}\right\|_F$$

In the next lemma, we consider the spectral norm bound.

LEMMA 2. *Let $\boldsymbol{H} = \boldsymbol{U}_{\rho-k}\boldsymbol{\Sigma}_{\rho-k}$. If matrix $(\boldsymbol{\Phi}\boldsymbol{U}_k)$ is full column rank, then the following inequality holds*

$$\left\|\boldsymbol{A} - \mathcal{P}_{\boldsymbol{C},k}(\boldsymbol{A})\right\| \le 2\left\|\boldsymbol{A} - \boldsymbol{A}_k\right\| + \left\|(\boldsymbol{\Phi}\boldsymbol{U}_k)^\dagger \boldsymbol{\Phi}\boldsymbol{H}\right\|$$

From the fact that for any two matrices $\boldsymbol{X}$ and $\boldsymbol{Y}$, $\|\boldsymbol{X}\boldsymbol{Y}\|_F \le \|\boldsymbol{X}\|\,\|\boldsymbol{Y}\|_F$, we have

$$\left\|(\boldsymbol{\Phi}\boldsymbol{U}_k)^\dagger \boldsymbol{\Phi}\boldsymbol{H}\right\|_F \le \left\|(\boldsymbol{U}_k^*\boldsymbol{D}^*\boldsymbol{F}_\Omega^*\boldsymbol{F}\boldsymbol{D}\boldsymbol{U}_k)^{-1}\right\| \left\|\boldsymbol{U}_k^*\boldsymbol{\Phi}^*\boldsymbol{\Phi}\boldsymbol{H}\right\|_F \tag{2}$$

Similar result can be obtained with the spectral norm of $(\boldsymbol{\Phi}\boldsymbol{U}_k)^\dagger \boldsymbol{\Phi}\boldsymbol{H}$.

We now denote random variables for random signs and sampling processes. Let $\epsilon_i = D_{ii}$ be i.i.d Rademacher random variables with $\mathbb{P}(\epsilon_i = \pm 1) = 1/2$. Also let δ_j be i.i.d Bernoulli 0/1 random variables with $\mathbb{P}(\delta_j = 1) = d/m$ whose subscript j represents the entry selected from a set $\{1, 2, ..., m\}$. As mentioned above, $j \in \Omega$. For consistence, we define $\boldsymbol{u}_i$ and $\boldsymbol{h}_k$ are row vectors of $\boldsymbol{U}_k$ and $\boldsymbol{H}$, respectively. Also denote $\{\boldsymbol{e}_j \in \mathbb{R}^m\}_{1\le j\le m}$ the standard basis in the Euclidean space. It is followed that $\boldsymbol{F}_\Omega^*\boldsymbol{F}_\Omega = \sum_{j\in\Omega} \boldsymbol{f}_j^*\boldsymbol{f}_j = \sum_{j=1}^m \delta_j \boldsymbol{f}_j^*\boldsymbol{f}_j$. Hence,

$$\begin{aligned}
&(\boldsymbol{U}_k^*\boldsymbol{D}^*)(\boldsymbol{F}_\Omega^*\boldsymbol{F}_\Omega)(\boldsymbol{D}\boldsymbol{H}) \\
&= \left(\sum_{i=1}^m \epsilon_i \boldsymbol{u}_i^*\boldsymbol{e}_i\right)\left(\sum_{j=1}^m \delta_j \boldsymbol{f}_j^*\boldsymbol{f}_j\right)\left(\sum_{k=1}^m \epsilon_k \boldsymbol{e}_k^*\boldsymbol{h}_k\right) \\
&= \sum_{j=1}^m\sum_{i=1}^m\sum_{k=1}^m \delta_j\epsilon_i\epsilon_k \boldsymbol{u}_i^*\left(\boldsymbol{e}_i\boldsymbol{f}_j^*\right)\left(\boldsymbol{f}_j\boldsymbol{e}_k^*\right)\boldsymbol{h}_k \\
&= \sum_{j=1}^m \delta_j \sum_{i=1}^m\sum_{k=1}^m \epsilon_i\epsilon_k F_{ij}^*F_{jk}\boldsymbol{u}_i^*\boldsymbol{h}_k \\
&= \sum_{j=1}^m \delta_j\left(\sum_{i=1}^m \epsilon_i F_{ij}^*\boldsymbol{u}_i^*\right)\left(\sum_{k=1}^m \epsilon_k F_{jk}\boldsymbol{h}_k\right) = \sum_{j=1}^m \delta_j \boldsymbol{x}_j^*\boldsymbol{y}_j
\end{aligned} \tag{3}$$

where row vectors

$$\boldsymbol{x}_j := \sum_{i=1}^m \epsilon_i F_{ij}\boldsymbol{u}_i \quad \text{and} \quad \boldsymbol{y}_j := \sum_{k=1}^m \epsilon_k F_{jk}\boldsymbol{h}_k. \tag{4}$$

Hence,

$$\boldsymbol{U}_k^*\boldsymbol{\Phi}^*\boldsymbol{\Phi}\boldsymbol{H} = \frac{m}{d}\sum_{j=1}^m \delta_j \boldsymbol{x}_j^*\boldsymbol{y}_j \tag{5}$$

Likewise, $\boldsymbol{U}_k^*\boldsymbol{\Phi}^*\boldsymbol{\Phi}\boldsymbol{U}_k = \frac{m}{d}\sum_{j=1}^m \delta_j \boldsymbol{x}_j^*\boldsymbol{x}_j$

In order to prove the Theorem 1, it is sufficient to

1. find a condition on d such that matrix $\sum_{j=1}^m \delta_j \boldsymbol{x}_j^*\boldsymbol{x}_j$ is invertible.

2. find the spectral norm bound of $\left(\sum_{j=1}^m \delta_j \boldsymbol{x}_j^*\boldsymbol{x}_j\right)^{-1}$.

3. find the Frobenius norm bound of $\sum_{j=1}^m \delta_j \boldsymbol{x}_j^*\boldsymbol{y}_j$.

The next theorem is dedicated for showing the bound of d upon which $\sum_{j=1}^m \delta_j \boldsymbol{x}_j^*\boldsymbol{x}_j$ is invertible and establish the probabilistic bound of $\left\|I - \frac{m}{d}\sum_{j=1}^m \delta_j \boldsymbol{x}_j^*\boldsymbol{x}_j\right\|$.

THEOREM 2. *Let $S = \left\|I - \frac{m}{d}\sum_{i=1}^m \delta_i \boldsymbol{x}_i^*\boldsymbol{x}_i\right\|$. Suppose the number of samples d obeys: $d \ge 25mq\max\|\boldsymbol{x}_j\|^2$ for $q \ge \log k$. Then,*

$$(\mathbb{E}S^q)^{1/q} \le 5\sqrt{\frac{m}{d}}\sqrt{q}\max_i\|\boldsymbol{x}_i\| \tag{6}$$

If $d \ge \frac{C_1}{a}\mu m \max\left\{k, \log\frac{2m}{\beta}\right\}\log k$ for a positive constant $C_1 \le 25$. Then,

$$\mathbb{P}(S \le a) \ge 1 - 2\beta \tag{7}$$

where a is any constant in $(0, 1)$

In the next theorem, we consider the Frobenius norm bound of the sum $\sum_{j=1}^m \delta_j \boldsymbol{x}_j^*\boldsymbol{y}_j$.

THEOREM 3. *Let $S_F = \left\|\sum_{j=1}^m \delta_j \boldsymbol{x}_j^*\boldsymbol{y}_j\right\|_F$ and denote $\alpha = \|\boldsymbol{A} - \boldsymbol{A}_k\|_F^2$. Then,*

$$\begin{aligned}
\mathbb{E}S_F \le& 4.65\max_i\|\boldsymbol{x}_i\|\max_i\|\boldsymbol{y}_i\| \\
&+ 2.56\sqrt{\frac{d}{m}}\max\left\{\sqrt{\alpha}\max_i\|\boldsymbol{x}_i\|, k^{1/4}\max_i\|\boldsymbol{y}_i\|\right\}
\end{aligned} \tag{8}$$

Also, there is a small numerical constant C such that,

$$\mathbb{P}\left(S_F \le C\mu\sqrt{\alpha}\sqrt{d\sqrt{k}\max\{\sqrt{k}, \log\frac{2m}{\beta}\}\log\frac{3}{\beta}}\right) \ge 1 - 3\beta. \tag{9}$$

PROOF. (*Theorem 1*)

