Disentangling Orthogonal Matrices

Teng Zhang\textsuperscript{1}

Department of Mathematics, University of Central Florida
Orlando, Florida 32816, USA

Amit Singer\textsuperscript{2}

Department of Mathematics and The Program in Applied and Computational Mathematics (PACM), Princeton University
Princeton, New Jersey 08544, USA

Abstract

Motivated by a certain molecular reconstruction methodology in cryo-electron microscopy, we consider the problem of solving a linear system with two unknown orthogonal matrices, which is a generalization of the well-known orthogonal Procrustes problem. We propose an algorithm based on a semi-definite programming (SDP) relaxation, and give a theoretical guarantee for its performance. Both theoretically and empirically, the proposed algorithm performs better than the naïve approach of solving the linear system directly without the orthogonal constraints. We also consider the generalization to linear systems with more than two unknown orthogonal matrices.

Keywords: SDP relaxation, orthogonal Procrustes problem, cryo-EM

MSC[2010] 15A24, 90C22

1. Introduction

In this paper, we consider the following problem: given known matrices $X_1, X_2 \in \mathbb{R}^{N \times D}$ and unknown orthogonal matrices $V_1, V_2 \in O(D)$, recover $V_1$ and $V_2$ from $X_3 \in \mathbb{R}^{N \times D}$ defined by

$$X_3 = X_1 V_1 + X_2 V_2.$$  \hspace*{1cm} (1)

A naïve approach would be solving (1) while dropping the constraints of orthogonality on $V_1$ and $V_2$. This linear system has $ND$ linear constraints and $2D^2$ unknown variables, therefore, this approach can recover $V_1$ and $V_2$ when $N \geq 2D$. The question is, can we develop an algorithm that takes the constraints of orthogonality into consideration, so that it is able to recover $V_1$ and $V_2$?
$V_2$ when $N < 2D$, and more stably when the observation $X_3$ is contaminated by noise?

The associated least squares problem

$$
\min_{V_1, V_2 \in O(D)} \|X_1 V_1 + X_2 V_2 - X_3\|_F^2
$$

(2)

can be considered as a generalization of the well-known orthogonal Procrustes problem [1]:

$$
\min_{V \in O(D)} \|X_1 V - X_2\|_F^2,
$$

(3)

with the main difference being that the minimization in (2) is over two orthogonal matrices instead of just one as in (3). Although the orthogonal Procrustes problem has a closed form solution using the singular value decomposition, problem (2) does not enjoy this property.

Still, (2) can be reformulated so that it belongs to a wider class of problems called the little Grothendieck problem [2], which again belongs to QO-OC (Quadratic Optimization under Orthogonality Constraints) considered by Nemirovski [3]. QO-OCs have been well studied and include many important problems as special cases, such as Max-Cut [4] and generalized orthogonal Procrustes [5, 6, 7]

$$
\min_{V_1, \ldots, V_n \in O(D)} \sum_{1 \leq i,j \leq n} \|X_i V_i - X_j V_j\|_F^2,
$$

(4)

which has applications to areas such as psychometrics, image and shape analysis and biometric identification.

The non-commutative little Grothendieck problem [8] is defined by:

$$
\min_{V_1, \ldots, V_n \in O(D)} \sum_{i,j=1}^n \text{tr}(C_{ij} V_i V_j^\top),
$$

(4)

Problem (2) can be considered as a special case of (4) with $n = 3$. The argument is as follows. For convenience, we homogenize [1] by introducing a slack unitary variable $V_3 \in O(D)$ and consider the augmented linear system

$$
X_1 V_1 + X_2 V_2 + X_3 V_3 = 0
$$

(5)

Clearly, if $(V_1, V_2, V_3)$ is a solution to (5), then the pair $(-V_1 V_4^\top, -V_2 V_5^\top)$ is a solution to the original linear system (4). The least squares formulation corresponding to (5) is

$$
\min_{V_1, V_2, V_3 \in O(D)} \|X_1 V_1 + X_2 V_2 + X_3 V_3\|_F^2.
$$

(6)

Let $C \in \mathbb{R}^{3D \times 3D}$ be a Hermitian matrix with the $(i, j)$–th $D \times D$ block given by $C_{ij} = X_i^\top X_j$. The least squares problem (6) is equivalent to

$$
\min_{V_1, V_2, V_3 \in O(D)} \sum_{i,j=1}^3 \text{tr}(C_{ij} V_i V_j^\top),
$$

(7)

which is the little Grothendieck problem (4) with $n = 3$. 

2
1.1. Motivation

Our problem arises naturally in single particle reconstruction (SPR) from cryo-electron microscopy (EM), where the goal is to determine the 3D structure of a macromolecule complex from 2D projection images of identical, but randomly oriented, copies of the macromolecule. Zvi Kam [9] showed that the spherical harmonic expansion coefficients of the Fourier transform of the 3D molecule, when arranged as matrices, can be estimated from 2D projection images up to an orthogonal matrix (for each degree of spherical harmonics). Based on this observation, Bhamre et al. [10] recently proposed “Orthogonal Replacement” (OR), an orthogonal matrix retrieval procedure in which cryo-EM projection images are available for two unknown structures $\varphi^{(1)}$ and $\varphi^{(2)}$ whose difference $\varphi^{(2)} - \varphi^{(1)}$ is known. It follows from Kam’s theory that we are given the spherical harmonic expansion coefficients of $\varphi^{(1)}$ and $\varphi^{(2)}$ up to an orthogonal matrix, and their difference. Then the problem of recovering the spherical harmonic expansion coefficients of $\varphi^{(1)}$ and $\varphi^{(2)}$ is reduced to the mathematical problem (1). If (1) can be solved for smaller $N$, then we can reconstruct $\varphi^{(1)}$ and $\varphi^{(2)}$ with higher resolution. The cryo-EM application serves as the main motivation of this paper. We refer the reader to [10] for further details regarding the specific application to cryo-EM.

2. Algorithm and Main result

The little Grothendieck problem and QO-OCs are generally intractable, for example, it is well-known that the Max-Cut Problem is NP-hard. Many approximation algorithms have been proposed and analyzed [4, 3, 11, 12, 2, 13], and the principle of these algorithms is to apply a semi-definite programming (SDP) relaxation followed by a rounding procedure. The SDP can be solved in polynomial time (for any finite precision). Based on the same principle, we relax the problem (1) to an SDP as follows.

Let $H \in \mathbb{R}^{D \times D}$ be a Hermitian matrix with the $(i,j)$-th $D \times D$ block given by $H_{ij} = V_i V_j^\top$, that is,

$$H = \begin{pmatrix} V_1 & V_2 & V_3 \end{pmatrix} (V_1^\top, V_2^\top, V_3^\top).$$

Then (1) is equivalent to

$$\min_{H \succeq 0, H_{ii} = I, \text{rank}(H) = D} \text{tr}(CH),$$

where $H \succeq 0$ denotes that $H$ is a positive semidefinite matrix. The only constraint which is non-convex is the rank constraint. Dropping it leads to the following SDP:

$$\min \text{tr}(CH), \text{ subject to } H \succeq 0 \text{ and } H_{ii} = I.$$

(8)
If the solution satisfies \( \text{rank}(H) = D \), then \( V_1, V_2 \) and \( V_3 \) are extracted by applying decomposition to \( H \) as follows. Let \( H = UU^T \), where

\[
U = \begin{pmatrix}
    U_1 \\
    U_2 \\
    U_3
\end{pmatrix} \in \mathbb{R}^{3D \times D}, \quad \text{and} \quad U_i \in \mathbb{R}^{D \times D}
\]

then \( V_i = U_i, 1 \leq i \leq 3 \) would be a solution.

Notice that the solution to (5) is not unique: if \((U_1, U_2, U_3)\) satisfies (5), then for any \( U \in O(D) \), the triplet \((U_1U, U_2U, U_3U)\) satisfies (3) as well. Although the solution to (5) is not unique, the solution to the original problem (2) is uniquely given by \((-U_1U_3^T, -U_2U_3^T)\).

