Summary for Low-rank matrix completion

Jingwen Liang

November 2014

1 Introduction

One needs roughly rn parameters to specific an $n \times n$ matrix A of rank r. Thus it can be implied that about same number of expansion coefficients of ρ (use some fix matrix basis) are sufficiently to unique specify ρ within the set of low-rank matrices. It is by far less clear whether ρ can be recovered from this limited set of coefficients in a computationally tractable way.

1.1 3 main improvements were achieved:

1. Most importantly, the mathematical effort for obtaining near-optimal bounds on the number of coefficients needed to determine a Low-rank matrix was cut dramatically, with a condensed (but complete) version of the proof fitting on a single page.
2. the new arguments depend much less on the specific properties of the basis used.
3. In some situations, the bounds obtained are tighter than those presented previously. In some cases, the gap between lower and upper bounds is reduced to a multiplicative constant.

1.2 Question

Given that rank $(\rho) \leq r$, how many randomly chosen coefficients (w_a, ρ) do we need to know, before we can efficiently reconstruct ρ?

1.3 Algorithm

convex optimization over the space of matrices:

$$\begin{array}{ll} \min & \|\sigma\|_* \\ \text{subject to} & (w_a, \sigma) = (w_a, \rho), \qquad \forall a \in \Omega. \end{array} \tag{1}$$

1.4 Setting

1. Matrices are"Hermitian Matrix"——$\sigma^* = \sigma$;
2. ρ is the Unknow low-rank (with rank-r) matrix that we want to recover;
3. Inner product:

$$\begin{array}{ll} (\sigma_1, \sigma_2) = tr(\sigma_1^* \sigma_2) & \text{The Hilbert-Schmidt inner prodect} \\ < \psi, \phi >= \psi^* \phi & \text{The standard inner prodect in} \mathbb{C}^n; \end{array}$$

4. Ortho-normal basis $\{w_a\}_{a=1}^{n^2}$ with respect to this inner product has been chosen. Thus, ρ can be expanded as $\rho = \sum_{a=1}^{n^2} (w_a, \rho) w_a$;

5. $\Omega \subset [1, n^2]$ be a random set of size m which is roughly $O(rn)$ coordinates we have information about. $\Omega^\perp$ is the set of coordinates that we have no information;

6. σ^* is the solution of the optimization;

7. Consider $\rho = US_rU^*$, where $S_r \in \mathbb{C}^{r\times r}$, is the diagonal matrix with singular values of ρ on its diagonal. $U \in \mathbb{C}^{n\times r}$ whose colomns are orthogonal to each other if you extend U to $V = [U|U^\perp]$ then V is unitary $n \times n$ matrix, i.e. $V^*V = VV^* = \mathbb{1}$ and the singular value decomposition gives us $\rho = V\Sigma V^*$;

8. Let u_k denote the kth colomn of U, $U = \text{span}(u_1, \ldots, u_r) = \text{range } \rho$ (row space and column space of ρ)

9. P_U orthogonal projection onto range ρ. The range of ρ can be achieve by apply ρ to any vector $x \in \mathbb{C}^n$ Apply P_U on vectors in range of ρ makes no change since P_U is orthogonal projection onto range ρ.
   i.e. $\rho x \in$ range ρ.
   $P_U\rho x = P_U U\Sigma U^* x = U\Sigma U^* x = \rho x$. Thus $P_U = UU^*$.

10. $T = \{\sigma | (\mathbb{1} - P_U)\sigma(\mathbb{1} - P_U) = 0\}$ is the space of matrices whose compression to $ker\rho$ vanishes.

$$\begin{aligned}
\mathbb{1} - P_U &= \mathbb{1} - UU^* = VV^* - UU^* \\
&= \begin{bmatrix} U & U^\perp \end{bmatrix} \begin{bmatrix} U^* \\ U^{\perp *} \end{bmatrix} - UU^* \\
&= UU^* + U^\perp U^{\perp *} - UU^* \\
&= U^\perp U^{\perp *} \\
&= P_U^\perp
\end{aligned}$$

   Set T is set of matrix that is somehow "orthogonal" to ρ .Think about what kind of σ can I put in $U^\perp U^{\perp *}\sigma U^\perp U^{\perp *}$ then get 0. It is any thing that is spanned by columns of U, because $U^\perp U = 0$.
   T is the linear space spanned by elements of the form $u_k x^*$ and xu_k^*, $1 \le k \le r$ where x is arbitrary

11. $T^\perp$ the orthogonal complements of T. $T^\perp$ is the subspace of matrices spanned by the family xx^* where x is any vector orthogonal to U.

12. Orthogonal decomposition $\mathbb{R}^{n\times n} = T \oplus T^\perp$.

13. The orthogonal projection onto T is given by

$$\mathcal{P}_T(\sigma) = P_U\sigma + \sigma P_U - P_U\sigma P_U$$

   ($\mathcal{P}_T$ for matrix valued projection and P for vector valued projection)

14. The orthogonal projection onto $T^\perp$ is given by

$$\mathcal{P}_{T^\perp}(\sigma) = (\mathbb{1} - \mathcal{P}_T)(\sigma) = (\mathbb{1} - P_U)\sigma(\mathbb{1} - P_U)$$

15. decompose $\Delta = \Delta_T + \Delta_T^\perp$, with $\Delta_T \in T$, $\Delta_T^\perp \in T^\perp$.

16. $m = nr\kappa$. κ is the "oversampling factor" which describes the leverage we allow ouerselves by going beyond the minimum number of parameters needed to describe ρ

17. Let s_i be singular value of a matrix σ. The usual matrix norm are

$$\begin{aligned}
\|\sigma\|_{op} &= \max_i s_i && \text{(Operator/spectral norm)} \\
\|\sigma\|_* &= tr|\sigma| = \left(\sum_i s_i\right) && \text{(Trace norm)} \\
\|\sigma\|_F &= (\sigma, \sigma)^{1/2} = \left(\sum_i s_i^2\right)^{1/2} && \text{(Frobenius norm).}
\end{aligned} \tag{2}$$

18. Both the identity matrix and the identity function on more general spaces are denoted by $\mathbb{1}$.

19. Inequality between matrix: $\sigma_1 \preceq \sigma_2$ i.f.f. $\sigma_1 - \sigma_2$ is positive semi-definite (a convention sometimes referred to as matrix order or Löwner partinal order).

20. sign function:

    For scalar: $sgn(x) = x/|x|$ for $x \neq 0$ and $sgn(0) = 0$.

    For "Hermitian matrix": sgn (σ) is the diagonal matrix in the same basis as σ but with eigenvalues sgn (λ_i), where λ_i are the eigenvalues of σ.

21. Let $A_1, \ldots, A_m$ be m random variables taking values in $[1, n^2]$.$(A_1, \ldots, A_m \in \Omega \subset [1, n^2]$)

    The sampling operator $\mathcal{R} : \sigma \mapsto \frac{n^2}{m} \sum_{i=1}^{m} w_{A_i}(w_{A_i}, \sigma)$

2 incoherence

Definition 1 (Coherence). *The $n \times n$-matrix ρ has coherence ν with respect to an operator basis $\{w_a\}_{a=1}^{n^2}$ if either*

$$\max_a \|w_a\|_{op}^2 \leq \nu \frac{1}{n},$$

or

$$\max_a \|\mathcal{P}_T w_a\|_F^2 \leq 2\nu \frac{r}{n},$$
$$\max_a \ (w_a, \mathrm{sgn}\rho)^2 \leq \nu \frac{r}{n^2}$$

hold.

If ρ has few non-zero expansion coefficients w.r.t. the basis $\{w_a\}$, the algorithm will perform bad. We need incoherence to avoid such situation —— must ensure that a typical coefficient will contain "enough non-trivial information" about ρ.

2.1 matrix incoherence explanition

The paper find that there are certain bases with the property that ANY low-rank matrix is incoherent w.r.t them.

Matrices with small operatior norm (spectral norm) $\max_a \|w_a\|_{op}$ are "incoherent" to all low-rank matrices simultaneously.