We are now ready to verify arguments in Theorem 1. Theorem 2 states that as we sample enough rows of $\boldsymbol{\Phi}$ ($d \ge \frac{C_1}{a}\mu m\max\left\{k, \log\frac{2m}{\beta}\right\}\log k$, say), $\|\boldsymbol{I} - \boldsymbol{U}_k^*\boldsymbol{\Phi}^*\boldsymbol{\Phi}\boldsymbol{U}_k\| < 1$ with high probability, which implies that $\boldsymbol{\Phi}\boldsymbol{U}_k$ is full column rank. Furthermore, every singular values of $\boldsymbol{\Phi}\boldsymbol{U}_k$ are bounded in the range

$$\sqrt{1-a} \le s_{\min}(\boldsymbol{\Phi}\boldsymbol{U}_k) \le s_{\max}(\boldsymbol{\Phi}\boldsymbol{U}_k) \le \sqrt{1+a} \tag{10}$$

It can be easy to verify that for a matrix $\boldsymbol{B}$, $\left\|(\boldsymbol{B}^*\boldsymbol{B})^{-1}\right\| \le 1/s_{min}^2(\boldsymbol{B})$. Therefore with the choice of $a = 1/5$, we obtain

$$\mathbb{P}\left(\left\|(\boldsymbol{U}_k^*\boldsymbol{\Phi}^*\boldsymbol{\Phi}\boldsymbol{U}_k)^{-1}\right\| \le \frac{5}{4}\right) \ge 1 - \beta \tag{11}$$

Based on the above inequalities, we now simply bound the second term of the Lemma 2 as follows

$$\begin{aligned}
\left\|(\boldsymbol{\Phi}\boldsymbol{U}_k)^\dagger\boldsymbol{\Phi}\boldsymbol{H}\right\| &\le \left\|(\boldsymbol{U}_k^*\boldsymbol{\Phi}^*\boldsymbol{\Phi}\boldsymbol{U}_k)^{-1}\right\|\|\boldsymbol{\Phi}\boldsymbol{U}_k\|\|\boldsymbol{\Phi}\boldsymbol{U}_{\rho-k}\|\|\boldsymbol{\Sigma}_{\rho-k}\| \\
&< \sqrt{\frac{2m}{d}}\|\boldsymbol{A} - \boldsymbol{A}_k\|
\end{aligned}$$

with probability at least $(1 - 2\beta)$. This inequality in combination with the Lemma 2 proves the second statement of Theorem 1.

Combine second claim of Theorem 3 and (2), (11), we have with probability at least $1 - 5\beta$

$$\begin{aligned}
\left\|(\boldsymbol{\Phi}\boldsymbol{U}_k)^\dagger\boldsymbol{\Phi}\boldsymbol{H}\right\|_F &\le C\frac{5m}{4d}\sqrt{d\sqrt{k}\max\{\sqrt{k}, \log\frac{2m}{\beta}\}\log\frac{3}{\beta}}\mu\sqrt{\alpha} \\
&:= \eta\sqrt{\alpha}
\end{aligned}$$

where $\eta < 1$. Set $C_2 := C^2(5/4)^2$, we get

$$d = C_2 \frac{1}{\eta}\mu^2 m^2 \max\left\{k, \sqrt{k}\log\frac{2m}{\beta}\right\}\log\frac{3}{\beta}$$

In combination with a condition on d that $\boldsymbol{\Phi U}_k$ is full row rank, d must satisfies

$$d = C\frac{1}{\eta}\mu^2 m^2 \max\left\{k, \sqrt{k}\log\frac{2m}{\beta}\right\}\max\left\{\log k, \log\frac{3}{\beta}\right\}$$

where $C := \max\{5C_1, C_2\}$ is a small numerical constant.

Also from Lemma 1, we conclude the first statement of Theorem 1

The running time can be bound similarly as in [8] and [7]. Note that with our SRM, we do not have to use matrix multiplication. Hence, the computational time is reduced by a factor of $d/\log d$.

□

4.1 Proof of Lemma 1

PROOF. The proof is similar to the proof of Theorem 1 in [4] with small modifications (see also Theorem 14 in [8]). Note that $\mathcal{P}_{\boldsymbol{C},k}(\boldsymbol{A})$ is the best rank-k approximation of $\boldsymbol{A}$ on the row space spanned by $\boldsymbol{C}$. Therefore,

$$\|\boldsymbol{A} - \mathcal{P}_{\boldsymbol{C},k}(\boldsymbol{A})\|_F \le \|\boldsymbol{A} - \boldsymbol{B}\|_F$$

where $\boldsymbol{B}$ is any matrix of rank-k whose rows are on the row space of $\boldsymbol{C}$. We also have

$$\|\boldsymbol{A} - \boldsymbol{B}\|_F \le \|\boldsymbol{A} - \boldsymbol{A}_k\|_F + \|\boldsymbol{A}_k - \boldsymbol{B}\|_F$$

We choose $\boldsymbol{B} = \boldsymbol{A}_k(\boldsymbol{\Phi A}_k)^\dagger \boldsymbol{C} = \boldsymbol{A}_k(\boldsymbol{\Phi A}_k)^\dagger \boldsymbol{\Phi A}$. In [4], the author showed that

$$\left\|\boldsymbol{A}_k - \boldsymbol{A}_k(\boldsymbol{\Phi A}_k)^\dagger \boldsymbol{\Phi A}\right\|_F = \left\|(\boldsymbol{\Phi U}_k)^\dagger \boldsymbol{\Phi U}_{\rho-k}\boldsymbol{\Sigma}_{\rho-k}\right\|_F$$

The proof is completed. □

4.2 Proof of Lemma 2

Before proving the Lemma 2 , we show that orthogonal projection of rows of a matrix $\boldsymbol{A}$ onto a matrix $\boldsymbol{C}$ also preserves the optimality of the spectral norm.

PROPOSITION 1.

$$\left\|\boldsymbol{A} - \boldsymbol{AC}^\dagger \boldsymbol{C}\right\| \le \|\boldsymbol{A} - \boldsymbol{B}\|$$

where $\boldsymbol{B}$ is any matrix whose rows are on the space spanned by rows of $\boldsymbol{C}$

PROOF. Denote $\hat{\boldsymbol{x}} = \operatorname{argmax}_{\|\boldsymbol{x}\|=1}\left\|\boldsymbol{x}^*\boldsymbol{A} - \boldsymbol{x}^*\boldsymbol{AC}^\dagger\boldsymbol{C}\right\|$ and let $\boldsymbol{B} = \boldsymbol{PC}$. We have

$$\begin{aligned}
\|\boldsymbol{A} - \boldsymbol{PC}\| &= \sup_{\|\boldsymbol{x}\|=1}\|\boldsymbol{x}^*\boldsymbol{A} - \boldsymbol{x}^*\boldsymbol{PC}\| \\
&= \sup_{\|\boldsymbol{x}\|=1}\|\boldsymbol{x}^*\boldsymbol{A} - \boldsymbol{z}^*\boldsymbol{C}\| \qquad (\text{denote } \boldsymbol{z}^* = \boldsymbol{x}^*\boldsymbol{P}) \\
&\ge \|\hat{\boldsymbol{x}}^*\boldsymbol{A} - \boldsymbol{z}^*\boldsymbol{C}\| \ge \left\|\hat{\boldsymbol{x}}^*\boldsymbol{A} - \hat{\boldsymbol{x}^*}\boldsymbol{AC}^\dagger\boldsymbol{C}\right\| \\
&= \left\|\boldsymbol{A} - \boldsymbol{AC}^\dagger\boldsymbol{C}\right\| \qquad (\text{by definition of } \boldsymbol{x}^*)
\end{aligned}$$

The last inequality holds since $\hat{\boldsymbol{x}^*}\boldsymbol{AC}^\dagger\boldsymbol{C}$ is the orthogonal projection of $\hat{\boldsymbol{x}}^*\boldsymbol{A}$ onto $\boldsymbol{C}$, and thus $\left\|\hat{\boldsymbol{x}}^*\boldsymbol{A} - \hat{\boldsymbol{x}^*}\boldsymbol{AC}^\dagger\boldsymbol{C}\right\|$ is minimal. □

The next proposition which has been stated in Theorem 1.6 of [15] and is simple to verify. It is said that if $\boldsymbol{B}$ is a matrix with bounded norm, then for any bounded-norm matrix $\boldsymbol{A}$, singular values of $\boldsymbol{AB}$ satisfy

PROPOSITION 2. *For every $i = 1, ..., rank(\boldsymbol{A})$*

$$s_i(\boldsymbol{AB}) \le \|\boldsymbol{B}\|\, s_i(\boldsymbol{A})$$

PROOF. (*Lemma 2*) From the triangular inequality, we have

$$\|\boldsymbol{A} - \mathcal{P}_{\boldsymbol{C},k}(\boldsymbol{A})\| \le \left\|\boldsymbol{A} - \boldsymbol{AC}^\dagger\boldsymbol{C}\right\| + \left\|\boldsymbol{AC}^\dagger\boldsymbol{C} - \mathcal{P}_{\boldsymbol{C},k}(\boldsymbol{A})\right\|$$