When \( \text{rank}(H) > D \), then there does not exist \( U \in \mathbb{R}^{3D \times D} \) such that \( H = UU^T \) and the linear system (1) does not have a solution. However, we could employ the rounding procedure described in [2]: Let \( H = UU^T \), where

\[
U = \begin{pmatrix}
    U_1 \\
    U_2 \\
    U_3
\end{pmatrix} \in \mathbb{R}^{3D \times 3D}, \quad \text{and} \quad U_i \in \mathbb{R}^{D \times 3D},
\]

then we generate approximate solutions by \( V_1 = f(-U_1U_3^T) \) and \( V_2 = f(-U_2U_3^T) \), where \( f \) is a rounding procedure to the nearest orthogonal matrix as follows. For any \( Z \in \mathbb{R}^{D \times D} \) with SVD decomposition \( Z = UZ \Sigma Z V_\top Z \), \( f(Z) = UZ V_\top Z = Z(Z^\top Z)^{-\frac{1}{2}} \).

2.1. Main results

The main contribution of this paper is a particular theoretical guarantee for the SDP approach to return a solution of rank \( D \) and recover \( V_1 \) and \( V_2 \) exactly. We start with a theorem that controls the lower bound of the objective function in (8). Throughout the paper, for any \( d \)-dimensional subspace \( L \) in \( \mathbb{R}^D \), \( P_L \) is a projector of size \( D \times d \) to the subspace.

**Theorem 2.1.** For generic \( X_1, X_2 \in \mathbb{R}^{N \times D} \) with \( N \geq D + 1 \), \( X_3 = -X_1 - X_2 \), \( k \geq D \), and

\[
\mathcal{U} = \left\{ U = \begin{pmatrix}
    U_1 \\
    U_2 \\
    U_3
\end{pmatrix} \in \mathbb{R}^{3D \times k} : U_i \in \mathbb{R}^{D \times k}, U_1U_1^\top = U_2U_2^\top = U_3U_3^\top = I \right\},
\]

then for any \( U \in \mathcal{U} \),

\[
\|XU\|_F \geq c(X_1, X_2)\|U_\top P_{L_1}\|_F^2,
\]

where \( X = (X_1, X_2, X_3) \in \mathbb{R}^{N \times 3D} \),

\[
L_1 = \{ x \in \mathbb{R}^D : x = (v, v, v) \text{ for some } v \in \mathbb{R}^D \},
\]

and \( c(X_1, X_2) \) is a constant depending on \( X_1 \) and \( X_2 \) and it is positive for generic \( X_1 \) and \( X_2 \).
Based on Theorem 2.1 and $\|XU\|_F^2 = \text{tr}(CH)$, this paper proves that when $N \geq D + 1$, the SDP method recovers the orthogonal matrices for generic cases, i.e., the property holds for $(X_1, X_2)$ that lies in a dense open subset of $\mathbb{R}^{N \times D} \times \mathbb{R}^{N \times D}$. This is formally stated next. Its part (b) shows that the SDP method is stable to noise.

**Theorem 2.2.** (a) For generic $X_1, X_2 \in \mathbb{R}^{N \times D}$ with $N \geq D + 1$, the SDP method recovers $V_1$ and $V_2$ exactly.

(b) Under the assumptions in (a), and suppose that the input matrices of the SDP method are $\hat{X}_i$ such that $\|\hat{X}_i - X_i\|_F \leq \epsilon$ for $1 \leq i \leq 3$, then the SDP method recovers $\{V_i\}_{i=1}^{K-1}$ approximately in the sense that the error between the recovered orthogonal matrix $\hat{V}_i$ and the true orthogonal matrix $V_i$, $\|\hat{V}_i - V_i\|_F$, is bounded above by $C\sqrt{\epsilon}$ for some $C$ that does not depend on $\epsilon$.

The result (a) shows that the SDP method successfully recovers the orthogonal matrices as long as $N \geq D + 1$, compared with the stringent requirement $N \geq 2D$ for the na"ive least squares approach. The condition $N \geq D + 1$ is nearly optimal. In (1), there are $ND$ constraints and $D(D - 1)$ variables. Hence, it is impossible to recover $V_1$ and $V_2$ when $N < D - 1$.

The result (b) shows that the SDP method is stable to noise in the input matrices. We remark that it might be possible to improve the stability analysis: While the current analysis gives an error of $O(\sqrt{\epsilon})$, the empirical performance usually has an error of $O(\epsilon)$, as shown in Table 2 of Section 3.

We also remark that Theorem 2.2 can be generalized to the complex case—the proof applies to the case of unitary matrices as well. For the complex case, there are $2ND$ constraints and $2D^2$ degrees of freedom. Therefore, it is impossible to recover $V_1$ and $V_2$ when $N < D$. Moreover, we suspect that recovery is impossible even for $N = D$, which would suggest that the sufficient condition $N \geq D + 1$ in Theorem 2.2(a) is also necessary: in fact, it is easy to verify the impossibility of recovering $V_1$ and $V_2$ when $N = D = 1$.

### 2.2. Generalization

A natural generalization of (1) is the following problem: given known matrices $X_1, X_2, \ldots, X_{K-1} \in \mathbb{R}^{N \times D}$ and unknown orthogonal matrices $V_1, V_2, \ldots, V_{K-1} \in O(D)$, recover $\{V_i\}_{i=1}^{K-1}$ from

$$X_K = \sum_{i=1}^{K-1} X_i V_i.$$  \hspace{1cm} (10)

For this generalized problem, the SDP method is formulated as follows. We first homogenize it to

$$\sum_{i=1}^{K} X_i V_i = 0,$$

and let $H \in \mathbb{R}^{KD \times KD}$ be a Hermitian matrix with the $(i, j)$–th $D \times D$ block given by $H_{ij} = V_i V_j^T$. Then the SDP method solves

$$\min \text{tr}(CH), \text{ subject to } H \succeq 0 \text{ and } H_{ii} = I \text{ for all } 1 \leq i \leq K.$$  \hspace{1cm} (11)
where $H_{ii}$ represents the $(i,i)$-th $D \times D$ block. Then we extract the orthogonal matrices by the procedure described in Section 2.

For this generalized problem and its associated SDP approach, we have the following theoretical guarantee.

**Theorem 2.3.** For generic $\{X_i\}_{i=1}^{K-1} \in \mathbb{R}^{N \times D}$, if $N \geq (K-2)D + 1$, then the SDP method recovers $\{V_i\}_{i=1}^{K-1}$ exactly.

Theorem 2.2(a) can be considered as a special case of Theorem 2.3 when $K = 3$. However, for $K > 3$, the condition $N \geq (K-2)D + 1$ is not close to optimal. Since (10) has $ND$ constraints and $D(D-1)(K-1)/2$ variables, the information-theoretic limit is $N = (D-1)(K-1)/2$. Simulations in Section 3 also show that the SDP approach empirically recovers the orthogonal matrices even when $N$ is smaller than $(K-2)D + 1$. However, the theoretical guarantee in Theorem 2.3 is still more powerful than the least squares approach of solving

$$\min_{\{V_i\}_{i=1}^{K-1} \in \mathbb{R}^{D \times D}} \|X_K - \sum_{i=1}^{K-1} X_i V_i\|_F^2,$$

which requires $N \geq (K-1)D + 1$ to recover $\{V_i\}_{i=1}^{K-1}$.

### 3. Numerical Experiments

In this section, we compare several methods for solving (1) and (10) on artificial data sets. The data sets are generated as follows: $\{X_i\}_{i=1}^{K-1}$ are random matrices with i.i.d standard Gaussian entries $\mathcal{N}(0, 1)$, $\{V_i\}_{i=1}^{K-1}$ are random orthogonal matrices (according to Haar measure) generated by QR decomposition of random matrices with i.i.d standard Gaussian entries, and $X_K$ is generated by (10).