Detial: If ρ is a matrix of rank r, normalized such that $\|\rho\|_F = 1$, then Hölder's inequality for matrices gives the estimate

$$|(w, \rho)|^2 \leq \|w\|_{op}^2 \|\rho\|_*^2 \leq \|w\|_{op}^2 r \tag{3}$$

for any matrix w. Hence the squared overlap on the left hand side is small if both r and $\|w\|$ are. As a corollary, we can actually derive $\max_a \|\mathcal{P}_T w_a\|_F^2 \leq 2\nu \frac{r}{n}$ from $\max_a \|w_a\|_{op}^2 \leq \nu \frac{1}{n}$. Indeed

$$\begin{aligned}
\|\mathcal{P}_T w_a\|_F^2 &= \sup_{\sigma \in T, \|\sigma\|_F = 1} (w_a, \sigma)^2 \\
&\leq \|w_a\|_{op}^2 \|\sigma\|_*^2 \\
&\leq \|w_a\|_{op}^2 2r \|\sigma\|_F^2 \\
&\leq 2\nu \frac{r}{n}
\end{aligned}$$

since $\max_{\sigma \in T}(\text{rank } \sigma) = 2r$. T is spanned by $U_k x^*$ and $x U^*$ which is at most the linear combination of $2r$ independent bases.

3 Main Result

Theorem 3 *Let ρ be a rank-r matrix with coherence ν with respect to an operator basis $\{w_a\}_{a=1}^{n^2}$. Let $\Omega \in [1, n^2]$ be a random set of size $|\Omega| = m \geq O(nr\nu^{(1+\beta)} \ln^2 n)$. Then the solution σ^* of the optimization problem (1) is unique and equal to ρ with probability at least $1 - n^{-\beta}$.*

$$|\Omega| = m > \log_2(2n^2\sqrt{r})64\nu(\ln(4n^2) + \ln(9\log_2 n) + \beta \ln n)rn$$

4 Intuition

Known information: space spanned by the $\{w_a | a \in \Omega\}$. There is a large affine space of matrices compatible with the available information. Goal is to specify an algorithm which picks one point from the high-dimensional affine space, and prove that our choice is identical to ρ with high probability. After used *trace heuristic* instead of lowest-rank, the objective thus becomes proving that the trace-norm restricted to the affine plane has a strict and global minimum at ρ.

If $\rho + \Delta \neq \rho$ is any matrix in the affine plane, we need to show that

$$\|\rho + \Delta\|_* > \|\rho\|_* \tag{4}$$

A short handwaving argument: *Adding a generic deviation Δ to a low-rank ρ is indeed likely to increase the trace-norm.*

Proof. Recall that the trace norm of a matrix is larger that the sum of the absolute values of the elements on the main diagonal. Let $\rho_1, \ldots, \rho_r$ be the eigenvalues of ρ. Then

$$\begin{aligned} \|\rho + \Delta\|_* &\geq \sum_{i=1}^{r} |\rho_i + \Delta_{i,i}| + \sum_{i=r+1}^{n} |\Delta_{i,i}| \\ &\geq \|\rho\|_* + \sum_{i=1}^{r} (\operatorname{sgn} \rho_i)\Delta_{i,i} + \sum_{i=r+1}^{n} |\Delta_{i,i}| \end{aligned} \tag{5}$$

For *generic* derivations Δ, we expect that the $\Delta_{i,i}$ all have comparable magnitudes. Therefore, as long as $r \ll n$, the second sum in (5) will dominate the first one as required. □

The only difficulty faced in this paper consists in proving that $\|\rho + \Delta\|_* > \|\rho\|_*$ holds not just for generic matrices $\rho + \Delta$ in the aforementioned affine plane, but for all such elements simultaneously. Key to that will be a simple concept from convex optimization theory: *a dual certificate*. By that we mean a matrix Y such that

$$\|\rho + \Delta\|_* > \|\rho\|_* + (Y, \Delta) \tag{6}$$

For $\Delta \neq 0$. If we can find such a Y which is also normal to the affine space, then the inner prodect above vanishes and $\|\rho + \Delta\|_* > \|\rho\|_* + (Y, \Delta)$ implies $\|\rho + \Delta\|_* > \|\rho\|_*$.

5 Main Proof

5.1 *The ensemble*

1. Let $A_1, \ldots, A_m$ be random variables taking values in $[1, n^2]$ with distribution specified momentarily.
2. w_{A_i} — random matrices
3. sampling operator:

$$\mathcal{R} : \sigma \mapsto \frac{n^2}{m} \sum_{i=1}^{m} w_{A_i}(w_{A_i}, \sigma) \tag{7}$$

4. analyze the semi-definite program

$$\begin{array}{ll} \min & \|\sigma\|_* \\ \text{subject to} & \mathcal{R}\sigma = \mathcal{R}\rho \end{array} \tag{8}$$

5. **Two type of solutions** The solution σ^* to

$$\begin{array}{ll} \min & \|\sigma\|_* \\ \text{subject to} & \mathcal{R}\sigma = \mathcal{R}\rho \end{array} \tag{9}$$

is unique and equal to ρ if and only if any non-zero deviation $\Delta = \sigma - \rho$ from ρ is eigher *infeasible*

$$\mathcal{R}\Delta \neq 0, \tag{10}$$

or causes the trace-norm to increase

$$\|\rho + \Delta\|_* > \|\rho\|_* \tag{11}$$

6. **Sample *without* replacement:** If the A_i's correspond to m samples drawn frmo $[1, n^2]$ *without* replacement, the programs

$$\begin{array}{ll} \min & \|\sigma\|_* \\ \text{subject to} & (\sigma, w_a) = (\rho, w_a), \qquad \forall a \in \Omega. \end{array} \tag{12}$$

and

$$\begin{array}{ll} \min & \|\sigma\|_* \\ \text{subject to} & \mathcal{R}\sigma = \mathcal{R}\rho \end{array} \tag{13}$$

are equivalent.

7. **Sample *with* replacement; collisions:** Consider A_i's are i.i.d. random variables. Due to independent, the situation is much easier to analze, but also imples the possibility of *collisions*. In the presence of collision, fewer than m distinct coefficients will contribute to (8). And thus plausible that any upper bound on the probability of failure of the i.i.d. scheme is also valid for *no replacement* situation.

   Thus, we can assume A_i's are i.i.d random variables.

   Using (10)$\mathcal{R}\Delta \neq 0$, we can give a simple proof of our earlier remark that sampleing with replacement can only decrease that probability of recovering ρ:

Proof. Let $p_{with}(m)$, $p_{wout}(m)$ be the prohabilities that the solution of (9) equals ρ, if the $A_*, \ldots, A_m$ are sampled, respectively, with or without replacement.

Let $\mathcal{R}'$ be defined as in (7), but with the sum extending only over distinct samples $A_i \neq A_j$ (denote the number of distince samples by m'). Then $ker\mathcal{R}' = ker\mathcal{R}$, and consequently (10) is true for $\mathcal{R}$ if and only if it is true for $\mathcal{R}'$.

Thus, the probability that the solution to (9) equals ρ is the same as the probability that the solution of

$$\min\|\sigma\|_* \qquad \text{subject to} \quad \mathcal{R}'\sigma = \mathcal{R}'\rho \tag{14}$$

equals ρ. But conditioned on any value of m', the distribution of $\mathcal{R}'$ is the same as the distribution of a sampling operator drawing m' basis elements without replacement. Hence

$$p_{with}(m) = \mathbb{E}_{m'}[p_{wout(m')}] \leq p_{wout}(m), \tag{15}$$

since $m' \leq m$ and clearly $p_{wout}(m') \leq p_{wout}(m)$ □

The i.i.d. scheme v.s. the "Bernoulli model":

iid model	bernoulli model
(w_{A_i}, ρ) are i.i.d.	$a \in [1, n^2]$ is included in Ω with probabiliry m/n^2
never obtains knowledte of more than m coefficients	can get knowledge of more tnan m coefficients
collisions has some tachnical drawbacks	

drawbacks for collosions: e.g. $\mathcal{R}$ will not be proportional to a projection.