Recall that $\mathcal{P}_{\boldsymbol{C},k}(\boldsymbol{A}) = \left(\boldsymbol{AC}^\dagger\boldsymbol{C}\right)_k$ is best rank-k approximation of $\boldsymbol{AC}^\dagger\boldsymbol{C}$. Hence,

$$\left\|\boldsymbol{AC}^\dagger\boldsymbol{C} - \mathcal{P}_{\boldsymbol{C},k}(\boldsymbol{A})\right\| = s_{k+1}(\boldsymbol{AC}^\dagger\boldsymbol{C})$$

By Proposition 2, $s_{k+1}(\boldsymbol{AC}^\dagger\boldsymbol{C}) \le \left\|\boldsymbol{C}^\dagger\boldsymbol{C}\right\| s_{k+1}(\boldsymbol{A}) = s_{k+1}(\boldsymbol{A}) = \|\boldsymbol{A} - \boldsymbol{A}_k\|$

In addition, from triangular inequality,

$$\begin{aligned}
\left\|\boldsymbol{A} - \boldsymbol{AC}^\dagger\boldsymbol{C}\right\| &\le \left\|\boldsymbol{A}_k - \boldsymbol{A}_k\boldsymbol{C}^\dagger\boldsymbol{C}\right\| + \left\|(\boldsymbol{A} - \boldsymbol{A}_k) - (\boldsymbol{A} - \boldsymbol{A}_k)\boldsymbol{C}^\dagger\boldsymbol{C}\right\| \\
&\le \left\|\boldsymbol{A}_k - \boldsymbol{A}_k\boldsymbol{C}^\dagger\boldsymbol{C}\right\| + \|\boldsymbol{A} - \boldsymbol{A}_k\|
\end{aligned}$$

Proposition 1 addresses that $\left\|\boldsymbol{A}_k - \boldsymbol{A}_k\boldsymbol{C}^\dagger\boldsymbol{C}\right\| \le \|\boldsymbol{A}_k - \boldsymbol{B}\|$ where $\boldsymbol{B}$ is any matrix whose rows are on the row space spanned by $\boldsymbol{C}$. As in Lemma 1, we choose $\boldsymbol{B} = \boldsymbol{A}_k(\boldsymbol{\Phi A}_k)^\dagger\boldsymbol{C}$. The proof in Theorem 1 of [4] also holds with spectral norm. We obtain

$$\left\|\boldsymbol{A}_k - \boldsymbol{A}_k(\boldsymbol{\Phi A}_k)^\dagger\boldsymbol{\Phi A}\right\| = \left\|(\boldsymbol{\Phi U}_k)^\dagger\boldsymbol{\Phi U}_{\rho-k}\boldsymbol{\Sigma}_{\rho-k}\right\|$$

The Lemma is followed. □

5. PROOFS OF THEOREMS 2 AND 3

At the moment, we admit that expectation bounds (6) and (8) of Theorem 2 and 3 holds. We now focus on verifying (7) and (9). The arguments for these expectation bound will be postponed to the Appendix.

At first, we state two lemmas for bounding $\max_i\|\boldsymbol{x}_j\|$ and $\max_i\|\boldsymbol{y}_j\|$ where $\boldsymbol{x}_j$ and $\boldsymbol{y}_j$ are the sum of vectors with random ± 1 weights. We leave the proof to the end of the section.

LEMMA 3. *Let $\boldsymbol{x}_j$ be defined in (4),*

$$\mathbb{P}\left(\max_{1\le j\le m}\|\boldsymbol{x}_j\| \le \sqrt{\mu k} + 4\sqrt{\mu}\sqrt{\log\frac{2m}{\beta}}\right) \ge 1 - \beta \qquad (12)$$

LEMMA 4. *Let $\boldsymbol{y}_j$ be defined in (4),*

$$\mathbb{P}\left(\max_{1\le j\le m}\|\boldsymbol{y}_j\| \le \sqrt{\mu\alpha} + 4\sqrt{\frac{\mu\alpha}{r_k}}\sqrt{\log\frac{2m}{\beta}}\right) \ge 1 - \beta \quad (13)$$

where $\alpha = \|\boldsymbol{A} - \boldsymbol{A}_k\|_F^2$, r_k is the numerical rank of $(\boldsymbol{A} - \boldsymbol{A}_k)$ which is defined as: $r_k = \alpha/\delta_{k+1}^2$.

5.1 Proof of Theorem 2

PROOF. Take $q = \log k$ and apply Markov's inequality. For each $t > 0$, $\mathbb{P}(S \ge t\mathbb{E}S) \le t^{-q}$. By choosing $t = e$ and $\beta \ge t^{-q}$, we attain

$$\mathbb{P}\left(S \le 5e\sqrt{\frac{m}{d}}\sqrt{\log k}\max_j\|x_j\|\right) \ge 1 - \beta.$$

Combine with Lemma 3 and let

$$a = C_1\sqrt{\frac{m}{d}}\sqrt{\log k}\sqrt{\mu}\max\{k, 4\log 2m/\beta\}$$

with $C_1 \leq 10e$ we conclude the proof. $\square$

5.2 Proof of Theorem 3

In order to bound Frobenius norm of the sum of $\sum_{j=1}^m \delta_j \boldsymbol{x}_j^* \boldsymbol{y}_j$, one of the easy way is to apply a simple Markov's inequality. However, the probabilistic bound is not tight. Instead, we use a remarkable result from Talagrand [16] (see also Corollary 7.8 of [17] which bound the supremum of a sum of independent random variables Z_1, Z_2, ..., Z_m in Banach space

$$S = \sup_{g\in\mathcal{G}}\sum_{i=1}^m g(Z_i)$$

LEMMA 5. *If $|g| \leq \eta$ for every $g \in \mathcal{G}$ and $\{g(Z_i)\}_{1\leq i\leq m}$ have zero mean for every $g \in \mathcal{G}$. Then for all $t \geq 0$,*

$$\mathbb{P}\left(|S - \mathbb{E}S| \geq t\right) \leq 3\exp\left(-\frac{t}{C\eta}\log\left(1 + \frac{\eta t}{\sigma^2 + \eta\mathbb{E}\overline{S}}\right)\right), \tag{14}$$

where $\sigma^2 = \sup_{g\in\mathcal{G}}\sum_{i=1}^n \mathbb{E}g^2(Z_i)$, $\overline{S} = \sup_{g\in\mathcal{G}}\left|\sum_{i=1}^n g(Z_i)\right|$, and $C > 0$ is a small numerical constant.

In the next Lemma, we claim that with high probability the deviation of $\left\|\sum_{j=1}^m \delta_j \boldsymbol{x}_j^* \boldsymbol{y}_j\right\|_F$ is small. This implies that the Frobenius norm of the sum is highly concentrated around its expectation

LEMMA 6. *With S_F defined in Theorem 3, its probabilistic bound is*

$$\mathbb{P}\left(S_F \leq C_1\sqrt{\log\frac{3}{\beta}}\cdot\mathbb{E}S_F\right) \geq 1 - \beta \tag{15}$$

where C_1 is a small numerical constant.