We compare the following five methods:

1. The SDP relaxation approach (SDP) described in Section 2.
2. The naïve least squares approach (LS):

$$\min_{\{V_i\}_{i=1}^{K-1} \in \mathbb{R}^{D \times D}} \|X_K - \sum_{i=1}^{K-1} X_i V_i\|_F^2.$$

3. Since the convex hull of the set of orthogonal matrices is the set of matrices with operator norm not greater than one, we can strengthen the LS approach by constraining its domain (C-LS):

$$\min_{\{V_i\}_{i=1}^{K-1} \in \mathbb{R}^{D \times D}} \|X_K - \sum_{i=1}^{K-1} X_i V_i\|_F^2, \text{ subject to } \|V_i\| \leq 1, 1 \leq i \leq K - 1$$

4. This is an approach suggested to us by Afonso Bandeira. Let us start with the case $K = 3$. If $V_3 = V_1 V_2^T$, then from $X_3 V_2^T = X_1 V_3 + X_2$ and $X_3 V_1^T = X_1 + X_2 V_3^T$. Then we solve the expanded least squares problem based on these three equations (LS+):

$$\min_{V_1, V_2, V_3} \|X_3 - X_1 V_1 - X_2 V_2\|_F^2 + \|X_3 V_2^T - X_1 V_3 - X_2\|_F^2 + \|X_3 V_1^T - X_1 - X_2 V_3^T\|_F^2.$$
Defining
\[
H = \begin{pmatrix}
I & V_3 & -V_1 \\
V_3^\top & I & -V_2 \\
-V_1^\top & -V_2^\top & I
\end{pmatrix},
\]
the optimization problem can be rewritten as
\[
\min_{H \in \mathbb{R}^{3D \times 3D}} \| (X_1, X_2, X_3) H \|^2_F, \quad \text{subject to } H = H^\top, H_{ii} = I.
\]

In general, for \( K \geq 3 \), this method can be formulated as
\[
\min_{H \in \mathbb{R}^{KD \times KD}} \text{tr}(CH^2), \quad \text{subject to } H = H^\top \quad \text{and } H_{ii} = I \quad \text{for all } 1 \leq i \leq K,
\]
where \( H_{ij} \) represents the \( ij \)-th \( D \times D \) block of \( H \).

5. The LS+ approach with constraints on the operator norm of \( H_{ij} \) (C-LS+):
\[
\min_{H \in \mathbb{R}^{KD \times KD}} \text{tr}(CH^2), \quad \text{subject to } H = H^\top, H_{ii} = I \quad \text{and } \| H_{ij} \| \leq 1 \quad \text{for all } 1 \leq i, j \leq K.
\]

To compare the SDP/LS+/C-LS+ approaches, we summarize their objective functions and their constraints in Table 1. There are two main differences. First, the objective functions are different. However, since \( \text{tr}(CH) = 0 \) if and only if \( \text{tr}(CH^2) = 0 \) (considering \( C \succ 0 \) and \( H \succ 0 \)), this difference does not affect the property of exact recovery. Second, the constraints of the SDP approach are more restrictive than those of the C-LS+ approach \( (H_{ii} = H_{jj} = I \quad \text{and } H \succ 0 \quad \text{imply } \| H_{ij} \| \leq 1) \), which is more restrictive than the C-LS approach. This observation partially justifies the fact that SDP performs better than C-LS+, and C-LS+ performs better than C-LS. However, these interpretations do not justify the empirical finding in Figures 1 and 3 that C-LS+ and SDP behave very similarly in the absence of noise. We leave the explanation of this observation as an open question.

|          | objective function | common constraint | other constraints |
|----------|--------------------|-------------------|------------------|
| SDP      | \( \text{tr}(CH) \) |                   | \( H \succ 0 \)  |
| LS+      | \( \text{tr}(CH^2) \) | \( H_{ii} = I, \ H = H^\top \) | \( \| H_{ij} \| \leq 1 \) |
| C-LS+    | \( \text{tr}(CH^2) \) |                   |                  |

Among these optimization approaches, the LS method has an explicit solution by decomposing it into \( D \) sub-problems, where each is a regression problem that estimates \( KD \) regression parameters. All other methods are convex and can be solved by CVX [15], where the default solver SeDuMi is used [16]. While the LS+ approach can also be written as a least squares problem with an explicit solution, this problem is not decomposable (unlike the LS method).

When the solution matrices of LS/C-LS are not orthogonal, they are rounded to the nearest orthogonal matrices using the approach in [14]. The rounding procedure of LS+/C-LS+ is the same as that of the SDP method.
Figure 1: The dependence of the mean recovery error (over 50 runs) with respect to $N$, when $D = 10$ (left panel) and $D = 20$ (right panel). The $y$-axis represents the mean recovery error of $V_1$ in Frobenius norm.

In the first simulation, we aim to find the size of $N$ such that the orthogonal matrices be exactly recovered by the suggested algorithms for $K = 3$. We let $D = 10$ or 20 and choose various values for $N$, and record the mean recovery error of $V_1$ (in Frobenius norm) over 50 repeated simulations in Figure 1. The performance of LS verifies our theoretical analysis: it recovers the orthogonal matrices for $N \geq 2D$. LS fails when $N < 2D$ because the null space of $[X_1, X_2]$ is nontrivial and there are infinite solutions. Besides, LS+ succeeds when $N \geq 3D/2$. SDP and C-LS+ are the best approaches and they succeed when $N \geq D + 1$, which verifies Theorem 2.2.

In the second simulation, we test the stability of the suggested algorithms when $K = 3$ and the measurement matrix $X_3$ is contaminated elementwisely by Gaussian noise $\mathcal{N}(0, \sigma^2)$. We use the setting $N = 12, 16, 22$, $D = 10$ and $\sigma = 0.01$ or 0.1 and record the mean recovery error over 50 runs in Table 2 which shows that the SDP relaxation approach is more stable to noise than competing approaches. This motivates our interest in studying the SDP approach.

Table 2: The mean recovery error over 50 runs in the noisy setting for $K = 3$ and $D = 10$.

| $N$ | $\sigma$ | SDP  | C-LS+ | LS+  | C-LS+ | LS  |
|-----|----------|------|-------|------|-------|-----|
| 12  | 0.01     | 0.071| 0.076 | 0.482| 0.508 | 2.260|
| 16  | 0.01     | 0.026| 0.031 | 0.037| 0.059 | 1.926|
| 22  | 0.01     | 0.018| 0.021 | 0.020| 0.030 | 0.077|
| 12  | 0.1      | 0.742| 0.742 | 1.088| 0.880 | 2.341|
| 16  | 0.1      | 0.261| 0.328 | 0.399| 0.459 | 2.034|
| 22  | 0.1      | 0.175| 0.217 | 0.216| 0.262 | 0.834|

In the third simulation, we compare these methods for $K = 5$ and $D = 5, 10$. 
The results are shown in Figure 3. This simulation verifies Theorem 2.3 by showing that the SDP approach successfully recovers the orthogonal matrices for $N \geq (K-2)D + 1$. Indeed, the empirical performance of the SDP approach is even better: it recovers $\{V_i\}_{i=1}^5$ at $N = 12$ and 25 respectively, which are smaller than $(K-2)D + 1$. Compared with LS/LS+/C-LS, the SDP and C-LS+ approaches recover the orthogonal matrices with smaller $N$.

At last, we record the running time for all approaches in Table 3. Although the running time is not the main focus of this paper, and CVX is not optimized for the approaches, this table gives a sense of the running times. Table 3 clearly shows that the LS approach is much faster than the other approaches, and the SDP approach is consistently faster than C-LS+. We suspect that it is due to the fact that SDP has fewer constraints, even though the constraint of SDP is more restrictive than that of C-LS+.

Table 3: The average running time (in seconds) when $\sigma = 0.1$, $K = 3$, $D = 10$, $N = 15$ (first row) and $\sigma = 0.1$, $K = 5$, $D = 10$, $N = 35$ (second row).

|        | SDP | C-LS+ | LS+ | C-LS | LS  |
|--------|-----|-------|-----|------|-----|
| First  | 0.64| 0.76  | 0.20| 0.48 | 0.0005 |
| Second | 5.33| 6.58  | 0.62| 0.93 | 0.0017 |

4. Proofs of main results

In this section, we first provide the proof for Theorem 2.2 assuming Theorem 2.1 and then provide the proofs for Theorems 2.1 and 2.3. The main reason for this organization is that, given Theorem 2.1 (whose proof is more technical), the proof of Theorem 2.2 is rather straightforward. This organization would
also emphasize the importance of Theorem 2.1, which plays an important role in the proof of Theorems 2.2.

### 4.1. Proof of Theorem 2.2

Part (a) follows from the result in part (b) with $\epsilon = 0$, so it is sufficient to prove part (b).

In the proof of part (b), we first claim that it is sufficient to prove the case $V_1 = V_2 = -I$, i.e., when $X_1 + X_2 + X_3 = 0$ and $\|\hat{X}_{i} - X_i\|_F \leq \epsilon$ for $1 \leq i \leq 3$, then the SDP method recovers $V_1$ and $V_2$ such that $\|\hat{V}_i + I\|_F \leq C\sqrt{\epsilon}$ for $i = 1, 2$.