5.2 Further layout of proof

1. In section I show that Δ is infeasible(fulfills (10)) as soon as $\|\Delta_T\|_F$ is"much larger" than $\|\Delta_T^{\perp}\|_F$
2. In section II show operator large deviation bounds
3. In section III show that $\|\rho+\Delta\|_* > \|\rho\|_* + (\text{sgn}\ \rho + \text{sgn}\ \Delta_T^{\perp}, \Delta)$. Thus as long as the scalar product on the r.h.s. is positive (not vanish), we conclude that Δ fulfells (11) $\|\rho+\Delta\|_* > \|\rho\|_*$. Then we use a powerful idea "Dual Certificate".

   More precisely it is shown that the aforementioned scalar product is guaranteed to be positive, as long as there is a matrix $Y \in \text{range}\ (\mathcal{R})$ such that

   (i) $\mathcal{P}_T Y$ is close to sgn (ρ), and

   (ii) $\|\mathcal{P}_T^{\perp} Y\|_{op}$ is small.
4. ** In section IV we establishes the existence of a certificate Y in the case of bases with small operator norm.
5. In section V we modified the previous work with any operator basis. (This complete the main results proof).
6. In section VI and VII, we introduce some matingale techniques and put them to use to drive tighter bounds.
7. In section VIII deals with non-Hermitian matrices.

5.3 *I. First case: large* Δ_T

In this section, we show that Δ is infeasible (with high probability) if $\|\Delta_T\|_F$ is much larger that $\|\Delta_T^{\perp}\|_F$. If $\|\mathcal{R}\Delta_T\|_F > \|\mathcal{R}\Delta_T^{\perp}\|_F$,then

$$\|\mathcal{R}\Delta\|_F = \|\mathcal{R}\Delta_T + \mathcal{R}\Delta_T^{\perp}\|_F \geq \|\mathcal{R}\Delta_T\|_F - \|\mathcal{R}\Delta_T^{\perp}\|_F > 0 \text{ (triangle inequality)}$$

To find criteria for this situation to occur, we need to put a lower bound on $\|\mathcal{R}\Delta_T\|_F$ and a upper bound on $\|\mathcal{R}\Delta_T^{\perp}\|_F$.

Upper bound on $\|\mathcal{R}_T^{\perp}\|_F$***:***

$$\|\mathcal{R}\Delta_T^{\perp}\|_F^2 = (\mathcal{R}\Delta_T^{\perp}, \mathcal{R}\Delta_T^{\perp}) \leq \|\mathcal{R}\|_{op}^2 \|\Delta_T^{\perp}\|_F^2 \tag{16}$$

It is easy to see that $\|\mathcal{R}\|_{op} = \frac{n^2}{m} C$, where $C := max_i|\{j|A_i = A_j\}|$, the highest number of collisions. And $C < m$ is certainly true. Since

$$\mathcal{R} : \sigma \mapsto \frac{n^2}{m} \sum_{i=1}^{m} (w_{A_i}, \sigma) w_{A_i}$$

$$\sigma \mapsto w_{A_i}, \sigma)$$

$$\sigma \mapsto (\overrightarrow{w}_{A_i}, \overrightarrow{\sigma})_{l_2{}^{n^2}}$$

$$\begin{array}{l} (\overrightarrow{w}_{A_1}, \overrightarrow{\sigma}) \\ (\overrightarrow{w}_{A_2}, \overrightarrow{\sigma}) \\ (\overrightarrow{w}_{A_3}, \overrightarrow{\sigma}) \qquad \Rightarrow \qquad W\overrightarrow{\sigma} \\ \cdots \\ (\overrightarrow{w}_{A_m}, \overrightarrow{\sigma}) \end{array}$$

Where W is $m \times n^2$ matrix. Thus $\mathcal{R} : \sigma \mapsto \frac{n^2}{m} W^* W \sigma$. Thus $\|\mathcal{R}\|_{op} = \frac{n^2}{m} C$

Hence we have

$$\|\mathcal{R}\Delta_T^{\perp}\|_F^2 \leq \|\mathcal{R}\|_{op}^2\|\Delta_T^{\perp}\|_F^2 = \frac{n^4}{m^2}C^2\|\Delta_T^{\perp}\|_F^2 \leq \frac{n^4}{m^2}m^2\|\Delta_T^{\perp}\|_F^2 \leq n^4\|\Delta_T^{\perp}\|_F^2$$

and thus

$$\|\mathcal{R}\Delta_T^{\perp}\|_F \leq n^2\|\Delta_T^{\perp}\|_F \tag{17}$$

Lower bound of $\|\mathcal{R}_T\|$:
Likewise,

$$\begin{aligned}
\|\mathcal{R}\Delta_T\|_F^2 &= (\mathcal{R}\Delta_T, \mathcal{R}\Delta_T) = (\frac{n^2}{m}W^*W\overrightarrow{\sigma}, \frac{n^2}{m}W^*W\overrightarrow{\sigma}) \\
&= \left(\frac{n^2}{m}\right)^2 \overrightarrow{\sigma}^*W^*WW^*W\overrightarrow{\sigma} \\
&= \left(\frac{n^2}{m}\right)^2 \overrightarrow{\sigma}^*W^*(I+H)W\overrightarrow{\sigma} \\
&= \left(\frac{n^2}{m}\right)^2 \overrightarrow{\sigma}^*W^*W\overrightarrow{\sigma} + \left(\frac{n^2}{m}\right)^2 \overrightarrow{\sigma}^*W^*HW\overrightarrow{\sigma} \\
&\leq \left(\frac{n^2}{m}\right)^2 \overrightarrow{\sigma}^*W^*W\overrightarrow{\sigma} \\
&= \frac{n^2}{m}(\Delta_T, \mathcal{R}\Delta_T) \\
&= \frac{n^2}{m}(\mathcal{P}_T\Delta_T, \mathcal{R}\mathcal{P}_T\Delta) \\
&= \frac{n^2}{m}(\Delta_T, \mathcal{P}_T\mathcal{R}\mathcal{P}_T\Delta_T) \\
&= \frac{n^2}{m}(\Delta_T, (\mathbb{1} - \mathbb{1} + \mathcal{P}_T\mathcal{R}\mathcal{P}_T)\Delta_T) \\
&= \frac{n^2}{m}(\Delta_T, \Delta_T) - (\Delta_T, (\mathbb{1} - \mathcal{P}_T\mathcal{R}\mathcal{P}_T)\Delta_T) \\
&\geq \frac{n^2}{m}(\|\Delta_T\|_F^2 - (\Delta_T, (\mathcal{P}_T + \mathcal{P}_T^{\perp} - \mathcal{P}_T\mathcal{R}\mathcal{P}_T)\Delta_T)) \\
&= \frac{n^2}{m}(\|\Delta_T\|_F^2 - (\Delta_T, (\mathcal{P}_T - \mathcal{P}_T\mathcal{R}\mathcal{P}_T)\Delta_T)) \\
&\geq \frac{n^2}{m}(\|\Delta_T\|_F^2 - \|\mathcal{P}_T - \mathcal{P}_T\mathcal{R}\mathcal{P}_T\|_{op}\|\Delta\|_F^2) \\
&= \frac{n^2}{m}(1 - \|\mathcal{P}_T - \mathcal{P}_T\mathcal{R}\mathcal{P}_T\|_{op})\|\Delta_T\|_F^2
\end{aligned} \tag{18}$$

$\mathcal{P}_{A_i}$ be the orthogonal projection onto w_{A_i}.
Since the matrices $\{w_a\}$ form an ortho - normal basis by defination, then:

$$\mathbb{E}[\mathcal{R}] = \frac{n^2}{m}\sum_{i=1}^{m}\mathbb{E}[\mathcal{P}_{A_i}] = \mathbb{1}$$

Thus follows

$$\mathbb{E}[\mathcal{P}_T\mathcal{R}\mathcal{P}_T] = \mathcal{P}_T\mathbb{1}\mathcal{P}_T = \mathcal{P}_T\mathcal{P}_T = \mathcal{P}_T$$

In order to evaluate (18) i.e. $\|\mathcal{R}\Delta_T\|_F^2 \geq \frac{n^2}{m}(1 - \|\mathcal{P}_T - \mathcal{P}_T\mathcal{R}\mathcal{P}_T\|_{op})\|\Delta_T\|_F^2$, we need to bound the deviation of $\mathcal{P}_T\mathcal{R}\mathcal{P}_T$ from its expectation $\mathcal{P}_T$ in operator norm for small m.