PROOF. At first we note that $\|\boldsymbol{X}\|_F = \sup_{\|\boldsymbol{G}\|_F=1}\text{trace}(\boldsymbol{X}^*\boldsymbol{G}) = \sup_{\|\boldsymbol{G}\|_F=1}\langle\boldsymbol{X},\boldsymbol{G}\rangle$. Let $\boldsymbol{Z}_j := \delta_j \boldsymbol{x}_j^* \boldsymbol{y}_j$, we have

$$S_F = \left\|\sum_{j=1}^m \boldsymbol{Z}_j\right\|_F = \sup_{\|\boldsymbol{G}\|_F=1}\sum_{j=1}^m\langle\boldsymbol{Z}_j,\boldsymbol{G}\rangle = \sup_{\|\boldsymbol{G}\|_F=1}\sum_{j=1}^m g\left(\boldsymbol{Z}_j\right)$$

Since $S_F > 0$, the expected value of S_F is equal to the expected value of $\overline{S_F}$. That means $\mathbb{E}S_F = \mathbb{E}\overline{S_F}$. The absolute value of $g(\boldsymbol{Z}_j)$ can be bounded

$$|g(\boldsymbol{Z}_j)| = \left|\langle\delta_j\boldsymbol{x}_j^*\boldsymbol{y}_j,\boldsymbol{G}\rangle\right| \leq \left\|\delta_j\boldsymbol{x}_j^*\boldsymbol{y}_j\right\|_F \leq \left\|\boldsymbol{x}_j^*\boldsymbol{y}_j\right\|_F = \|\boldsymbol{x}_j\|\,\|\boldsymbol{y}_j\|$$

Hence, we can take $\eta := \max_j\|\boldsymbol{x}_j\|\max_j\|\boldsymbol{y}_j\|$. We now compute

$$\mathbb{E}g^2\left(\boldsymbol{Z}_j\right) = \mathbb{E}\delta_j\left\langle\boldsymbol{x}_j^*\boldsymbol{y}_j,\boldsymbol{G}\right\rangle^2 = \frac{d}{m}\left\langle\boldsymbol{x}_j^*\boldsymbol{y}_j,\boldsymbol{G}\right\rangle^2 \leq \frac{d}{m}\left\|\boldsymbol{x}_j^*\boldsymbol{y}_j\right\|_F^2$$

and therefore,

$$\sum_{j=1}^m \mathbb{E}g^2\left(Z_j\right) = \frac{d}{m}\sum_{j=1}^m\left\|\boldsymbol{x}_j^*\boldsymbol{y}_j\right\|_F^2 = \frac{d}{m}\sum_{j=1}^m\text{trace}\left(\boldsymbol{x}_j^*\boldsymbol{y}_j\boldsymbol{y}_j^*\boldsymbol{x}_j\right)$$

$$= \frac{d}{m}\sum_{j=1}^m\|\boldsymbol{y}_j\|^2\,\text{trace}\left(\boldsymbol{x}_j^*\boldsymbol{x}_j\right) \leq \frac{d}{m}\max_j\|\boldsymbol{y}_j\|^2\,\text{trace}\left(\sum_{j=1}^m\boldsymbol{x}_j^*\boldsymbol{x}_j\right)$$

Combine with (23) (see section 6), we conclude

$$\sum_{j=1}^m \mathbb{E}g^2\left(Z_j\right) \leq \frac{d}{m}k\max_j\|\boldsymbol{y}_j\|^2$$

Prove similarly and combine with (24), we also attain

$$\sum_{j=1}^m \mathbb{E}g^2\left(Z_j\right) \leq \frac{d}{m}\max_j\|\boldsymbol{x}_j\|^2\,\text{trace}\left(\sum_{j=1}^m\boldsymbol{y}_j^*\boldsymbol{y}_j\right) = \frac{d}{m}\alpha\max_j\|\boldsymbol{x}_j\|^2$$

So, we choose

$$\sigma^2 = \sup_{g\in\mathcal{G}}\sum_{i=1}^n\mathbb{E}g^2(Z_i) := \frac{d}{m}\max\left\{\alpha\max_j\|\boldsymbol{x}_j\|^2, k\max_j\|\boldsymbol{y}_j\|^2\right\}$$

Apply the powerful Talagrand's result (14) and note that from expectation inequality (8), $\sigma^2+\eta\mathbb{E}S_F \leq \sigma\mathbb{E}S_F+\eta\mathbb{E}S_F = \mathbb{E}^2S_F$

$$\mathbb{P}\left(S_F \geq t + \mathbb{E}S_F\right) \leq 3\exp\left(-\frac{t}{C\eta}\log\left(1 + \frac{\eta t}{\mathbb{E}^2S_F}\right)\right)$$

$$\leq 3\exp\left(-\frac{1}{C}\frac{t^2}{\mathbb{E}^2S_F}\right).$$

The last inequality comes from a simple observation that $\log(1+x) \geq 2x/3$ at $0 \leq x \leq 1$. Hence, t must be selected such that $\eta t \leq \mathbb{E}^2S_F$.

Choose $t = C\sqrt{\log\frac{3}{\beta}}\mathbb{E}S_F$ where C is a small numerical constant. By simple algebraic calculation, one can show that $\eta t \leq \mathbb{E}^2S_F$ as $d \geq C^2\mu m\log\frac{3}{\beta}$. Therefore,

$$\mathbb{P}\left(S_F \geq \left(C\sqrt{\log\frac{3}{\beta}} + 1\right)\mathbb{E}S_F\right) \leq 3\exp\left(-\log\frac{3}{\beta}\right) = \beta$$

There will exist a small constant such that $C_1\sqrt{\log\frac{3}{\beta}} = C\sqrt{\log\frac{3}{\beta}} + 1$. The proof is now concluded. $\square$

We are now ready to prove the Theorem 3

PROOF. (*Theorem 3*)

Lemmas 3 and 4 imply that with the probability at least $1-\beta$

$$\max_{1\leq j\leq m}\|\boldsymbol{x}_j\| \leq C_1\sqrt{\mu}\sqrt{\max\left\{k, \log\frac{2m}{\beta}\right\}} \quad \text{and}$$

$$\max_{1\leq j\leq m}\|\boldsymbol{y}_j\| \leq C_2\sqrt{\mu\alpha}\sqrt{\log\frac{2m}{\beta}}$$

where $C_1 \leq 5$ and $C_2 \leq 5$. We consider two cases: $k \geq \log\frac{2m}{\beta}$ and $k < \log\frac{2m}{\beta}$. For the former, define probabilistic evens

$$M = \left\{\max_{1\leq j\leq m}\|\boldsymbol{x}_j\| \leq 5\sqrt{\mu k}\right\} \quad \text{and}$$

$$N = \left\{\max_{1\leq j\leq m}\|\boldsymbol{y}_j\| \leq 5\sqrt{\mu\alpha}\sqrt{\log\frac{2m}{\beta}}\right\}$$

then from (8), suppose M and N hold, we have

$$\begin{aligned}\mathbb{E}S_F &\leq 4.56C_1C_2\mu\sqrt{\alpha}\sqrt{k\log\frac{2m}{\beta}} \\ &+ 2.56\sqrt{\frac{d}{m}}\max\left\{C_1\sqrt{\alpha}\sqrt{\mu k}, C_2k^{1/4}\sqrt{\mu\alpha\log\frac{2m}{\beta}}\right\} \\ &\leq \mu\sqrt{\alpha}\left[C_3k + C_4\sqrt{d\sqrt{k}\max\{\sqrt{k},\log\frac{2m}{\beta}\}}\right] \\ &\leq C_5\mu\sqrt{\alpha}\sqrt{d\sqrt{k}\max\{\sqrt{k},\log\frac{2m}{\beta}\}}\end{aligned}$$

where $C_3 = 4.56C_1C_2 \leq 114$, $C_4 = 2.56 * C_1 < 13$ and $C_5 = C_3 + C_4 < 127$. The second inequality follows from $\mu \geq 1/m$

We define the even

$$P = \left\{\mathbb{E}S_F \leq C_5\mu\sqrt{\alpha}\sqrt{d\sqrt{k}\max\{\sqrt{k},\log\frac{2m}{\beta}\}}\right\}$$

which occurs as both evens M and N hold.

We have $\mathbb{P}(P^c) \leq \mathbb{P}(M^c \cup N^c) \leq \mathbb{P}(M^c) + \mathbb{P}(N^c) \leq 2\beta$. Hence $\mathbb{P}(P) \geq 1 - 2\beta$.

Combine with Lemma 6 and set $C = C_5 \times C_1$, we conclude that with probability no less than $(1 - 3\beta)$

$$S_F \leq C\mu\sqrt{\alpha}\sqrt{d\sqrt{k}\max\{\sqrt{k},\log\frac{2m}{\beta}\}\log\frac{3}{\beta}}$$

Likewise, if $k < \log\frac{2m}{\beta}$, we obtain with probability at least $(1 - 3\beta)$

$$S_F \leq C\mu\sqrt{\alpha}\sqrt{d\sqrt{k}\log\frac{2m}{\beta}\log\frac{3}{\beta}}$$

Combine both condition on k, we complete the proof of Theorem 3.

□

Remark 3. It is important to compare the use of uncomplicated Markov's inequality to the beautiful Talagrand concentration measurement (Lemma 5) applied in Lemma 6. If the former is utilized, then Lemma 6 is guaranteed with a small constant probability, for instant, 1/2. This leads to the conclusion of Theorem 3 with probability 1/2. However, in this case the running time will be boosted by a logarithmic proportion of m ($\log m$) in order for the algorithm to success with extremely high probability, $1 - m^{-1}$, say (see also remark 2 for a fair comparison with other's works and how our technique is better in term of computational complexity).