This result implies that if the input of the SDP method is $(-X_1V_1, -X_2V_2, X_3)$ and the output is denoted by $(\hat{V}_1, \hat{V}_2)$, then $\|\hat{V}_i + I\|_F \leq C\sqrt{\epsilon}$ for $i = 1, 2$.

Additionally, it can be verified that if the SDP method outputs $(V_1, V_2)$ when the input is $(X_1, X_2, X_3)$, $U_1$ and $U_2$ are two orthogonal matrices, then the output for $(X_1U_1, X_2U_2, X_3)$ would be $(U_1^TV_1, U_2^TV_2)$. Applying this observation, we have $\hat{V}_i = -\hat{V}_i^T$. Combining it with $\|\hat{V}_i + I\|_F \leq C\sqrt{\epsilon}$ for $i = 1, 2$, the theorem is proved.

The rest of the proof will assume $V_1 = V_2 = -I$ and $X_1 + X_2 + X_3 = 0$. We represent the noisy setting in [8] by $\hat{X}$, $\hat{C}$ and $\hat{H}$, the clean setting by $X$, $C$ and $H$, and write the decomposition of $H$ and $\hat{H}$ by $H = UU^T$ and $\hat{H} = \hat{U}U^T$.

Since $\hat{U}_i\hat{U}_i^T = I$, $\|\hat{U}\| \leq \sum_{i=1}^{3} \|\hat{U}_i\| = 3$, [30] implies
\[
\|X\hat{U}\|_F - \|\hat{X}\hat{U}\|_F \leq \|(X - \hat{X})\hat{U}\|_F \leq 3\|X - \hat{X}\|_F \leq 9\epsilon
\]
and following the same argument,
\[
\|\hat{X}\hat{U}\|_F \leq 9\epsilon + \|X\hat{U}\|_F.
\] (13)

Since $\hat{H} = \hat{U}\hat{U}^T$ is the minimizer of the SDP problem, we have $\|\hat{X}\hat{U}\|_F \leq \|X\hat{U}\|_F$. Combining it with $\|X\hat{U}\|_F = 0$ and (13),
\[
\|X\hat{U}\|_F \leq 9\epsilon.
\] (14)

Combining (11), (12) with Theorem 2.1
\[
9\epsilon \geq \|X\hat{U}\|_F \geq \|\hat{X}\hat{U}\|_F - 9\epsilon \geq c(X)\|\hat{U}\|_F^2 - 9\epsilon
\]
so we have
\[
\|\hat{U}\|_F^2 \leq \frac{18\epsilon}{c(X)}.
\] (16)

Combining it with Lemma 4.2
\[
\|\hat{U}_1\hat{U}_3^T - I\|_F = \|\hat{U}_1 - \hat{U}_3\|_F = \|\hat{U}^T(I, 0, -I)\|_F = \|\hat{U}\|_F \|P_{L_1^+}^T(I, 0, -I)\|_F
\]
\[
\leq \|\hat{U}\|_F \|P_{L_1^+}^T(I, 0, -I)\| \leq 2 \sqrt{\frac{18\epsilon}{c(X)}}.
\]
Since the post-processing step \( f(Z) \) is a continuous and differentiable function with respect to \( Z \) and \( f(-I) = -I \), the difference between the recovered orthogonal matrix \( \hat{V}_1 \) and \( V_1 = -I \), \( \| \hat{V}_1 + I \|_F \), is bounded above by \( C\sqrt{\epsilon} \) when \( c(X) > 0 \). Similarly we have \( \| \hat{V}_2 + I \|_F < C\sqrt{\epsilon} \).

4.2. Proof of Theorem 2.1

Proof. The main idea of the proof is to investigate \( \tilde{U}^* \), which is defined to be the nearest matrix to \( U \) in the set \( \tilde{U} \) defined in (17). Then we represent \( \tilde{U}^* \) in the form of (21), and show that \( \| L \|_F \) is bounded by \( C_1 \| XU \|_F \), for some \( C_1 > 0 \).

With additional bounds \( \| KY_1 \|_F, \| KY_2 \|_F \leq C_2 \sqrt{\| XU \|_F} \) and

\[
\| \tilde{U}^* P_{L_1^+} \|_F \leq \left\| \begin{pmatrix} (LY_1)^\top & (LY_2)^\top & 0 \\ (KY_1)^\top & (KY_2)^\top & 0 \end{pmatrix} \right\|_F,
\]

we will show that \( \| \tilde{U}^* P_{L_1^+} \|_F \) is bounded above by a function of \( \| XU \|_F \) in (24). By analyzing the properties of \( \tilde{U}^* \), the same statement holds for \( \| U P_{L_1^+} \|_F \), and the theorem is proved.

We first remark that it is sufficient to prove the case \( N = D + 1 \). If this is true, then for \( N > D + 1 \), (9) holds when \( X \) is replaced by \( X' \), the submatrix consists of the first \( D + 1 \) rows of \( X \). Since \( \| XU \|_F \geq \| X'U \|_F \), (9) is proved. Therefore, for the rest of the proof, we assume \( N = D + 1 \).

We first define the following:

\[
\tilde{U} = \{ U \in \mathbb{R}^{3D \times k} : XU = 0 \},
\]

\[
\tilde{U} = \{ \tilde{U} \in \mathbb{R}^{3D \times k} : XU = 0, \tilde{U}_3 = U_3 \},
\]

and in (17), \( \tilde{U}_3 \) and \( U_3 \) represent the submatrix consists of the last \( D \) rows of \( \tilde{U} \) and \( U \). We also define the distances between two matrices and the distances between a matrix and a set by

\[
\text{dist}(U, U') = \| U - U' \|_F, \quad \text{dist}(U, \tilde{U}) = \min_{U' \in \tilde{U}} \| U - U' \|_F.
\]

Then we have

\[
\text{dist}(U, \tilde{U}) \geq C \text{dist}(U, \tilde{U}),
\]

for \( C = 1/2 \). The proof of (18) is deferred to Section 4.2.1.

Assuming that \( \sigma_{\min}(X) \) is the smallest singular value of \( X \), and for any matrix \( A \in \mathbb{R}^{m \times n} \), \( \text{Sp}(A) \) represents the subspace spanned by the row vectors of \( A \) in \( \mathbb{R}^n \), then we have

\[
\| XU \|_F \geq \sigma_{\min}(X) \| P_{\text{Sp}(X)} U \|_F = \sigma_{\min}(X) \text{dist}(U, \tilde{U}) \geq C \sigma_{\min}(X) \text{dist}(U, \tilde{U}),
\]

where the last inequality follows from (18).
Assuming that $\tilde{U}^* = \arg \min_{\tilde{U} \in \tilde{U}} \text{dist}(\tilde{U}, U)$, then using 
\[
\begin{pmatrix}
U_3 \\
U_3 \\
U_3
\end{pmatrix}
\in \tilde{U}
\]
we have
\[
\text{dist}(\tilde{U}^*, U) \leq \text{dist}\left( \begin{pmatrix}
U_3 \\
U_3 \\
U_3
\end{pmatrix}, U \right) \leq \sqrt{8D}.
\] (20)

Now let us investigate $\text{dist}(\tilde{U}^*, U)$ further. If $Y_1$ and $Y_2 \in \mathbb{R}^{(2D-N)\times D}$ are chosen such that $[X_1, X_2][Y_1, Y_2] = 0$, then using $X_1 + X_2 + X_3 = 0$, there exist $L \in \mathbb{R}^{D \times (3D-N)}$, $K \in \mathbb{R}^{(k-D) \times (3D-N)}$ and an orthogonal matrix $U'_3 \in \mathbb{R}^{k \times k}$ such that
\[
\tilde{U}^* = \begin{pmatrix}
I + LY_1 & KY_1 \\
I + LY_2 & KY_2 \\
0 & 0
\end{pmatrix} U'_3.
\] (21)

That is, if we write $\tilde{U}^* = \begin{pmatrix} \tilde{U}_1^* \\ \tilde{U}_2^* \\ \tilde{U}_3^* \end{pmatrix}$, then
\[
\tilde{U}_1^* = (I + LY_1, KY_1) U'_3, \quad \tilde{U}_2^* = (I + LY_2, KY_2) U'_3, \quad \tilde{U}_3^* = U_3
\]
($\tilde{U}_3^* = U_3$ follows from definition of $\tilde{U}$). Since for any $U_1 \in \mathbb{R}^{k \times D}$ with SVD decomposition $U_1 = U_1 \Sigma U_1 V_1^T$, the closest orthogonal matrix in $\mathbb{R}^{k \times D}$ is given by $U U_1 V_1^T$, so the distance between $\tilde{U}^*$ and $U$ is
\[
\text{dist}(\tilde{U}^*, U) = \sqrt{\sum_{i=1}^3 \|\Sigma_{\tilde{U}^*_i} - I\|_F^2}.
\]