Lemma 5. *It holds that*

$$\mathbb{P}[\|\mathcal{P}_T\mathcal{R}\mathcal{P}_T - \mathcal{P}_T\|_{op} \geq t] \leq 4nr \exp\left(-\frac{t^2\kappa}{8\nu}\right) \tag{19}$$

for all $t < 2$.

We assume that $t = 1/2$ in the following.

Let $p_1 :=$ the probability of that event not occurring. Then using (17)(18) i.e.
$\|\mathcal{R}\Delta_T^{\perp}\|_F \leq n^2\|\Delta_T^{\perp}\|_F$ and
$\|\mathcal{R}\Delta_T\|_F^2 \geq (1 - \|\mathcal{P}_T - \mathcal{P}_T\mathcal{R}\mathcal{P}_T\|_{op})\|\Delta_T\|_F^2$
We have that $\mathcal{R}\Delta \neq 0$ if

$$\frac{n^2}{m}\|\Delta_T\|_F^2 \geq n^4\|\Delta_T^{\perp}\|_F^2$$
$$\Leftrightarrow \|\Delta_T\|_F^2 \geq 2mn^2\|\Delta_T^{\perp}\|_F^2$$

For the later sections, it is thus sufficient to treat the case of

$$\|\Delta_T\|_F < \sqrt{2mn}\|\Delta_T^{\perp}\|_F < n^2\|\Delta_T^{\perp}\|_F \tag{20}$$

5.4 *II. Operator large deviation bounds*

The basic recipe of this part is: Take a textbook proof of Bernstein's inequality and substitute all inequalities between real numbers by matrix inequalities(in the sense of matrix order)

Basic Markov-inequality:

Let Θ be the "operator step function" define by:

$$\Theta(\sigma) = \begin{cases} 0 & \sigma \prec \mathbb{1} \\ 1 & \sigma \not\preceq \mathbb{1} \end{cases}$$

If σ is positive semi-define, the trivial estimate $\Theta(\sigma) \leq tr(\sigma)$. Thus for any number $\lambda > 0$ and matrix-valued random variable S:

$$\begin{aligned} \mathbb{P}[S \not\preceq t\mathbb{1}] &= \mathbb{P}\left[S - t\mathbb{1} \not\preceq 0\right] \\ &= \mathbb{P}\left[e^{\lambda S - \lambda t\mathbb{1}} \not\preceq \mathbb{1}\right] \\ &= \mathbb{E}\left[\Theta(e^{\lambda S - \lambda t\mathbb{1}})\right] \\ &\leq \mathbb{E}\left[tr(e^{\lambda S - \lambda t\mathbb{1}}\right] \\ &= e^{-\lambda t}\mathbb{E}\left[tr(e^{\lambda S})\right] \end{aligned} \tag{21}$$

Now let X be an operator-valued r.v., X_i be i.i.d. copies of X, and $S = \sum_i^m X_i$. Then

$$\begin{aligned}
& \mathbb{E}\left[tr\exp\left(\lambda\sum_i^m X_i\right)\right] \\
\leq\ & \mathbb{E}\left[tr\exp\left(\lambda\sum_i^{m-1} X_i\right)\exp\left(\lambda X_m\right)\right] \\
=\ & tr\left(\mathbb{E}\left[\exp\left(\lambda\sum_i^{m-1} X_i\right)\right]\mathbb{E}\left[\exp(\lambda X)\right]\right) \\
=\ & tr\left(\mathbb{E}\left[\exp\left(\lambda\sum_i^{m-1} X_i\right)\right]T\Lambda T'\right) \text{ eigenvalue decomposation} \\
=\ & tr\left(\mathbb{E}\left[\exp\left(\lambda\sum_i^{m-1} X_i\right)\right]T\Lambda\right) \quad \text{unitery matrix T' is invariant under trace} \\
=\ & tr\left(\Lambda\mathbb{E}\left[\exp\left(\lambda\sum_i^{m-1} X_i\right)\right]T\right) \quad \text{change orter under trace} \\
=\ & tr\left(\Lambda\mathbb{E}\left[\exp\left(\lambda\sum_i^{m-1} X_i\right)\right]\right) \quad \text{unitery matrix T' is invariant under trace} \\
\leq\ & \mathbb{E}\left[tr\exp\left(\lambda\sum_i^{m-1} X_i\right)\right]\|\mathbb{E}[\exp(\lambda X)]\|_{op} \quad \text{bounded by the largest singular value} \\
\leq\ & \dots \\
\leq\ & \mathbb{E}[tr\exp(\lambda X_1)]\|\mathbb{E}[\exp(\lambda X)]\|_{op}^{m-1} \\
\leq\ & \|\mathbb{E}[e^{\lambda X}]\|_{op}^m
\end{aligned} \tag{22}$$

, where the second line is the Colden-Thompson inequality.

We use a Bernstein-type estimate bounding Eq.(22) by the second moments of the X_i.

Indeed, assume that $\mathbb{E}[Y] = 0$ and $\|Y\|_{op} \leq 1$ for some random variable Y. Recall the standard estimate

$$1 + y \leq e^y \leq 1 + y + y^2$$

valid for real numbers $y \in [-1, 1]$(and,strictly speaking, a bit beyond). From the upper bound, we get $e^Y \leq \mathbb{1} + Y + Y^2$, as both sides of the inequality are simultaneously diagonalizable. Taking expectation and employing the lower bound:

$$\mathbb{E}[e^Y] \leq \mathbb{1} + \mathbb{E}[Y^2] \leq \exp(\mathbb{E}[Y^2]), \tag{23}$$

and thus $\|\mathbb{E}[e^Y]\| \leq \|\exp(\mathbb{E}[Y^2])\| = \exp(\|\mathbb{E}[Y^2]\|)$.

Lemma 6 (Operator-Bernstein inequality). *Let $X_i, \quad i = 1, \dots, m$ be i.i.d., zero-mean, Hermitian matrix-valued random variables. Assume $V_0, c \in \mathbb{R}$ are such that $\|E[X_i^2]\|_{op} \leq V_0^2$ and $\|X_i\|_{op} \leq c$. Set $S = \sum_{i=1}^m X_i$ and let $V = mV_o^2$ (an upper bound to the variance of S). Then*

$$\mathbb{P}\left[\|S\|_{op} > t\right] \leq 2n\exp\left(-\frac{t^2}{4V}\right), \tag{24}$$

for $t \leq 2V/c$, and

$$\mathbb{P}[\|S\|_{op} > t] \leq 2n\exp\left(-\frac{t}{2c}\right), \tag{25}$$

for larger values of t.

The second equation (25) will be used only once, in section VII.

Proof. Combine Eq. (21,22,23) to get the estimate

$$\mathbb{P}[S \not\preceq t\mathbb{1}] \leq n \exp(-\lambda t + \lambda^2 m V_0^2).$$

Let $s = t/V$ be the deviation in units of V. Then

$$\mathbb{P}[S \not\preceq t\mathbb{1}] \leq n \exp(-\lambda s V + \lambda^2 V^2).$$

Choose $\lambda = s/(2V)$. The exponent becomes

$$-s^2/2 + s^2/4 = -s^2/4$$

valid as long as $\lambda \|X\|_{op} \leq 1$, which is certainly fulfilled if

$$s \leq \frac{2V}{c} \tag{26}$$

If (26) does not hold, set $\lambda = 1/c$ and compute for the exponent

$$-sV/c + V^2/c^2 = -sV/(2c) - (sV/(2c) - V^2/c^2) < -sV/(2c) = -t/(2c).$$

The same estimates hold for $-S$, giving the advertised bound with the factor of 2 coming from the union bound)which is also known as Bool's inequality: the probabiliry of ar least one of a set of events occurring is not larger than the sum of their individual probabiliries).