5.3 Proofs of Lemma 3 and 4

In order to bound $\max_i \|x_i\|$ and $\max_i \|y_i\|$, we use a powerful result from Theorem 7.3 of [17] which strongly bound the supremum of a sum of vectors $\boldsymbol{b}_1, \boldsymbol{b}_2, ..., \boldsymbol{b}_m$ with random weights in Banach space.

Lemma 7. *Let $\{\eta_i\}_{1\leq i\leq m}$ be a sequence of independent random variable such that $\|\eta_i\| \leq 1$ almost surely with $i = 1, 2, ..., m$ and let $\boldsymbol{b}_1$, $\boldsymbol{b}_2$, ..., $\boldsymbol{b}_m$ be vectors in Banach space. Then for every $t \geq 0$,*

$$\mathbb{P}\left(\left\|\sum_{i=1}^m \eta_i\boldsymbol{b}_i\right\| \geq M + t\right) \leq 2\exp\left(-\frac{t^2}{16\sigma^2}\right), \qquad (16)$$

where M is either the mean or median of $\left\|\sum_{i=1}^m \eta_i\boldsymbol{b}_i\right\|$ and $\sigma^2 = \sup_{\|\boldsymbol{g}\|\leq 1}\sum_{i=1}^m \langle\boldsymbol{g},\boldsymbol{b}_i\rangle^2$

Lemma 7 asserts that the sum is distributed like Gaussian around its mean or median, with standard deviation $2\sqrt{2}\sigma$.

Applying Lemma 7, we can bound the maximum of $\|\boldsymbol{x}_j\|$ and $\|\boldsymbol{y}_j\|$

Proof. (*Lemma 3*) We have $\|x_j\| = \left\|\sum_{i=1}^m \epsilon_i F_{ij}\boldsymbol{u}_i\right\| = \left\|\sum_{i=1}^m \epsilon_i\boldsymbol{b}_i\right\|$ where $\boldsymbol{b}_i := F_{ij}\boldsymbol{u}_i$. The bound for σ^2 can be obtained by

$$\begin{aligned}\sigma^2 &= \sup_{\|\boldsymbol{g}\|\leq 1}\sum_{i=1}^m \langle\boldsymbol{g},\boldsymbol{b}_i\rangle^2 = \sup_{\|\boldsymbol{g}\|\leq 1}\boldsymbol{g}\left(\sum_{i=1}^m F_{ij}^*F_{ij}\boldsymbol{u}_i^*\boldsymbol{u}_i\right)\boldsymbol{g}^* \\ &\leq \mu\sup_{\|\boldsymbol{g}\|\leq 1}\boldsymbol{g}\left(\sum_{i=1}^m \boldsymbol{u}_i^*\boldsymbol{u}_i\right)\boldsymbol{g}^* = \mu\|\boldsymbol{U}_k\|^2 = \mu\end{aligned}$$

From Jensen's inequality: $\mathbb{E}Z \leq \sqrt{\mathbb{E}Z^2}$ we have that $M = \mathbb{E}\|\boldsymbol{x}_j\| \leq \sqrt{\mathbb{E}\|\boldsymbol{x}_j\|^2}$ where

$$\begin{aligned}\|\boldsymbol{x}_j\|^2 &= \sum_{i,k=1}^n \epsilon_i\epsilon_k F_{ij}^*F_{kj}\boldsymbol{u}_i^*\boldsymbol{u}_k \\ &= \sum_i \epsilon_i^2F_{ij}^*F_{ij}\boldsymbol{u}_i^*\boldsymbol{u}_i + \sum_{i\neq k}\epsilon_i\epsilon_kF_{ij}^*F_{kj}\boldsymbol{u}_i^*\boldsymbol{u}_k\end{aligned}$$

Since $\{\epsilon_i\}$ is an i.i.d Rademacher sequence, $\epsilon_i^2 = 1$ and $\mathbb{E}\epsilon_i\epsilon_k = 0$ with $i \neq k$. Hence,

$$\mathbb{E}\|\boldsymbol{x}_j\|^2 = \sum_i F_{ij}^*F_{ij}\boldsymbol{u}_i^*\boldsymbol{u}_i \leq \mu\sum_{i=1}^m \boldsymbol{u}_i^*\boldsymbol{u}_i = \mu\|\boldsymbol{U}_k\|_F^2 = \mu k$$

which leads $M \leq \sqrt{\mu k}$. Lemma 7 now gives us

$$\mathbb{P}\left(\|\boldsymbol{x}_j\| \geq M + t\right) \leq 2\exp\left(-\frac{t^2}{16\mu}\right)$$

Apply a union bound for a supremum of a random process

$$\mathbb{P}\left(\max_{1\leq j\leq m}\|\boldsymbol{x}_j\| \leq M + t\right) \leq 2m\exp\left(-\frac{t^2}{16\mu}\right)$$

By choosing $t = 4\sqrt{\mu}\sqrt{\log\frac{2m}{\beta}}$, we obtain

$$\mathbb{P}\left(\max_{1\leq j\leq m}\|\boldsymbol{x}_j\| \leq \sqrt{\mu k} + 4\sqrt{\mu}\sqrt{\log\frac{2m}{\beta}}\right) \leq 2me^{-\log\frac{2m}{\beta}} = \beta$$

The Lemma follows. □

Proof. (*Lemma 4*) Following the same line of proof as in Lemma 3 with $\boldsymbol{y}_j = \sum_{i=1}^m \epsilon_iF_{ji}\boldsymbol{h}_i$, we can obtain a upper bound for σ^2

$$\begin{aligned}\sigma^2 &= \sup_{\|\boldsymbol{g}\|=1}\sum_{i=1}^m \langle\boldsymbol{g},F_{ji}\boldsymbol{h}_i\rangle = \sup_{\|\boldsymbol{g}\|=1}\boldsymbol{g}\left(\sum_{i=1}^m F_{ji}^*F_{ji}\boldsymbol{h}_i^*\boldsymbol{h}_i\right)\boldsymbol{g}^* \\ &\leq \mu\sup_{\|\boldsymbol{g}\|=1}\boldsymbol{g}\left(\sum_{i=1}^m \boldsymbol{h}_i^*\boldsymbol{h}_i\right)\boldsymbol{g}^* = \mu\|\boldsymbol{H}^*\boldsymbol{H}\|,\end{aligned}$$

where $\boldsymbol{H}^*\boldsymbol{H} = \boldsymbol{\Sigma}_{\rho-k}^*\boldsymbol{U}_{\rho-k}^*\boldsymbol{U}_{\rho-k}\boldsymbol{\Sigma}_{\rho-k} = \boldsymbol{\Sigma}_{\rho-k}^2$. Hence,

$$\sigma^2 \leq \mu\left\|\boldsymbol{\Sigma}_{\rho-k}^2\right\| = \mu\|\boldsymbol{A} - \boldsymbol{A}_k\|^2 = \mu\delta_{k+1}^2 = \mu\frac{\alpha}{r_k},$$

and $M = \mathbb{E}\|\boldsymbol{y}_j\| \leq \sqrt{\mathbb{E}\|\boldsymbol{y}_j\|^2}$ where

$$\begin{aligned}\mathbb{E}\|\boldsymbol{y}_j\|^2 &= \sum_{i=1}^m F_{ji}^*F_{ji}\boldsymbol{h}_i^*\boldsymbol{h}_i \leq \mu\sum_{i=1}^m \boldsymbol{h}_i^*\boldsymbol{h}_i = \mu\cdot\text{trace}\left(\boldsymbol{H}^*\boldsymbol{H}\right) \\ &= \mu\cdot\text{trace}\left(\boldsymbol{\Sigma}_{\rho-k}^2\right) = \mu\|\boldsymbol{A} - \boldsymbol{A}_k\|_F^2 = \mu\alpha\end{aligned}$$

Therefore, $M \leq \sqrt{\mu\alpha}$. Apply Lemma 7 and then take the union bound for the supremum of $\|y_j\|$, we attain

$$\mathbb{P}\left(\max_{1\leq j\leq m}\|\boldsymbol{y}_j\| \leq M+t\right) \leq 2m\exp\left(-\frac{t^2}{16\mu\alpha/r_k}\right)$$

Choose $t = 4\sqrt{\frac{\mu\alpha}{r_k}}\sqrt{\log\frac{2m}{\beta}}$ and combine with $M < \sqrt{\mu\alpha}$,

$$\mathbb{P}\left(\max_{1\leq j\leq m}\|\boldsymbol{y}_j\| \geq \sqrt{\mu\alpha}+4\sqrt{\mu}\sqrt{\frac{\alpha}{r_k}}\sqrt{\log\frac{2m}{\beta}}\right) \leq 2me^{-\log\frac{2m}{\beta}} = \beta$$

The proof is now completed. $\square$

6. EXPECTATION BOUNDS

Our main arguments are mostly based on Noncommutative Khintchine inequality which bounds the Schatten norm of a sum of Rademacher series [18].