Applying (20), all singular values of $\tilde{U}_1$, $\tilde{U}_2$ and $\tilde{U}_3$ (i.e., all diagonal entries of $(\Sigma_{\tilde{U}^*_i})_{i=1}^3$) are smaller than $\sqrt{8D} + 1$. Let $C' = \sqrt{8D} + 2$, then dist($U, \tilde{U}$) can be controlled as follows:
\[
C'^2 \text{dist}^2(U, \tilde{U}) = C'^2 \text{dist}^2(\tilde{U}^*, U) \geq C'^2 \text{dist}^2(\tilde{U}^*, U) = C'^2 \sum_{i=1}^3 \|\Sigma_{\tilde{U}^*_i} - I\|_F^2 \\
\geq \sum_{i=1}^3 \|\Sigma_{\tilde{U}^*_i} - I\|_F^2 = \|\tilde{U}_1^* U_1^T - I\|_F^2 + \|\tilde{U}_2^* U_2^T - I\|_F^2 + \|\tilde{U}_3^* U_3^T - I\|_F^2 \\
= (\|LY_1 + Y_1^T L^T - Y_1^T (L^T L + K^T K) Y_1\|_F^2 \\
+ \|LY_2 + Y_2^T L^T - Y_2^T (L^T L + K^T K) Y_2\|_F^2) \\
\geq (\min(0, \lambda_{\min}(LY_1 + Y_1^T L^T)))^2 + (\min(0, \lambda_{\min}(LY_2 + Y_2^T L^T)))^2,
\] (22)

where the last inequality follows from the observation that $Y_1^T (L^T L + K^T K) Y_1$ and $Y_2^T (L^T L + K^T K) Y_2$ are positive semidefinite, and for any symmetric
Considering that \( \|LX + Y \|_F \geq -\frac{C'}{C_{\sigma_{min}(X)}} \lambda_{min}(LX) \) and \( \lambda_{min}(LY_2 + Y_2^T L^T) \geq -\frac{C'}{C_{\sigma_{min}(X)}} \lambda_{min}(LY_2) \), which violates (22) and (19). Therefore, by contradiction we proved the smallest eigenvalue, then \( \|L\|_F \leq \epsilon \) for generic \( Y \) and \( Z \) where \( c(Y, Z) > 0 \) for generic \( Y \) and \( Z \).

The proof of Lemma 4.1 is rather technical and deferred to Section 4.3. Applying Lemma 4.1 for generic \( Y_1 \) and \( Y_2 \) (and as a result, for generic \( X_1 \) and \( X_2 \)) there exists \( C_1 \) depending on \( Y_1 \) and \( Y_2 \) such that \( \|L\|_F \leq C_1 \|XU\|_F \). In addition, we have

\[
\|LY_1 + Y_1^T L^T - Y_1^T (L^T L + K^T K) Y_1\|_F \\
\geq \|Y_1^T K Y_1\|_F - \|Y_1^T L Y_1\|_F - \|LY_1 + Y_1^T L^T\|_F,
\]

and \( \|Y_1^T K Y_1\|_F \geq -\frac{1}{\sqrt{\beta}} \text{tr}(Y_1^T K Y_1) = -\frac{1}{\sqrt{\beta}} \|K Y_1\|_F^2 \). As a result, there exists \( C_2 \) depending on \( Y_1, Y_2, X \) such that if \( \|K Y_1\|_F > C_2 \sqrt{\|XU\|_F} \) then

\[
\|LY_1 + Y_1^T L^T - Y_1^T (L^T L + K^T K) Y_1\|_F \geq \frac{C'}{C_{\sigma_{min}(X)}} \frac{\|XU\|_F}{\sqrt{\|X^2\|_F}}
\]

which violates (22) and (19). Therefore, by contradiction we proved \( \|K Y_1\|_F \leq C_2 \sqrt{\|XU\|_F} \), and similarly \( \|K Y_2\|_F \leq C_2 \sqrt{\|XU\|_F} \). Combining it with \( \|L\|_F \leq C_1 \|XU\|_F \), we have

\[
\|U^T P_{L^+}\|_F = \|U^T P_{L^+}\|_F = \left(\begin{array}{ccc} (LY_1)^T & (LY_2)^T & 0 \\ (KY_1)^T & (KY_2)^T & 0 \end{array}\right) \|P_{L^+}\|_F
\]

\[
\leq \left(\begin{array}{ccc} (LY_1)^T & (LY_2)^T & 0 \\ (KY_1)^T & (KY_2)^T & 0 \end{array}\right) \|LY_1\|_F + \|LY_2\|_F + \|KY_1\|_F + \|KY_2\|_F
\]

\[
\leq (\|Y_1\| + \|Y_2\|)C_1 \|XU\|_F + 2C_2 \sqrt{\|XU\|_F}.
\]

Recall that \( C_1 \) and \( C_2 \) only depends on \( X_1 \) and \( X_2 \) (\( X, Y_1, \) and \( Y_2 \) are generated from \( X_1 \) and \( X_2 \)), combining (19) and (24) we have

\[
\|U^T P_{L^+}\|_F \leq \|U^T P_{L^+}\|_F + \|U - U^*\| P_{L^+}\|_F \leq \|U^T P_{L^+}\|_F + \|U - U^*\|_F
\]

\[
\leq (\|Y_1\| + \|Y_2\|)C_1 \|XU\|_F + 2C_2 \sqrt{\|XU\|_F} + \frac{1}{\sqrt{\|X\|_F}} \|XU\|_F.
\]

Considering that \( \|U\| \leq 3 \) and \( \|XU\|_F \leq \|U\|\|X\|_F \leq 3\|X\|_F \), so if we let \( C_4 = 3\|X\|_F \), then

\[
\|U^T P_{L^+}\|_F \leq \left(\|Y_1\| + \|Y_2\|\right)C_1 \sqrt{C_4} + 2C_2 + \frac{1}{\sqrt{\|X\|_F}} \|XU\|_F
\]

13
and Theorem 2.1 is proved.

4.2.1. Proof of (18)
Suppose that \( \bar{U}^* = \arg \min_{\bar{U} \in \bar{U}} \text{dist}(\bar{U}, U) \) and \( U - \bar{U}^* = \begin{pmatrix} V_1 \\ V_2 \\ V_3 \end{pmatrix} \), where \( V_i \in \mathbb{R}^{D \times k} \) for \( i = 1, 2, 3 \), then
\[
\tilde{U} = \bar{U}^* + \begin{pmatrix} V_3 \\ V_3 \\ V_3 \end{pmatrix}
\]
would satisfy that \( \tilde{U} \in \tilde{U} \), and as a result,
\[
\text{dist}(U, \bar{U}) = \text{dist}(U, \bar{U}^*) = \sqrt{\|V_1\|^2_F + \|V_2\|^2_F + \|V_3\|^2_F} \geq C \sqrt{\|V_1 + V_3\|^2_F + \|V_2 + V_3\|^2_F}
\]
where \( C \) can be chosen to be \( 1/2 \).

4.3. Proof of Theorem 2.3

Proof. We start with the same argument as in the proof of Theorem 2.2 and assume \( V_i = -I \) for all \( 1 \leq i \leq K - 1 \) and \( \sum_{i=1}^{K} X_i = 0 \). Then the proof can be divided into three steps. First, we show that it is sufficient to prove that a property defined in (26) is satisfied for generic \( Y \in \mathbb{R}^{p \times KD} \) where \( p = \max((K - 1)D - N, 0) \). Then we establish that (26) indeed holds for generic \( Y \). To this end, secondly, we show that any \( Y \) that does not satisfy this property lies in a certain set. Finally, in the third step, we show that this set is of measure zero.