□

Thus the we are able to prove Lemma 5, which claimed that

$$\mathbb{P}[\|\mathcal{P}_T \mathcal{R} \mathcal{P}_T - \mathcal{P}_T\|_{op} \geq t] \leq 4nr \exp\left(-\frac{t^2 \kappa}{8\nu}\right)$$

for all $t < 2$.

Proof. (*of lemma 5*) For $a \in [1, n^2]$, let$\mathcal{P}_a$ be the orthogonal projection onto w_a. We define a family of linear operators Z_a by

$$Z_a := \frac{n^2}{m} \mathcal{P}_T \mathcal{P}_a \mathcal{P}_T.$$

Then

$$\mathcal{P}_T \mathcal{R} \mathcal{P}_T = \sum_{i=1}^{m} Z_{A_i}.$$

Since $\mathbb{E}[Z_{A_i}] = \frac{1}{m}\mathcal{P}_T$ the operator whose norm we want to bound can be written as

$$\mathcal{P}_T \mathcal{R} \mathcal{P}_T - \mathcal{P}_T = \sum_{i=1}^{m} (Z_{A_i} - \mathbb{E}[Z_{A_i}]).$$

We will thus apply the Operator Bernstein inequality to the random variables $X_{A_i} := Z_{A_i} - \mathbb{E}[Z_{A_i}]$. To this end, we need to estimate the constant V_0^2, c appearing in Theorem 6. Compute:

$$\begin{aligned}
\mathbb{E}[Z_{A_i}^2] &= (\frac{n^2}{m})^2 \mathbb{E}[\mathcal{P}_T \mathcal{P}_{A_i} \mathcal{P}_T^2 \mathcal{P}_{A_i} \mathcal{P}_T] \\
&= (\frac{n^2}{m})^2 \mathbb{E}[\mathcal{P}_T |w_{A_i}><w_{A_i}| \mathcal{P}_T |w_{A_i}><w_{A_i}| \mathcal{P}_T] \\
&= (\frac{n^2}{m})^2 \mathbb{E}[|\mathcal{P}_T w_{A_i}><w_{A_i}, \mathcal{P}_T w_{A_i}><w_{A_i} \mathcal{P}_T|] \\
&= (\frac{n^2}{m})^2 \mathbb{E}[<w_{A_i}, \mathcal{P}_T w_{A_i}> |\mathcal{P}_T w_{A_i}><w_{A_i} \mathcal{P}_T|] \\
&= (\frac{n^2}{m})^2 \mathbb{E}[(w_{A_i}, \mathcal{P}_T w_{A_i}) Z_{A_i}].
\end{aligned} \tag{27}$$

where $\mathcal{P}_{A_i} = |w_{A_i} >< w_{A_i}|$

From the properity of incoherence $\max_a \|w_a\|_{op}^2 \leq \nu\frac{1}{n}$, we have $(w_{A_i}, \mathcal{P}_T w_{A_i}) \leq \frac{2\nu r}{n}$, and thus

$$\mathbb{E}[Z_{A_i}^2] \leq \frac{n^2}{m}\frac{2\nu r}{n}\mathbb{E}[Z_{A_i}] = \frac{2n\nu r}{m^2}\mathcal{P}_T.$$

Having used that $Z_{A_i} \not\prec 0$. Hence

$$\begin{aligned}\|\mathbb{E}[X_{A_i}^2]\|_{op} &= \|\mathbb{E}[Z_{A_i}^2] - (\mathbb{E}[Z_{A_i}])^2\|_{op} \\ &\leq \frac{2n\nu r - 1}{m^2}\|\mathcal{P}_T\|_{op} \\ &\leq \frac{2n\nu r}{m^2} = \frac{2\nu}{m\kappa} =: V_0^2\end{aligned}$$

Next:

$$\begin{aligned}\|X_{A_i}\|_{op} &= \frac{1}{m}\|n^2\mathcal{P}_T\mathcal{P}_{A_i}\mathcal{P}_T - \mathcal{P}_T\|_{op} \\ &\leq \frac{1}{m}\|n^2\mathcal{P}_T\mathcal{P}_{A_i}\mathcal{P}_T\|_{op} \\ &= \frac{n^2}{m}\|\mathcal{P}_T w_{A_i}\|_F^2 \\ &\leq \frac{n^2}{m}2\nu\frac{r}{n} = \frac{2\nu nr}{m} = \frac{2\nu}{\kappa} =: c,\end{aligned}$$

So that

$$2nV_0^2\frac{1}{\|X_{A_i}\|_{op}} \geq \frac{2m\nu nr}{m^2}\frac{\kappa}{\nu} = \frac{2\kappa nr}{m} = 2$$

The claim follows from Theorem 6. After applied theorem 6, we got coefficient as 2n. No idea where comes 4nr in the theorem 5 □

5.5 *III. Second case: small* Δ_T

In this section, we will show that

$$\|\Delta_T\|_F < n^2\|\Delta_T^\perp\|_F, \tag{28}$$

$$\Delta \in range(\mathcal{R}^\perp) \tag{29}$$

together imply $\|\rho + \Delta\|_* > \|\rho\|_*$, if we can find a "certificate" $Y \in range(\mathcal{R})$ with certain properties.

Set $U = range(\rho)$ and let P_U be the orthogonal projection onto U. We will make repeated use of the basic identity

$$\|\sigma\|_* = tr|\sigma| = tr((\text{sgn }(\sigma))\sigma) = (\text{sgn}(\sigma), \sigma).$$

Since for hermitian matrix, $s_i = |\lambda_i|$

We then find

$$
\begin{aligned}
& \|\rho+\Delta\|_* \\
\geq\ & \|P_U(\rho+\Delta)P_U\|_* + \|P_U^\perp(\rho+\Delta)P_U^\perp\|_* \qquad \text{(pinching inequality)} \qquad (30)\\
=\ & \|UU^*U\Sigma U^*UU^* + P_U\Delta P_U\|_* + \|P_U^\perp\rho P_U^\perp + P_U^\perp\Delta P_U^\perp\|_* \\
=\ & \|\rho + P_U\Delta P_U\|_* + \|(\mathbb{1}-P_U)\Delta(\mathbb{1}-P_U)\|_* \\
=\ & \|\rho + P_U\Delta P_U\|_* + \|\Delta - P_U\Delta - \Delta P_U + P_U\Delta P_U\|_* \\
=\ & \|\rho + P_U\Delta P_U\|_* + \|\Delta - \mathcal{P}_T\Delta\|_* \\
=\ & \|\rho + P_U\Delta P_U\|_* + \|(\mathbb{1}-\mathcal{P}_T)\Delta\|_* \\
=\ & \|\rho + P_U\Delta P_U\|_* + \|\mathcal{P}_T^\perp\Delta\|_* \\
=\ & \|\rho + P_U\Delta P_U\|_* + \|\Delta_T^\perp\|_* \\
=\ & \|\text{sgn }\rho\|_{op}\|\rho + P_U\Delta P_U\|_* + (\text{sgn }\Delta_T^\perp, \Delta_T^\perp) \\
\geq\ & (\text{sgn }\rho, \rho + P_U\Delta P_U) + (\text{sgn }\Delta_T^\perp, \Delta_T^\perp) \qquad \text{(holder's inequality)} \qquad (31)\\
=\ & \|\rho\|_* + (\text{sgn }\rho, P_U\Delta P_U) + (\text{sgn }\Delta_T^\perp, \Delta_T^\perp) \\
=\ & \|\rho\|_* + (P_U\text{sgn }\rho P_U, \Delta) + (\text{sgn }\Delta_T^\perp, \Delta_T + \Delta_T^\perp) \\
=\ & \|\rho\|_* + (\text{sgn }\rho, \Delta) + (\text{sgn }\Delta_T^\perp, \Delta) \\
=\ & \|\rho\|_* + (\text{sgn }\rho + \text{sgn }\Delta_T^\perp, \Delta) \qquad (32)
\end{aligned}
$$

The estimate (30) is sometimes known as the "pinching inequality", and in line (31) we used Holder's inequality.