Lemma 8. ***(Noncommutative Khintchine inequality)*** *Let $\{\boldsymbol{X}_i\}$ $(1 \leq i \leq n)$ be a set of matrices of the same dimension and let $\{\epsilon_i\}$ be an independent Rademacher sequence. For each $q \geq 2$,*

$$\left(\mathbb{E}_\epsilon\left\|\sum_i \epsilon_i\boldsymbol{X}_i\right\|_{S_q}^q\right)^{1/q} \leq C_q\times$$
$$\max\left\{\left\|\left(\sum_i \boldsymbol{X}_i^*\boldsymbol{X}_i\right)^{1/2}\right\|_{S_q}, \left\|\left(\sum_i \boldsymbol{X}_i\boldsymbol{X}_i^*\right)^{1/2}\right\|_{S_q}\right\}, \tag{17}$$

where the constant $C_q \leq 2^{-1/4}\sqrt{\frac{\pi}{e}}\sqrt{q}$.

The next theorem is used to prove the expectation bound of (8). We now state a stronger result

Theorem 4. *Let $\boldsymbol{X}$ and $\boldsymbol{Y}$ be two matrices of size $m\times k_1$ and $m \times k_2$ which satisfy $\boldsymbol{X}^*\boldsymbol{Y} = 0$ and let $\{\boldsymbol{x}_i\}$ and $\{\boldsymbol{y}_i\}$ be row vectors of $\boldsymbol{X}$ and $\boldsymbol{Y}$, respectively. Denote $\{\delta_i\}$ to be a sequence of independent identically distributed $\{0/1\}$ Bernoulli random variables with $\mathbb{P}(\delta_i = 1) = \overline{\delta}$. Then at $q \geq 2$*

$$\left(\mathbb{E}_\delta\left\|\sum_i \delta_i\boldsymbol{x}_i^*\boldsymbol{y}_i\right\|_{S_q}^q\right)^{1/q} \leq 2\sqrt{2}C_q^2\max_i\|\boldsymbol{x}_i\|\max_i\|\boldsymbol{y}_i\| +$$
$$2\sqrt{\overline{\delta}}C_q\max\left\{\max_i\|\boldsymbol{x}_i\|\left\|\sum_i \boldsymbol{y}_i^*\boldsymbol{y}_i\right\|_{S_q}^{1/2}, \max_i\|\boldsymbol{y}_i\|\left\|\sum_i \boldsymbol{x}_i^*\boldsymbol{x}_i\right\|_{S_q}^{1/2}\right\}, \tag{18}$$

where the constant C_q is defined in Lemma 17.

At first, we start with a Lemma which is useful for the proof of the above Theorem

Lemma 9. *Let $\{\boldsymbol{x}_i\}_{1\leq i\leq m}$ be a set of row vectors of the same length k and denote $\{\delta_i\}$ to be a sequence of independent identically distributed $\{0/1\}$ Bernoulli random variables with $\mathbb{P}(\delta_i = 1) = \overline{\delta}$. The following inequality is satisfied*

$$\left(\mathbb{E}_\delta\left\|\sum_i \delta_i\boldsymbol{x}_i^*\boldsymbol{x}_i\right\|_{S_q}^q\right)^{1/q} \leq 2C_q^2\max_i\|\boldsymbol{x}_i\|^2 + \overline{\delta}\left\|\sum_i \boldsymbol{x}_i^*\boldsymbol{x}_i\right\|_{Sq} \tag{19}$$

where $q \geq 2$ and the constant C_q is defined in Lemma 17.

Proof. The line of proof is similar to Theorem 3.1 of Rudelson and Vershynin [19]. Let $\{\delta_i'\}$ be an independent copy of the sequence $\{\delta_i\}$. By first applying the Holder's inequality and then Jensen's inequality

$$\begin{aligned}
E_1 &= \left(\mathbb{E}_\delta\left\|\sum_i \delta_i\boldsymbol{x}_i^*\boldsymbol{x}_i\right\|_{S_q}^q\right)^{1/q} \\
&\leq \left(\mathbb{E}_\delta\left\|\sum_i \left(\delta_i-\overline{\delta}\right)\boldsymbol{x}_i^*\boldsymbol{x}_i\right\|_{S_q}^q\right)^{1/q} + \overline{\delta}\left\|\sum_i \boldsymbol{x}_i^*\boldsymbol{x}_i\right\|_{Sq} \\
&= \left(\mathbb{E}_\delta\left\|\mathbb{E}_{\delta'}\left(\sum_i \left(\delta_i-\delta_i'\right)\boldsymbol{x}_i^*\boldsymbol{x}_i\right)\right\|_{S_q}^q\right)^{1/q} + \overline{\delta}\left\|\sum_i \boldsymbol{x}_i^*\boldsymbol{x}_i\right\|_{Sq} \\
&\leq \left(\mathbb{E}_\delta\mathbb{E}_{\delta'}\left\|\sum_i \left(\delta_i-\delta_i'\right)\boldsymbol{x}_i^*\boldsymbol{x}_i\right\|_{S_q}^q\right)^{1/q} + \overline{\delta}\left\|\sum_i \boldsymbol{x}_i^*\boldsymbol{x}_i\right\|_{Sq}.
\end{aligned} \tag{20}$$

Define $\{\epsilon_i\}$ to be an independent Rademacher sequence and independent of the sequences $\{\delta_i\}$ and $\{\delta_i'\}$. Since $(\delta_i - \delta_i')$ is symmetric, $(\delta_i - \delta_i')$ has the same distribution as $\epsilon_i(\delta_i - \delta_i')$. Therefore, the first term of (20) is bounded by

$$\begin{aligned}
&\left(\mathbb{E}_\delta\mathbb{E}_{\delta'}\left\|\sum_i \left(\delta_i-\delta_i'\right)\boldsymbol{x}_i^*\boldsymbol{x}_i\right\|_{S_q}^q\right)^{1/q} \\
&= \left(\mathbb{E}_\delta\mathbb{E}_{\delta'}\mathbb{E}_\epsilon\left\|\sum_i \epsilon_i\left(\delta_i-\delta_i'\right)\boldsymbol{x}_i^*\boldsymbol{x}_i\right\|_{S_q}^q\right)^{1/q} \\
&\leq 2\left(\mathbb{E}_\delta\mathbb{E}_\epsilon\left\|\sum_i \epsilon_i\delta_i\boldsymbol{x}_i^*\boldsymbol{x}_i\right\|_{S_q}^q\right)^{1/q} = 2\left(\mathbb{E}_\delta E_2\right)^{1/q},
\end{aligned}$$

where the second inequality is followed from Holder's inequality.

Apply Khintchine inequality (17) to bound E_2, we obtain

$$\begin{aligned}
E_2 = \mathbb{E}_\epsilon\left\|\sum_i \epsilon_i\delta_i\boldsymbol{x}_i^*\boldsymbol{x}_i\right\|_{S_q}^q &\leq \left(C_q\left\|\left(\sum_i \delta_i\boldsymbol{x}_i^*\boldsymbol{x}_i\|\boldsymbol{x}_i\|^2\right)^{1/2}\right\|_{S_q}\right)^q \\
&\leq \left(C_q\left\|\sum_i \delta_i\boldsymbol{x}_i^*\boldsymbol{x}_i\|\boldsymbol{x}_i\|^2\right\|_{S_q}^{1/2}\right)^q
\end{aligned}$$

Each term $\boldsymbol{x}_i^*\boldsymbol{x}_i\|\boldsymbol{x}_i\|^2$ of the sum is positive definite, so from Weyl's result (Theorem 4.3.1 of [20]) which mentions that by adding a positive definite matrix to a positive definite matrix, all singular values will be increasing. Therefore, we can replace all the weights $\|x_j\|^2$ by $\max_j\|x_j\|^2$ and move outside the norm

$$\mathbb{E}_\epsilon\left\|\sum_i \epsilon_i\delta_i\boldsymbol{x}_i^*\boldsymbol{x}_i\right\|_{S_q}^q \leq \left(C_q\max_i\|\boldsymbol{x}_i\|\right)^q\left(\left\|\sum_i \delta_i\boldsymbol{x}_i^*\boldsymbol{x}_i\right\|_{S_q}^{1/2}\right)^q.$$

Hence,

$$
\begin{aligned}
\left(\mathbb{E}_\delta E_2\right)^{1/q} &\le C_q \max_i \|\boldsymbol{x}_i\| \left(\mathbb{E}_\delta \left\|\sum_i \delta_i \boldsymbol{x}_i^* \boldsymbol{x}_i\right\|_{S_q}^{q/2}\right)^{1/q} \\
&\le C_q \max_i \|\boldsymbol{x}_i\| \left(\left(\mathbb{E}_\delta \left\|\sum_i \delta_i \boldsymbol{x}_i^* \boldsymbol{x}_i\right\|_{S_q}^{q}\right)^{1/q}\right)^{1/2} \\
&= C_q \max_i \|\boldsymbol{x}_i\| \sqrt{\left(\mathbb{E}_\delta E_2\right)^{1/q}},
\end{aligned}
\tag{21}
$$

where the last inequality follow from $\mathbb{E}\sqrt{Z} \le \sqrt{\mathbb{E}(Z)}$.