4.3.1. Step 1: reduction of the problem to the property (26)

By the assumption that \( V_i = -I \) for all \( 1 \leq i \leq K - 1 \), \( X_1 + \ldots + X_K = 0 \), and
\[
\text{tr} \left( H(I, \ldots, I) (I, \ldots, I)^\top \right) = \text{tr} \left( (I, \ldots, I) H(I, \ldots, I) \right) = \|X_1 + \ldots + X_K\|^2_F = 0.
\]
Considering that \( \text{tr}(HC) \geq 0 \) for any \( H \succ 0 \), if the solution to the SDP problem is not uniquely given by \( (I, \ldots, I) (I, \ldots, I) \), then there exists \( H \neq (I, \ldots, I) (I, \ldots, I) \) such that \( \text{tr}(CH) = 0 \). Let \( H = UU^\top \) for a matrix \( U \in \mathbb{R}^{KD \times k} \), then using the properties of \( H \), we have \( U \in \mathcal{U} \) for
\[
\mathcal{U} = \left\{ U = \begin{pmatrix} U_1 \\ \vdots \\ U_K \end{pmatrix} : U_i \in \mathbb{R}^{D \times k}, U_i U_i^\top = I, \forall 1 \leq i \leq K, P_{t_i} U \neq 0 \right\},
\]
L_1 defined by

\[ L_1 = \{ z \in \mathbb{R}^{KD} : z = (x, x, \ldots, x) \text{ for some } x \in \mathbb{R}^D \}, \]

and \( P_{L_1}^\top U \neq 0 \) means that \( U_1, U_2, \cdots, U_K \) are not all the same.

Since \( \text{tr}(CH) = 0 \), we have \( \|XU\|_F = 0 \). Let \( \text{Sp}(A) \) and \( \text{Col}(A) \) be the subspaces spanned by the row vectors of \( A \) and the column vectors of \( A \) respectively, then

\[ \text{Sp}(X) \perp \supseteq \text{Col}(U). \] (25)

For any two subspace \( L \) and \( L' \), we use \( L + L' \) to represent the subspace \( \{ x + y : x \in L, y \in L' \} \), then we claim that to prove Theorem 2.3, it is sufficient to prove the following statement with \( p = \max((K-1)D - N, 0) \):

For generic \( Y \in \mathbb{R}^{p \times KD} \), \( \text{Col}(U) \not\subseteq \text{Sp}(Y) + L_1 \) for every \( U \in \mathcal{U} \). (26)

The argument is as follows. Since \( \sum_{i=1}^K X_i = 0 \),

\[ \dim(\text{Sp}(X)) = \text{rank}(X) = \text{rank}([X_1, X_2, \ldots, X_{K-1}, X_K]) \]

\[ = \text{rank}([X_1, X_2, \ldots, X_{K-1}]), \]

which is min \(( (K-1)D, N) \) for generic \( \{X_1\}_{i=1}^{K-1} \in \mathbb{R}^{N \times D} \), so \( \text{Sp}(X) \) is a generic min \(( (K-1)D, N) \)-dimensional subspace in \( L_1^\perp \) (and \( L_1^\perp \) is a subspace of \( \mathbb{R}^{KD} \)).

So, \( \text{Sp}(X) \perp \) is the sum of \( L_1 \) and a generic \( p \)-dimensional subspace in \( \mathbb{R}^{KD} \). Therefore, for generic \( \{X\}_{i=1}^{K-1} \), \( \text{Sp}(X) \perp \) is equivalent to \( \text{Sp}(Y) + L_1 \), where \( Y \) is a generic matrix of size \( p \times KD \). If \( (26) \) holds, then \( (25) \) would not hold for generic \( \{X\}_{i=1}^{K-1} \) and every \( U \in \mathcal{U} \). By the analysis before \( (25) \), the solution to the SDP problem is uniquely given by \((I, \ldots, I)^\top (I, \ldots, I)\), and Theorem 2.3 is proved.

4.3.2. Step 2: finding matrices that do not satisfy (26).

In this part we show that every \( Y \) violating \( (26) \) lies in the set \( \cup_{d=1}^p \mathcal{M}_d \), where \( \mathcal{M}_d \) is the range of the function

\[ g_d \left( \{Y_i\}_{i=0}^{K-1} , Z, L, L_0 \right) = P_L \left( [Y_1 P_{L_1}^\top, \cdots, Y_K P_{L_1}^\top] + [Y_0, \cdots, Y_0] \right) + P_{L_1}Z. \]

The domain of the function \( g_d \) is as follows: \( Y_i \in \mathbb{R}^{d \times d} \) for \( 1 \leq i \leq K - 1 \), \( Y_0 \in \mathbb{R}^{d \times D} \), \( Z \in \mathbb{R}^{(p-d) \times KD} \), \( L_0 \) is a \( d \)-dimensional subspace in \( \mathbb{R}^D \), and \( L \) is a \( d \)-dimensional subspace in \( \mathbb{R}^p \). In addition, \( Y_K = -\sum_{i=1}^{K-1} Y_i \).

For every \( Y \) violating \( (26) \), there exists \( U \in \mathcal{U} \) such that \( \text{Col}(U) \not\subseteq \text{Sp}(Y) + L_1 \). We let \( U = U^{(1)} + U^{(2)} \), where the columns of \( U^{(1)} \) lie in \( L_1 \) and the columns of \( U^{(2)} \) are orthogonal to \( L_1 \). As a result, \( \text{Col}(U^{(2)}) \) is a subspace in \( \mathbb{R}^{KD} \) that intersects \( L_1 \) only at origin, and we let \( d = \dim(\text{Col}(U^{(2)})) \). We have \( d \geq 1 \), since otherwise \( U^{(2)} \) is a zero matrix, and \( P_{L_1} U = P_{L_1}^\top U^{(1)} = 0 \), which contradicts \( U \in \mathcal{U} \).
Denote 
\[ U^{(1)} = \begin{pmatrix} U_1^{(1)} \\ \vdots \\ U_K^{(1)} \end{pmatrix} \] and 
\[ U^{(2)} = \begin{pmatrix} U_1^{(2)} \\ \vdots \\ U_K^{(2)} \end{pmatrix}, \]
then \( U_1^{(1)} = U_2^{(1)} = \cdots = U_K^{(1)} \). Recall for all \( 1 \leq i \leq K \), \( U_i^{(1)} U_i^{(1)\top} + U_i^{(2)\top} U_i^{(2)} = U_i U_i\top = I \), we have
\[ U_1^{(2)\top} U_1^{(2)} = U_2^{(2)\top} U_2^{(2)} = \cdots = U_K^{(2)\top} U_K^{(2)}. \]
Therefore,
\[ \text{Col} \left( U_1^{(2)} \right) = \text{Col} \left( U_2^{(2)} \right) = \cdots = \text{Col} \left( U_K^{(2)} \right), \] (27)
and
\[ \dim \left( \text{Col}(U_1^{(2)}) \right) = \text{rank} \left( U_1^{(2)} \right) \leq \text{rank} \left( U^{(2)} \right) = \dim \left( \text{Col}(U^{(2)}) \right) = d. \]

Since \( \text{Col}(U) = \text{Col}(U^{(2)}) + \text{Col}(U^{(1)}) \), and \( \text{Col}(U^{(1)}) \subseteq L_1 \), the assumption \( \text{Sp}(Y) + L_1 \supseteq \text{Col}(U) \) is equivalent to \( \text{Sp}(Y) + L_1 \supseteq \text{Col}(U^{(2)}) \). Recall \( \dim(\text{Sp}(Y)) \leq p \), and \( \text{Col}(U^{(2)}) \) is a subspace in \( \mathbb{R}^{K D} \) that intersects \( L_1 \) only at origin, we have \( d \leq p \).

Apply \( \text{Sp}(Y) + L_1 \supseteq \text{Col}(U^{(2)}) \) and \( \dim(\text{Col}(U^{(2)})) = d \), there exists \( Y_0 \in \mathbb{R}^{d \times D} \) and \( L \), a \( d \)-dimensional subspace in \( \mathbb{R}^{p} \), such that
\[ \text{Sp} \left( P_L \left[ Y - ( Y_0, Y_0, \cdots, Y_0) \right] \right) = \text{Col} \left( U^{(2)} \right). \] (28)
Recall the property (27), there exists \( Y_i \in \mathbb{R}^{d \times d} \) for \( 1 \leq i \leq K \) and \( L_0 \), a \( d \)-dimensional subspace in \( \mathbb{R}^{d} \) that contains \( \text{Sp}(U_1^{(2)\top}) \), such that
\[ P_L \left[ Y - ( Y_0, Y_0, \cdots, Y_0) \right] = ( Y_1 P_{L_0}, Y_2 P_{L_0}, \cdots, Y_K P_{L_0}^\top). \] (28)
In addition, since \( \text{Col}(U^{(2)}) \) is orthogonal to \( L_1 \),
\[ Y_K = - \sum_{i=1}^{K-1} Y_i. \] (29)
Combining (28), (29), and the estimation \( 1 \leq d \leq p \), every \( Y \) that does not satisfy (26) lies in the set \( \bigcup_{d=1}^{p} M_d \).