Pinching Inequality: All unitary invariant norms are reduced by pinchings. If $P_1, \ldots, P_k$ are mutually orthogonal projections, such that $P_1 \oplus P_2 \oplus \cdots \oplus P_k = \mathbb{1}$ then the operator on $\mathcal{M}_n$ defines as

$$\mathcal{C}(A) = \sum_{i=1}^{k} P_i A P_i$$

is called a pinching operator. It is easy to see that

$$|||\mathcal{C}(A)||| \leq |||A|||$$

for every unitary invariant norm. We will call this the pinching inequality.

To conclude that $\|\rho+\Delta\|_* > \|\rho\|_*$, it is hence sufficient to show that $(\text{sgn }\rho + \text{sgn }\Delta_T^\perp), \Delta > 0$. Choose any $Y \in range(\mathcal{R})$. Using (29):

$$(\text{sgn }\rho + \text{sgn }\Delta_T^\perp, \Delta) = (\text{sgn }\rho + \text{sgn }\Delta_T^\perp - Y, \Delta) \qquad (33)$$

Since $Y \perp \Delta$.

Assume that Y fulfills

$$\|\mathcal{P}_T Y - \text{sgn }\rho\|_F \leq \frac{1}{2n^2}, \qquad \|\mathcal{P}_T^\perp Y\|_{op} \leq \frac{1}{2} \qquad (34)$$

Then (33) becomes

$$
\begin{aligned}
& (\text{sgn }\rho + \text{sgn }\Delta_T^\perp - Y, \Delta) \\
=\ & (\text{sgn }\rho - Y, \Delta_T) + (\text{sgn }\Delta_T^\perp - Y, \Delta_T^\perp) \\
\geq\ & -\frac{1}{2n^2}\|\Delta_T\|_F + \frac{1}{2}\|\Delta_T^\perp\|_* \\
\geq\ & -\frac{1}{2n^2}\|\Delta_T\|_F + \frac{1}{2}\|\Delta_T^\perp\|_F \\
\geq\ & \frac{1}{4}\|\Delta_T^\perp\|_F
\end{aligned}
$$

Using holder's inequality:

$$\begin{aligned}
& (\text{sgn } \rho - Y, \Delta_T) \\
= \; & (\text{sgn } \rho - \mathcal{P}_T Y - \mathcal{P}_T^{\perp} Y, \Delta_T) \\
= \; & (\text{sgn } \rho - \mathcal{P}_T Y, \Delta_T) \\
= \; & -(\mathcal{P}_T Y - \text{sgn } \rho, \Delta_T) \\
\geq \; & -\|\mathcal{P}_T Y - \text{sgn } \rho\|_F \|\Delta_T\|_F \\
\geq \; & -\frac{1}{2n^2}\|\Delta_T\|_F
\end{aligned}$$

$$\begin{aligned}
& (Y - \text{sgn } \Delta_T^{\perp}, \Delta_T^{\perp}) \\
= \; & (\mathcal{P}_T Y + \mathcal{P}_T^{\perp} Y - \text{sgn } \Delta_T^{\perp}, \Delta_T^{\perp}) \\
= \; & (\mathcal{P}_T^{\perp} Y - \text{sgn } \Delta_T^{\perp}, \Delta_T^{\perp}) \\
= \; & (\mathcal{P}_T^{\perp} Y, \Delta_T^{\perp}) - \|\Delta_T^{\perp}\|_* \\
\leq \; & \|\mathcal{P}_T^{\perp} Y\|_{op} \|\Delta_T^{\perp}\|_* - \|\Delta_T^{\perp}\|_* \\
\leq \; & \frac{1}{2}\|\Delta_T^{\perp}\|_* - \|\Delta\|_* \\
= \; & -\frac{1}{2}\|\Delta_T^{\perp}\|_*
\end{aligned}$$

We summarize. Assume there is a certificate $Y \in range(\mathcal{R})$ fulfilling (34). Let σ^* be the solution of the optimization problem, let $\Delta^* = \rho - \sigma^*$. Then Δ^* must fulfill (29), for else it would be unfeasible. It must also fulfill (28), by section III

But then, from the previous calculation $(\Delta^*)_T^{\perp}$ must be zero, as otherwise $\|\sigma^*\|_* > \|\rho\|_*$. This implies that $(\Delta^*)_T$ is also zero, again using (28). So Δ^* is zero, and therefore $\sigma^* = \rho$ is the unique solution to (9).

It remains to prove the existence of the certificate Y.

5.6 *IV. The certificate: bases of Fourier type*

In this section, we construct a $Y \in range\mathcal{R}$ with

$$\|\mathcal{P}_T Y - \text{sgn } (\rho)\|_F \leq \frac{1}{2n^2}, \qquad \|\mathcal{P}_T^{\perp} Y\|_{op} \leq \frac{1}{2} \tag{35}$$

assuming that $max_a \|w_a\|_{op}^2 \leq \frac{\nu}{n}$. A modified proof valid in the general case will be given in next section. We present a strongly simplified proof using two key ideas: a further application of the operator Bernstein inequality; and a certain, recursive random process which quickly converges to the sought- for Y.

5.6.1 *Intuition:*

A first, natural ansatz for finding Y could be as follows. Define

$$X_a = \frac{n^2}{m} w_a (w_a, \text{sgn } (\rho)), \qquad Y = \sum_i^m X_{A_i}. \tag{36}$$

It is obvious that Y is in the range of $\mathcal{R}$ and that its expectation value(equal to sgn ρ) fulfills the conditions in (35). What's more, the operator Chernoff bound can be used to control the deviation of Y from that expected value - so there is hope that we have found a solution.

However, a short calculation shows that convergence is (barely) too slow for our purpose.

Intuitively, it is easy to see what is "wrong" with the previous random process. Assume we sample $k < m$ basis elements. Employing (36), our general "best guess" at this poing for a matriix Y_1 which resembles sgn ρ on T (i.e. with $\|\mathcal{P}_T Y_1 - \mathrm{sgn}\rho\|_F$ "small")would be

$$Y_1 = \frac{n^2}{k} \sum_i^k w_{A_i}(w_{A_i}, \mathrm{sgn}\rho)$$

Now given this information, the matrix we really should be approximating in the next steps is $\mathcal{P}_T(\mathrm{sgn}\rho - Y_1)$. The process (36), in contrast, does not update its "future strategy based on past result". Tying to perform better, we will draw a further batch of k coefficients and set

$$Y_{op} = Y_1 + \frac{n^2}{k} \sum_{i=k+1}^{2k} w_{A_i}(w_{A_i}, \mathrm{sgn}\rho - \mathcal{P}_T Y_1)$$

The sequence $\mathcal{P}_T Y_i$ will be shown to converge exponentially fast to sgnρ. For resons which should be all too obvious from (fig 1)

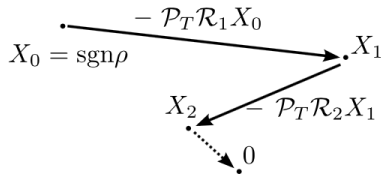

Fig. 3. Caricature of the "golfing scheme" used to construct the certificate. In the ith step, X_{i-1} designates the vector we aim to represent. The approximation of X_{i-1} actually obtained is $\mathcal{P}_T\mathcal{R}_i X_{i-1}$. The distance of the new goal $X_i = X_{i-1} - \mathcal{P}_T\mathcal{R}_i X_{i-1}$ to the origin is guaranteed to be only half the previous one. The sequence X_i thus converges exponentially fast to the origin.

We will call this adapted strategy the *golfing scheme*.

Size k: on the one hand, k have to be large enough to allow for the application of the operator large-deviation bounds tailored for *independent* random variables. On the other hand, k must not be too large, as the speed of convergence is ecponential in $l = m/k$.

5.6.2 Proof:

Before supplying the details of this scheme, we state a lemma which will allow us to control the operator norm $\|\mathcal{P}_T^\perp Y\|_{op}$ of the approximations. The operator-Bernstein inequality makes this a simple calculation.