From (21), one can see that: $\left(\mathbb{E}_\delta E_2\right)^{1/q} \le C_q^2 \max_i \|\boldsymbol{x}_i\|^2$. The Lemma 9 is now followed. □

Proof. (*Theorem 4*) As the above proof, define $\{\delta_i'\}$ as an independent copy of the sequence $\{\delta_i\}$. Since $\boldsymbol{X}^*\boldsymbol{Y} = 0$, then following similarly as the above Lemma's proof, we obtain

$$
\begin{aligned}
E1 &= \left(\mathbb{E}_\delta \left\|\sum_i \delta_i \boldsymbol{x}_i^* \boldsymbol{y}_i\right\|_{S_q}^{q}\right)^{1/q} = \left(\mathbb{E}_\delta \left\|\sum_i \left(\delta_i - \bar{\delta}\right) \boldsymbol{x}_i^* \boldsymbol{y}_i\right\|_{S_q}^{q}\right)^{1/q} \\
&= \left(\mathbb{E}_\delta \left\|\mathbb{E}_{\delta'} \left(\sum_i \left(\delta_i - \delta_i'\right) \boldsymbol{x}_i^* \boldsymbol{y}_i\right)\right\|_{S_q}^{q}\right)^{1/q} \\
&\le 2\left(\mathbb{E}_\delta \mathbb{E}_\epsilon \left\|\sum_i \epsilon_i \delta_i \boldsymbol{x}_i^* \boldsymbol{y}_i\right\|_{S_q}^{q}\right)^{1/q} = 2\left(\mathbb{E}_\delta E_2\right)^{1/q},
\end{aligned}
$$

where $\{\epsilon_i\}$ is an independent Rademacher sequence.

Applying Khintchine's inequality to E_2, we obtain

$$
E_2 \le C_q^q \max\{B_1, B_2\}^q = C_q^q \max\{B_1^q, B_2^q\}
$$

where $B_1 = \left\|\left(\sum_i \delta_i \boldsymbol{x}_i^* \boldsymbol{x}_i \|\boldsymbol{y}_i\|^2\right)^{1/2}\right\|_{S_q}$ and B_2 is defined the same as B_1 except $\boldsymbol{x}_i$ is replaced by $\boldsymbol{y}_i$. Expectation of E_2 is now bounded by

$$
\mathbb{E}_\delta E_2 \le C_q^q \mathbb{E}_\delta \left(\max\{B_1^q, B_2^q\}\right) \le C_q^q \max\{\mathbb{E}_\delta B_1^q, \mathbb{E}_\delta B_2^q\},
$$

where the second inequality follows from: $\mathbb{E}\max\{a, b\} \le \max\{\mathbb{E}a, \mathbb{E}b\}$ with nonnegative a, b. We have

$$
E1 \le 2C_q \max\left\{\left(\mathbb{E}_\delta B_1^q\right)^{1/q}, \left(\mathbb{E}_\delta B_2^q\right)^{1/q}\right\}
$$

It is sufficient to bound $(\mathbb{E}_\delta B_1^q)^{1/q}$, $(\mathbb{E}_\delta B_2^q)^{1/q}$ can be attained likewise. Also from Theorem 4.3.1 of [20], one can see that: $B_1 \le \max_i \|\boldsymbol{y}_i\| \left\|\left(\sum_i \delta_i \boldsymbol{x}_i^* \boldsymbol{x}_i\right)\right\|_{S_q}^{1/2}$. Hence,

$$
\left(\mathbb{E}_\delta B_1^q\right)^{1/q} \le \max_i \|\boldsymbol{y}_i\| \sqrt{\mathbb{E}_\delta \left\|\left(\sum_i \delta_i \boldsymbol{x}_i^* \boldsymbol{x}_i\right)\right\|_{S_q}^{1/q}} := \max_i \|\boldsymbol{y}_i\| \sqrt{E_3}
$$

where the inequality holds from $\mathbb{E}\sqrt{Z} \le \sqrt{\mathbb{E}(Z)}$.

Upper bound for $\sqrt{E_3}$ is followed from the Lemma (9), and with nonnegative a and b, $\sqrt{a+b} \le \sqrt{a} + \sqrt{b}$

$$
\sqrt{E_3} \le \sqrt{2} C_q \max_i \|\boldsymbol{x}_i\| + \sqrt{\bar{\delta}} \left\|\sum_i \boldsymbol{x}_i^* \boldsymbol{x}_i\right\|_{S_q}^{1/2}
$$

The proof is completed. □

One can observe that the first claim of the Theorem 3 is a corollary of Theorem 4. The condition $\boldsymbol{X}^*\boldsymbol{Y} = 0$ obeys since

$$
\begin{aligned}
\boldsymbol{X}^*\boldsymbol{Y} &= \sum_{i=1}^m \boldsymbol{x}_i^* \boldsymbol{y}_i = \left(\boldsymbol{U}_k^* \boldsymbol{D}^*\right)\left(\boldsymbol{F}^*\boldsymbol{F}\right)\left(\boldsymbol{D}\boldsymbol{H}\right) \\
&= \boldsymbol{U}_k^* \boldsymbol{H} = \boldsymbol{U}_k^* \boldsymbol{U}_{\rho-k} \boldsymbol{\Sigma}_{\rho-k} = 0
\end{aligned}
$$

where the third equality holds due to the orthonormality of $\boldsymbol{F}$ and $\boldsymbol{D}$ (see (3)).

We restate in a corollary.

Corollary 1. *With the same notations as in the Theorem 4. Denote $\{\delta_i\}$ to be a sequence of independent identically distributed $\{0/1\}$ Bernoulli random variables with $\mathbb{P}(\delta_i = 1) = \frac{d}{m}$. Then*

$$
\begin{aligned}
\mathbb{E}_\delta \left\|\sum_i \delta_i \boldsymbol{x}_i^* \boldsymbol{y}_i\right\|_F &\le 4.65 \max_i \|\boldsymbol{x}_i\| \max_i \|\boldsymbol{y}_i\| \\
&+ 2.56\sqrt{\frac{d}{m}} \max\left\{\sqrt{\alpha} \max_i \|\boldsymbol{x}_i\|, k^{1/4} \max_i \|\boldsymbol{y}_i\|\right\}.
\end{aligned}
\tag{22}
$$

Proof. Applying Theorem 4 to this case, one can find the equations for the expected spectral and Frobenius norm of the sums $\sum_j \boldsymbol{x}_j^* \boldsymbol{x}_j$ and $\sum_j \boldsymbol{y}_j^* \boldsymbol{y}_j$. We first compute

$$
\boldsymbol{x}_j^* \boldsymbol{x}_j = \boldsymbol{U}_k^* \boldsymbol{D}^* \boldsymbol{F}^* \boldsymbol{F} \boldsymbol{D} \boldsymbol{U}_k = \boldsymbol{U}_k^* \boldsymbol{U}_k = \boldsymbol{I}_k
$$

Hence, the spectral and Frobenius norms of this sum are as follows

$$
\left\|\sum_{j=1}^m \boldsymbol{x}_j^* \boldsymbol{x}_j\right\| = 1 \quad \text{and} \quad \left\|\sum_{j=1}^m \boldsymbol{x}_j^* \boldsymbol{x}_j\right\|_F = \sqrt{k} \tag{23}
$$

Similarly, $\sum_{j=1}^m \boldsymbol{y}_j^* \boldsymbol{y}_j = \boldsymbol{H}^*\boldsymbol{H} = \boldsymbol{V}_{\rho-k} \boldsymbol{\Sigma}_{\rho-k}^2 \boldsymbol{V}_{\rho-k}^*$. Therefore,

$$
\begin{aligned}
&\left\|\sum_{j=1}^m \boldsymbol{y}_j^* \boldsymbol{y}_j\right\| = s_{k+1}^2 \quad \text{and,} \\
&\left\|\sum_{j=1}^m \boldsymbol{y}_j \boldsymbol{y}_j^*\right\|_F = \left\|\boldsymbol{\Sigma}_{\rho-k}^2\right\|_F \le \|\boldsymbol{A} - \boldsymbol{A}_k\|_F^2 = \alpha
\end{aligned}
\tag{24}
$$

□

So far, we only consider the Schatten q-norm with $2 \le q < \infty$ of a sum of matrices with random Bernoulli weights. As $q = \infty$, the Schatten norm is the spectral norm. In the next Theorem, we derive another useful result which is analogue to the Theorem 3.1 of Rudelson and Vershynin [19]. The Theorem guarantees the invertibility of a sub-matrix which is formed from sampling a few columns (or rows) of a matrix $\boldsymbol{X}$.