4.3.3. Step 3: counting the dimension of \( M_d \)
In this step, we count the dimensions of \( M_d \) for all \( 1 \leq d \leq p \), and show that they are smaller than \( p K D \), the dimension of \( \mathbb{R}^{p \times K D} \), which implies that generic \( Y \in \mathbb{R}^{p \times K D} \) does not belong to \( \bigcup_{d=1}^{p} M_d \), and (26) is proved.
For any \( d \), the degree of freedom is \( \{ Y_i \}_{j=1}^{K-1} \) is \( (K - 1)d^2 \), the degree of freedom of \( Y_0 \) is \( Dd \), the degree of freedom of \( Z \) is \( KD(p - d) \), the degree of
freedom of $L$ and $L_1$ are $d(p-d)$ and $d(D-d)$ respectively. Considering that $d \leq p \leq D-1$, the total dimension of $\mathcal{M}_d$ is smaller than $KDp$, the dimension of $\mathbb{R}^{p\times KD}$. Since $g_d$ is smooth and the dimension of its range is larger than its domain, all elements in $\mathcal{M}_d$ are its critical values. Applying [17, Theorem 6.8], $\mathcal{M}_d$ has measure zero in $\mathbb{R}^{KD\times(D-1)}$. Therefore, $\mathbb{R}^{D-1\times KD \setminus \mathcal{M}_d}$ is dense.

Since $\mathbb{R}^{D-1\times KD \setminus \mathcal{M}_d}$ is a closed set, generic $Y$ does not lie in the set $\mathcal{M}_d$. Combining this result for all $1 \leq d \leq p$, generic $Y$ does not lie in the set $\cup_{d=1}^{p} \mathcal{M}_d$.

### 4.4. Proof of Lemma 4.1

We first state two lemmas that are rather easy to verify.

**Lemma 4.2.** When $A \in \mathbb{R}^{m \times n}$, $B \in \mathbb{R}^{n \times l}$, where $l \geq n$ and the singular values of $B$ are $\sigma_1 \geq \sigma_2 \geq \cdots \geq \sigma_n$, then

$$\sigma_n \|A\|_F \leq \|AB\|_F \leq \sigma_1 \|A\|_F. \quad (30)$$

**Proof.** First we claim that for any $x \in \mathbb{R}^n$,

$$\sigma_n^2 \|x\|^2 \leq \|x^\top B\|^2 \leq \sigma_1^2 \|x\|^2. \quad (31)$$

Assuming that the SVD decomposition of $B$ is given by $B = U_B \text{diag}(\sigma_1, \cdots, \sigma_n)V_B^\top$, then the first inequality in (31) can be proved as follows:

$$\|x^\top B\|^2 = x^\top BB^\top x = x^\top U_B \text{diag}(\sigma_1^2, \cdots, \sigma_n^2)U_B^\top x \geq \sigma_n^2 \|x\|_2^2 = \sigma_n^2 \|x\|^2,$$

and second inequality in (31) can be proved similarly.

Assuming that $A = (a_1, \ldots, a_m)$, and combining (31) with $x = a_i$ for $1 \leq i \leq m$, (30) is proved.

**Lemma 4.3.** The smallest eigenvalue of

$$\begin{pmatrix} a & b \\ b & 0 \end{pmatrix}$$

is smaller than

$$- \frac{b^2}{\max(a, 0) + |b|}.$$

**Proof.** The smaller eigenvalue is

$$\frac{a - \sqrt{a^2 + 4b^2}}{2} = - \frac{2b}{a + \sqrt{a^2 + 4b^2}} \leq - \frac{2b}{a + (|a| + 2|b|)} = - \frac{b^2}{\max(a, 0) + |b|}.$$

**Proof of Lemma 4.1.** First of all, WLOG we may assume that

$$Y = \begin{pmatrix} I_{M \times M} \\ 0_{M \times D-M} \end{pmatrix}. \quad (32)$$
If we proved the case (32), then other cases can be proved as follows. For generic $Y$, there are invertible matrices $B \in \mathbb{R}^{M \times M}$ and $A \in \mathbb{R}^{D \times D}$ such that

$$BYA = \begin{pmatrix} I_{M \times M} \\ 0_{M \times D-M} \end{pmatrix}.$$ 

Note that

$$(A^T L B^{-1})(BYA) + (BYA)^T (A^T L B^{-1})^T = A^T (LY + Y^T L^T) A,$$

we have

$$\lambda_{\min}( (ALB^{-1})(BYA) + (BYA)^T (ALB^{-1})^T ) \geq -\|A\|^2 \epsilon,$$

and similarly

$$\lambda_{\min}( (ALB^{-1})(BZA) + (BZA)^T (ALB^{-1})^T ) \geq -\|A\|^2 \epsilon.$$

Since the case (32) is assumed to be proved,

$$\|ALB^{-1}\|_F \leq \epsilon \|A\|^2 c(Y,Z),$$

Applying Lemma 4.2, $\|ALB^{-1}\|_F \geq \|L\|_F \sigma_{\min}(A)/\|B\|$, and the generic case is proved with $c(Y,Z) = \|A\|^2 \sigma_{\min}(A) c(BYA,BZA)$, which is positive for generic $Z$ since $c(BYA,BZA)$ is positive for generic $BZA$.

The rest of the proof will assume (32) and use induction on $k$, which is the integer such that $k(D-M) < M \leq (k+1)(D-M)$. For $k = 1$, let us denote

$$L = \begin{pmatrix} L_1 \\ L_2 \end{pmatrix}, \quad Z = (Z_1, Z_2),$$

where $L_1, Z_1 \in \mathbb{R}^{M \times M}$, $L_2 \in \mathbb{R}^{M \times (D-M)}$, and $Z_2 \in \mathbb{R}^{(D-M) \times M}$. Then

$$LY + Y^T L^T = \begin{pmatrix} L_1 + L_1^T \\ L_2 \\ 0 \end{pmatrix}.$$

If $\|L_2\| = b$ and $\|L_1\| = a$, then there exists $u \in \mathbb{R}^M, v \in \mathbb{R}^{D-M}$ such that $\|u\| = \|v\| = 1$ and $u^T L_2 v = b$. Then

$$\begin{pmatrix} u \\ 0 \end{pmatrix} (LY + Y^T L^T) \begin{pmatrix} u \\ 0 \end{pmatrix}^T = \begin{pmatrix} u^T (L_1 + L_1^T) u & b \\ b & 0 \end{pmatrix},$$

and its smallest eigenvalue is larger than $-\epsilon$ since $\begin{pmatrix} u \\ 0 \end{pmatrix}^T \begin{pmatrix} u \\ 0 \end{pmatrix} = I$. Applying Lemma 4.3 with the estimation $u^T (L_1 + L_1^T) u \leq 2a$, we have

$$b^2 \leq \epsilon (2a + b).$$
In another aspect, applying Lemma 4.2 we have

For generic $Z, C_1 \| L_1 \|_F \geq \| L_1 Z_2 \|_F \geq C_2 \| L_1 \|_F$ for some $C_1, C_2 > 0$.