Lemma 7. *Let $F \in T$. Then*

$$\mathbb{P}\left[\|\mathcal{P}_T^\perp \mathcal{R} F\|_{op} > t\right] \leq 2n \exp\left(-\frac{t^2 \kappa r}{4\nu \|F\|_F^2}\right)$$

for $t \leq \sqrt{2/r}\|F\|_F$ and,

$$\mathbb{P}\left[\|\mathcal{P}_T^\perp \mathcal{R} F\|_{op} > t\right] \leq 2n \exp\left(-\frac{t\kappa\sqrt{r}}{2\sqrt{2}\nu \|F\|_F}\right)$$

for large values of t.

Proof. It is sufficient to treat the case where $\|F\|_F = 1$. Set

$$X_a = \frac{n^2}{m} \mathcal{P}_T^\perp w_a(w_a, F).$$

Then $\sum_i^m X_{A_i} = \frac{1}{m}\mathcal{P}_T^\perp F$, and

$$\mathbb{E}[X_{A_i}] = \frac{1}{m}\mathcal{P}_T^\perp F = 0.$$

Using (The property of incoherence) $\max_a \|w_a\|_{op}^2 \le \nu\frac{1}{n}$ and the fact that $\|\mathcal{P}_T^{\perp} w_a\|_{op} \le \|w_a\|_{op}$ we estimate the variance:

$$\begin{aligned}\mathbb{E}[X_{A_i}^2] &\le \frac{n^2}{m^2}\sum_a (w_a, F)^2 \|(\mathcal{P}_T^{\perp} w_a)^2\|_{op} \\ &\le \frac{n^2}{m^2}\frac{\nu}{2n}\|F\|_F^2 = \frac{n\nu}{m^2} = \frac{\nu}{m\kappa r} := V_0^2\end{aligned} \tag{37}$$

Next,

$$\|X_{A_i}\|_{op} \le \frac{n^2}{m}\sqrt{\frac{\nu}{n}\frac{2\nu r}{n}} = \frac{n\nu\sqrt{2r}}{m} = \frac{\sqrt{2}\nu}{\sqrt{r}\kappa},$$

so that

$$\frac{2mV_0^2}{\|X_{A_i}\|_{op}} \ge \frac{2m\nu}{m\kappa r}\frac{\sqrt{r}\kappa}{\sqrt{2}\nu} = \frac{\sqrt{2}}{\sqrt{r}}$$

Now use Theorem 6. □

We sample l batches of basis elements, the ith set consisting of $m_i = \kappa_i r n$ matrices.
For $1 \le i \le l$, let

$$\mathcal{R} : \sigma \mapsto \frac{n^2}{m_i}\sum_{j=m_1+\cdots+m_{i-1}+1}^{m_1+\cdots+m_i} w_{A_i}(w_{A_i}, \sigma)$$

be the ith sampling operator associated with the ith batch and set

$$X_0 = \mathrm{sgn}\rho, \qquad Y_i = \sum_{j=1}^{i}\mathcal{R}_j X_{j-1}, \qquad X_i = \mathrm{sgn}\rho - \mathcal{P}_T Y_i$$

From this, we get

$$X_i = (\mathbb{1} - \mathcal{P}_T\mathcal{R}_j\mathcal{P}_T)(\mathbb{1} - \mathcal{P}_T\mathcal{R}_{j-1}\mathcal{P}_T)\ldots(\mathbb{1} - \mathcal{P}_T\mathcal{R}_1\mathcal{P}_T)X_0 \tag{38}$$

Assume the in the ith run

$$\|(\mathbb{1} - \mathcal{P}_T\mathcal{R}_i\mathcal{P}_T)X_{i-1}\|_F < c_i\|X_{i-1}\|_F \tag{39}$$

Denote $p_{op}(i)$ be the probability of this event not occurring. Clearly, if (39) does hold for all i, then

$$\|X_i\|_F = \|(\mathbb{1} - \mathcal{P}_T\mathcal{R}_i\mathcal{P}_T)X_{i-1}\|_F \le c_i\|X_{i-1}\|_F$$

So that $\|X_{Ai}\|_F \le \sqrt{r}\prod_{j=1}^{i} c_j$.
Assume further that for all i the estimate

$$\|\mathcal{P}_T^{\perp}\mathcal{R}_i X_{i-1}\|_{op} \le t_i\|X_{i-1}\|_F$$

is true, with $p_3 i$ bounding the probability of failure. Then

$$\|\mathcal{P}_T^{\perp} Y_l\|_{op} \le \sum_{i=1}^{l}\|\mathcal{P}_T^{\perp}\mathcal{R}_j X_{j-1}\|_{op} \le \sum_{i=1}^{l} t_i\|X_{i-1}\|_F.$$

A first simple choice of parameters (to ne refined in section II is

$$\begin{aligned} c_i &= 1/2 \\ t_i &= 1/(4/\sqrt{r}) \\ \kappa_i &= 64\nu(\ln(4nr) + \ln(2l) + \beta\ln n)\end{aligned}$$

for some $\beta > 0$. It follows that

$$\|X_i\|_F \le \sqrt{r}2^{-i}, \qquad \|\mathcal{P}_T^{\perp} Y_l\|_{op} \le \frac{1}{4}\sum_{i=1}^{l} 2^{-(i-1)} < \frac{1}{2}$$

with $l = [\log_2(2n^2\sqrt{r})]$, the conditions in Equation (35) are met. Using Lemma 5 and Lemma 7 te failure probabiliries become

$$\begin{aligned} p_1 &\leq 4nr \exp\left(-\frac{\kappa}{32\nu}\right), \\ p_{op}(i) &\leq 4nr \exp\left(-\frac{\kappa_i}{32\nu}\right), \\ p_3(i) &\leq 2nr \exp\left(-\frac{\kappa_i}{64\nu}\right) \end{aligned}$$

all of which are bounded above by $\frac{1}{2l}n^{-\beta}$. Theorem 3 for Fourier-type bases thus follows from a simple application of the union bound. The number of coefficients sampled must exceed

$$\begin{aligned} m = l\kappa_i &= 64\nu(\ln(4nr) + \ln(2l) + \beta \ln n) \log_2(2n^2\sqrt{r})rn \\ &= O(rn\nu(1+\beta)\ln^2 n) \end{aligned}$$

5.7 *V. The certificate: general case*

In this section, we show that the construction of Y described above continues to work if the assumption by $\max_a \|w_a\|_{op}^2 \leq \nu\frac{1}{n}$ on the operator norm of the basis elements is replaced by the incoherence properties

$$\begin{aligned} \max_a \|\mathcal{P}_T w_a\|_F^2 &\leq 2\nu\frac{r}{n}, \\ \max_a \ (w_a, \mathrm{sgn}\rho)^2 &\leq \nu\frac{r}{n^2} \end{aligned}$$

Indeed, in the discussion of the golfing scheme, we reffered to the operator norm of w_a exactly once. In the proof of Lemma 7, we considered the quantity

$$X_a = \frac{n^2}{m}\mathcal{P}_T^{\perp} w_a (w_a, F). \tag{40}$$

After Equation (37), the variance

$$\|\mathbb{E}[X_{A_i}^2]\|_{op} \leq \frac{n^2}{m^2}\sum_a (w_a, F)^2 \|(\mathcal{P}_T^{\perp} w_a)^2\|_{op}$$

was upper-bounded using the fact that $\|(\mathcal{P}_T^{\perp} w_a)^2\|_{op} \leq \frac{\nu}{n}$. Clearly the absence of this assumption can be compensated for by a suitable bound on $(w_a, F)^2$. This will be made precise below.

Assume that F os sp,e ,atrox om T with $\|F\|_F = 1$. Further, assume that at least one of the following two bounds

$$\max_a \|w_a\|_{op}^2 \leq \frac{v}{n} \tag{41}$$

$$\max_a |(w_a, F)|^2 \leq \frac{v}{n^2} \tag{42}$$

holds.