Theorem 5. *Let $\{\boldsymbol{x}_i\}_{1 \le i \le m}$ be rows of a matrix $\boldsymbol{X}$ of size $m \times k$ which obeys $\boldsymbol{X}^*\boldsymbol{X} = \boldsymbol{I}$ and denote $\{\delta_i\}$ to be a sequence of independent identically distributed $\{0/1\}$ Bernoulli random variables with $\mathbb{P}(\delta_i = 1) = \bar{\delta}$. Then with $q \ge \log k$, the following inequality is satisfied*

$$
\left(\mathbb{E}_\delta \left\|I_{k \times k} - \frac{1}{\bar{\delta}} \sum_{i=1}^m \delta_i \boldsymbol{x}_i^* \boldsymbol{x}_i\right\|^q\right)^{1/q} \le C\sqrt{\frac{q}{\bar{\delta}}} \max_i \|\boldsymbol{x}_i\| \tag{25}
$$

provided that the right-hand side of (25) and the constant $C = 2^{3/4}\sqrt{\pi e} \approx 5$

PROOF. Denote E the expectation of the left-hand side. Remark that $\|\boldsymbol{X}\| \leq \|\boldsymbol{X}\|_{S_q}$, we have

$$E \leq \frac{1}{\bar{\delta}} \left(\mathbb{E}_\delta \left\| \sum_i \left(\delta_i - \bar{\delta} \right) \boldsymbol{x}_i^* \boldsymbol{x}_i \right\|_{S_q}^q \right)^{1/q}$$

Following precisely the proof of the Lemma 9 and remark that $\|\boldsymbol{X}\|_{S_q} \leq \mathrm{e} \|\boldsymbol{X}\|$ as $q \geq \log(\mathrm{rank}(\boldsymbol{X}))$, we obtain

$$\begin{aligned} E &\leq \frac{2}{\bar{\delta}} C_q \max_i \|\boldsymbol{x}_i\| \left(\left(\mathbb{E}_\delta \left\| \sum_i \delta_i \boldsymbol{x}_i^* \boldsymbol{x}_i \right\|_{S_q}^q \right)^{1/q} \right)^{1/2} \\ &\leq 2\mathrm{e} C_q \sqrt{\frac{1}{\bar{\delta}}} \max_i \|\boldsymbol{x}_i\| \left(\left(\mathbb{E}_\delta \left\| \frac{1}{\bar{\delta}} \sum_i \delta_i \boldsymbol{x}_i^* \boldsymbol{x}_i \right\|^q \right)^{1/q} \right)^{1/2} \end{aligned}$$

From the Minkowski's inequality: $(\mathbb{E}\|X+Y\|^q)^{1/q} \leq (\mathbb{E}\|X\|^q)^{1/q} + (\mathbb{E}\|X\|^q)^{1/q}$ we see that

$$\begin{aligned} \left(\mathbb{E}_\delta \left\| \frac{1}{\bar{\delta}} \sum_i \delta_i \boldsymbol{x}_i^* \boldsymbol{x}_i \right\|^q \right)^{1/q} &\leq \left(\mathbb{E}_\delta \left\| I_{k \times k} - \frac{1}{\bar{\delta}} \sum_i \delta_i \boldsymbol{x}_i^* \boldsymbol{x}_i \right\|^q \right)^{1/q} \\ &= E + 1 \end{aligned}$$

Therefore, $E \leq 2\mathrm{e} C_q \sqrt{\frac{1}{\bar{\delta}}} \max_i \|\boldsymbol{x}_i\| \sqrt{E+1}$. If $E \leq 1$, then $\sqrt{E+1} \leq \sqrt{2}$ which leads to

$$E \leq 2\sqrt{2}\mathrm{e} C_q \sqrt{\frac{1}{\bar{\delta}}} \max_i \|\boldsymbol{x}_i\|$$

provided that the right-hand side is less than 1. Substitute the value of C_q in Lemma 17, we finish the proof. □

The first claim of Theorem 2 is the exact corollary of the Theorem 5 with $\bar{\delta} = d/m$.

7. CONCLUSION

In this paper, we presented a fast and efficient algorithm for low-rank matrix approximation as well as least-square approximation. Using remarkable techniques in Banach space, we showed that our algorithm can produce a rank-k matrix approximation which achieves relative error bound in Frobenius norm. In experiments, we observe that our algorithm also obtain the relative error bound in spectral norm as singular values somehow decay in power laws. We leave the problem of how to prove this bound for future research.

Acknowledgements.
We are grateful to reviewers for valuable comments which improve overall quality of the paper.

8. REFERENCES

[1] P. Drineas, R. Kanna, and M. W. Mahoney, "Fast monte carlo algorithms for matrices ii: Computing a low-rank approximation to a matrix," *SIAM Journal on Computing*, vol. 36.

[2] G. H. Golub and C. F. V. Loan, *Matrix Computations*, Johns Hopkins University Press, Baltimore, 1983.

[3] A. Frieze, R. Kannan, and S. Vempala, "Fast monte-carlo algorithms for finding low-rank approximations," *Journal of the ACM*, vol. 51.

[4] P. Drineas, M. W. Mahoney, and S. Muthukrishna, "Subspace sampling and relative error matrix approximation: Column-based methods," *Proc. of APPROX-RANDOM*, pp. 316–326, 2006.

[5] S. Har-Peled, "Low rank matrix approximation in linear time," Manuscript.

[6] A. Deshpande and S. Vempala, "Adaptive sampling and fast low-rank matrix approximation," *Proc. of the 10th International Workshop on Randomization and Computation*, 2006.

[7] A. Deshpande, L. Rademacher, S. Vempala, and G. Wang, "Matrix approximation and projective clustering via volume sampling," *Theory of Computing*, vol. 2, pp. 225 – 247, 2006.

[8] T. Sarlós, "Improve approximation algorithms for large matrices via random projection," *Proc. of the 47th Annual IEEE Symposium on Foundations of Computer Science*, pp. 143–152, 2006.

[9] N. Ailon and B. Chazzelle, "Approximation nearest neighbors and the fast jonson-lindenstrauss transform," *Proc. of the 38th Annual ACM Symposium on Theory of Computing*, pp. 557–563, 2006.

[10] T. T. Do, T. D. Tran, and L. Gan, "Fast compressive sampling with structurally random matrices," *Proc. IEEE Int. Conf. of Acous., Speech and Signal Proc.*, pp. 3369–3372, May 2008.

[11] F. Woolfe, E. Liberty, V. Rokhlin, and M. Tygert, "A fast randomized algorithm for the approximation of matrices," UCLA University Technical report No. 1386.

[12] P. Drineas, M. W. Mahoney, S. Muthukrishnan, and T. Sarlos, "Faster least square approximation," under review, SIAM Journal on Computing, 2008.

[13] N. Ailon and E. Liberty, "Fast dimension reduction using rademacher series on dual BCH codes," *Symposium on Discrete Algorithms (SODA)*, pp. 1–9, 2008.

[14] N. Ailon and E. Liberty, "Dense fast random projections and lean walsh transforms," *Workshop on Randomization and Computation (RANDOM)*, pp. 512–522, 2008.

[15] B. Simon, *Trace Ideals and Their Applications*, American Mathematical Society, 2005.

[16] M. Talagrand, "New concentration inequalities in product space," *Inventionnes Math*, vol. 126, pp. 505–563, 1996.

[17] M. Ledoux, *The Concentration of Measure Phenomenon*, American Mathematical Society, 2001.

[18] A. Buchholz, "Operator Khintchine inequality in non-commutative probability," *Math. Annalen*, vol. 319, 2001.

[19] M. Rudelson and R. Vershynin, "Sampling from large matrices: an approach through geometric functional analysis," to appear in Journal of the ACM.

[20] R. A. Horn and C. R. Johnson, *Matrix Analysis*, Cambridge University Press, 2005.