Note that

$$\|\mathbb{E}[X_{A_i}^2]\|_{op} \leq \frac{n^3}{m^2} underset\psi \max \sum_a (w_a, F)^2 \frac{1}{n} < \psi, w_a^2 \psi >, \tag{43}$$

where the maximum is over all normalized vectors $\psi \in (range\,\rho)^{\perp}$. Let ψ_0 be a vector achieving the maximum. Define two vectors p, q in $\mathbb{R}^{n^2}$ by setting their components to

$$q_a := (w_a, F)^2, \qquad p_a := \frac{1}{n} < \psi_0, w_a^2 \psi_0 > \tag{44}$$

The assumption that $\|F\|_F^2 = 1$ implies that $\|q\|_1 = \sum_a |q_a| = 1$. Slightly less obvious is the fact thatthe same is true for the other vector. $\|p\|_1 = 1$, regardless of the basis chosen. This relation is ascertained by the next lemma.

Lemma 8. *Let $\{w_a\}$, be a set of $n \times n-$matrices (not necessarily Hermitian) that fulfill the completness relation*

$$\sum_a (\bar{w}_a)_{i_1,j_1}(w_a)_{i_{op},j_{op}} = \delta_{i_1,i_{op}}\delta_{i_{op},j_{op}}. \tag{45}$$

Then

$$\sum_a w_a^* w_a = n\mathbb{1}$$

Proof. Compute:

$$\left(\sum_a w_a^* w_a\right)_{i,j} = \sum_{a,k} (\bar{w}_a)_{k,i}(w_a)_{k,j} = \sum_k \delta_{i,j} = n\delta_{i,j}$$

□

Thus,

$$\|p\|_1 = \sum_a p_a = \frac{1}{n} < \psi_0, n\mathbb{1}\psi_0 >$$

We return to the vectors in (44). The assumptions made imply that at least one of the vectors is element-wise bounded above by $\frac{\nu}{n^2}$.Thus

$$\left|\sum_a p_a q_a\right| \leq \min\{\|p\|_1\|q\|_\infty, \|p\|_\infty\|q\|_1\} \leq \frac{\nu}{n^2} \tag{46}$$

Plugging this estimate into the computation of the variance (43) we obtin

$$\mathbb{E}[X_{A_i}^2]\|_{op} \leq \frac{n^3}{m^2}\frac{\nu}{n^2} = \frac{\nu}{m\kappa r}.$$

We have proved the general analogue of Lemma 7:

Lemma 9. *Let $F \in T$. Let $f \geq \|F\|_F$ be an upper bound on the Frobenius norm of F. Assume that one of the two bounds*

$$\max_a \|w_a\|_{op}^2 \leq \frac{v}{n} \tag{47}$$

$$\max_a |(w_a, F)|^2 \leq \frac{v}{n^2} f^2 \tag{48}$$

holds. Then

$$\mathbb{P}\left[\|\mathcal{P}_T^{\perp}\mathcal{R}F\|_{op} > t\right] \leq 2n \exp\left(-\frac{t^2\kappa r}{4\nu f^2}\right), \tag{49}$$

for $t \leq \sqrt{2/r}f$.

Next, we have to justify the bounds on $(w_a, F)^2$ we imposed in the previous lemma, By assumption $\max_a (w_a, \mathrm{sgn}\rho)^2 \leq \nu\frac{r}{n^2}$, the estimate does hold for $F = \mathrm{sgn}\rho$, i.e. Lemma 9 may be applied during the first leg $X_0 = \mathrm{sgn}\rho$ of the "golfing scheme". However, there is no a priori reason that the same be true for $X_1 = (\mathbb{1} - \mathcal{P}_T\mathcal{R}_1\mathcal{P}_T)X_0$. For nor, all we know about X_1 is that it is an element of T and hence low-rank. This property was enough for Fourier-type bases, but in the general case, it proves too weak. We thus hae to ensure that"inhomogeneity" of X_i implies inhomoheneity of X_{i+1}, a fact that can be ascertained using yet another Chernoff bound.

Let $\mu(F) = \max_a (w_a, F)^2$ be the maximal squared overlap between F and any element of the operator basis.

Lemma 10. *Let $F \in T$. Then*

$$\mathbb{P}[\mu(\mathbb{1} - \mathcal{P}_T \mathcal{R} \mathcal{P}_T)F > t] \leq 2n^2 \exp\left(-\frac{t\kappa}{4\mu(F)\nu}\right)$$

for all $t \leq \mu(F)$.

Proof. Fix $b \in [1, n^2]$. Define

$$X_a = \frac{1}{m}(w_a, F) - (w_b, \frac{n^2}{m}\mathcal{P}_T w_a)(w_a, F). \tag{50}$$

Then

$$\sum_i^m X_{A_i} = (w_b, (\mathbb{1} - \mathcal{P}_T \mathcal{R} \mathcal{P}_T)F).$$

Note that the first term in (50) is the expectation value of the second one. Therefore, $\mathbb{E}[X_{A_i}] = 0$ and the variance of X_{A_i} is bounded above by the variance of the second term alone (as in the proof of Lemma 5):

$$\begin{aligned}
\mathbb{E}[X_{A_i}^2] &\leq \frac{1}{n^2}\sum_a (w_b, \frac{n^2}{m}\mathcal{P}_T w_a)^2 (w_a, F)^2 \\
&\leq \frac{n^2}{m}\mu(F)\sum_a (\mathcal{P}_T w_b, w_a)^2 \\
&= \frac{n^2}{m}\mu(F)\|\mathcal{P}_T w_b\|_F^2 \\
&\leq \frac{n^2 \mu(F)\nu r}{m^2 n} \\
&= \frac{\mu(F)\nu}{m\kappa} =: V_0^2
\end{aligned}$$

Further,

$$|X_{A_i}| \leq \frac{1}{m}\mu(F)^{1/2}\left(1 + n^2\frac{\nu r}{n}\right) = \frac{1}{m}\mu(F)^{1/2}(1 + n\nu)r.$$

Thus, from the Chernoff bound:

$$\mathbb{P}\left[|(w_b, (\mathbb{1} - \mathcal{P}_T \mathcal{R} \mathcal{P}_T)F))| > \sqrt{t}\right] \leq 2\exp\left(-\frac{t\kappa}{4\mu(F)\nu}\right)$$

as long as $\sqrt{t}$ does not exceed

$$\frac{2mV_0^2}{|X_{A_i}|} = \frac{2m\mu(F)\nu}{m\kappa}\frac{m}{\mu(F)^{1/2}(1 + n\mu r)} \leq \mu(F)^{1/2}$$

The advertised estimate follows by taking squares and applying the union bound over the n^2 elements of the basis. □

With these preparations made, we can repeat the "golfing" argument from the last section. As an additional constraint, we demand that

$$\mu(X_i) \leq c_i^2 \mu(X_{i-1})$$

be fulfilled for all i, with probabiliry of failure given by $p_4(i)$.

Then, with

$$\begin{aligned}
c_i &= 1/2 \\
t_i &= 1/(2/\sqrt{r}) \\
\kappa_i &= 64\nu(\ln(4n^2) + \ln(3l) + \beta \ln n)
\end{aligned}$$

it follows that

$$\|X_i\|_F \leq 2^{-i}\|\mathrm{sgn}\rho\|_F = 2^{-i}\sqrt{r}, \mu(X_i) \leq 2^{-2i}\mu(\mathrm{sgn}\rho) \leq \frac{\nu}{n^2}(2^{-2i}r).$$

Thus, in ith iteration of the golfing scheme, we can apply Lemma 9 with $F = X_i$ and $f = 2^{-i}\sqrt{r}$.

The failure probabilities $p_1, p_{op}(i), p_3(i)$ are as before. Further

$$p_4(i) \leq 2n^2 \exp\left(-\frac{\kappa_i}{16\nu}\right),$$

which, as the other probabilities, is bounded above by $\frac{1}{3l}n^{-\beta}$. By the union bound, Theorem 3 holds as long as

$$m > \log_2(2n^2\sqrt{r})64\nu(\ln(4n^2) + \ln(3l) + \beta\ln n)rn$$