Therefore, we can find $u \in \mathbb{R}^M$ and $v \in \mathbb{R}^{N-M}$ such that $|u^T(L_1 Z_2)v| \geq C_2 a$. Note that

$$
\begin{pmatrix}
u & v \\
0 & v
\end{pmatrix}
(L Z + Z^T L^T)
\begin{pmatrix}
u & v \\
0 & v
\end{pmatrix}^T
= (u^T(L_1 Z_1 + Z_1^T L_1^T)u - u^T(Z_2^T L_1^T)v) + L',
$$

where $\|L'\| < C_3 b$. Since $|u^T(L_1 Z_1 + Z_1^T L_1^T)u| \leq C_4 a$ for some $C_4 > 0$, Lemma 4.3 shows that the smallest eigenvalue of

$$
\begin{pmatrix}
u & v \\
0 & v
\end{pmatrix}
(L Z + Z^T L^T)
\begin{pmatrix}
u & v \\
0 & v
\end{pmatrix}
$$

is smaller than

$$
-\frac{C_2^2}{C_4 + C_1} a.
$$

Let $C_4' = \frac{C_2^2}{C_4 + C_1}$, applying $\lambda_{\min}(L Z + Z^T L^T) \geq -\epsilon$ we have

$$
C_3 b - C_4' a > -\epsilon. \tag{34}
$$

This means $a < \frac{1}{C_4'} (C_3 b + \epsilon)$. Plug it into (33), we have

$$
b^2 \leq \epsilon(b + 2a) \leq \epsilon \left(b + \frac{2}{C_4'} (C_3 b + \epsilon)\right) = \epsilon \left(1 + \frac{2C_3}{C_4'}\right)b + \frac{2}{C_4'} \epsilon^2,
$$

which implies that $b < C \epsilon$. Applying (34), we also have $a < C' \epsilon$ and the Lemma is proved for $k = 1$.

For $k > 1$, let us first write

$$
L = \begin{pmatrix}
L_{1,1} & L_{1,2} \\
L_{2,1} & L_{2,2}
\end{pmatrix},
$$

where $L_{1,1} \in \mathbb{R}^{M \times (2M-D)}, L_{1,2} \in \mathbb{R}^{M \times (D-M)}, L_{2,1} \in \mathbb{R}^{(D-M) \times (2M-D)}, L_{2,2} \in \mathbb{R}^{(D-M) \times (D-M)}$ and similarly write

$$
Z = \begin{pmatrix}
Z_{1,1} & Z_{1,2} \\
Z_{2,1} & Z_{2,2}
\end{pmatrix},
$$

where $Z_{1,1} \in \mathbb{R}^{(2M-D) \times M}, Z_{1,2} \in \mathbb{R}^{(D-M) \times M}, Z_{2,1} \in \mathbb{R}^{(2M-D) \times (D-M)}, Z_{2,2} \in \mathbb{R}^{(D-M) \times (D-M)}$. WLOG we may assume that $Z_{1,2} = 0$, by finding an appropriate orthogonal matrix $A \in \mathbb{R}^{M \times M}$ and consider $(LA', AY, AY)$ instead of $(L, Y, Z)$, then

$$
Z = \begin{pmatrix}
Z_{1,1} & 0 \\
Z_{2,1} & Z_{2,2}
\end{pmatrix},
$$

19
and for generic $Z$, $Z_{2,2}$ is full-rank, i.e., the rank is $D-M$. Let $b = \|([L_{2,1}, L_{2,2}])_{F}$, $a_1 = \|L_{1,1}\|_{F}$ and $a_2 = \|L_{1,2}\|_{F}$. Then following the proof of (33), applying $\lambda_{\text{min}}(LY + Y^\top L^\top) \geq -\epsilon$ we have

$$\frac{b^2}{a_1 + a_2 + b} \leq \epsilon.$$  

(35)

If another aspect,

$$LZ + Z^\top L^\top = \begin{pmatrix} L_{1,1}Z_{1,1} + L_{1,2}Z_{2,1} + Z_{1,1}^\top L_{1,1}^\top + Z_{1,2}^\top L_{2,1}^\top & L_{1,2}Z_{2,2} \\ Z_{2,2}^\top L_{1,2}^\top & 0 \end{pmatrix} + L^\prime,$$

where $\|L^\prime\| < C_1b$. Again Lemma 4.2 means that we have $C_2a_2 \leq \|L_{1,2}Z_{2,2}\| \leq C_3a_2$ and $\|L_{1,1}Z_{1,1} + L_{1,2}Z_{2,1} + Z_{1,1}^\top L_{1,1}^\top + Z_{1,2}^\top L_{2,1}^\top\| \leq C_4(a_1 + a_2)$. Lemma 4.3 then implies

$$\frac{C_2a_2^2}{C_4(a_1 + a_2) + C_3a_2} \leq \epsilon + C_1b.$$  

(36)

At last, note that $L_{1,1}Z_{1,1} + L_{1,2}Z_{2,1} + Z_{1,1}^\top L_{1,1}^\top + Z_{1,2}^\top L_{2,1}^\top$ is a submatrix of $LZ + Z^\top L^\top$, so its smallest eigenvalue is also larger than $-\epsilon$. Since there exists $C_5$ such that $\|L_{1,2}Z_{2,1} + Z_{1,2}^\top L_{2,1}^\top\| \leq C_5a_2$, the smallest eigenvalue of $L_{1,1}Z_{1,1} + Z_{1,1}^\top L_{1,1}^\top$ is larger than $-\epsilon - C_5a_2$. Let

$$Y_{1,1} = \begin{pmatrix} I_{(2M-D) \times (2M-D)} \\ 0_{(2M-D) \times (D-M)} \end{pmatrix}$$

and using the same argument, the smallest eigenvalue of $L_{1,1}Z_{1,1} + Z_{1,1}^\top L_{1,1}^\top$ is larger than $-\epsilon - C_5a_2$. Since $(k-1)(D-M) < 2M-D \leq k(D-M)$, we may apply the case $k-1$ to $L_{1,1}$, $Y_{1,1}$ and $Z_{1,1}$ and have

$$a_1 \leq C_6((C_5 + C_5')a_2 + \epsilon).$$  

(37)

Plug in (37) to (35) and (36) we have

$$b^2 \leq \epsilon C_7(\epsilon + a_2 + b)$$  

(38)

and

$$a_2^2 \leq C_8(\epsilon + a_2)(\epsilon + b), \text{ i.e., } a_2(a_2 - C_8b) \leq \epsilon C_8(\epsilon + a_2 + b).$$  

(39)

If $a_2 \geq 2C_8b$, then (39) implies

$$\frac{1}{2}a_2^2 \leq \epsilon C_8(\epsilon + a_2 + \frac{1}{2C_8}a_2),$$

which implies $a_2 \leq C \epsilon$. This then implies $b \leq C' \epsilon$ (from assumption) and $a_1 \leq C'' \epsilon$ (from (37)).

If $a_2 < 2C_8b$, then (38) implies $b < C \epsilon$, which then implies $a_1, a_2 < C' \epsilon$.

For either case we have $a_1 + a_2 + b < C'' \epsilon$, and Lemma 4.1 is proved since $\|L\|_{F} \leq \|L_{1,1}\|_{F} + \|L_{1,2}\|_{F} + \|(L_{2,1}, L_{2,2})\|_{F} = a + b + c$. 

□

20
Acknowledgment

The authors were partially supported by Award Number R01GM090200 from the NIGMS, FA9550-12-1-0317 and FA9550-13-1-0076 from AFOSR, LTR DTD 06-05-2012 from the Simons Foundation, and the Moore Foundation Data-Driven Discovery Investigator Award. The authors would like to thank the anonymous reviewers for their helpful comments and suggestions.

References

[1] J. Gower, G. Dijksterhuis, Procrustes Problems, Oxford Statistical Science Series.

[2] A. S. Bandeira, C. Kennedy, A. Singer, Approximating the little Grothendieck problem over the orthogonal and unitary groups, Mathematical Programming (2016) 1–43.

[3] A. Nemirovski, Sums of random symmetric matrices and quadratic optimization under orthogonality constraints, Mathematical Programming 109 (2-3) (2007) 283–317.

[4] M. X. Goemans, D. P. Williamson, Improved approximation algorithms for maximum cut and satisfiability problems using semidefinite programming, J. ACM 42 (6) (1995) 1115–1145.

[5] J. Gower, Generalized procrustes analysis, Psychometrika 40 (1) (1975) 33–51.

[6] J. Ten Berge, Orthogonal procrustes rotation for two or more matrices, Psychometrika 42 (2) (1977) 267–276.

[7] A. Shapiro, J. D. Botha, Dual algorithm for orthogonal procrustes rotations, SIAM Journal on Matrix Analysis and Applications 9 (3) (1988) 378–383.

[8] A. S. Bandeira, C. Kennedy, A. Singer, Approximating the little grothendieck problem over the orthogonal and unitary groups, Mathematical Programming 160 (1) (2016) 433–475.

[9] Z. Kam, The reconstruction of structure from electron micrographs of randomly oriented particles, Journal of Theoretical Biology 82 (1) (1980) 15 – 39.

[10] T. Bhamre, T. Zhang, A. Singer, Orthogonal matrix retrieval in cryo-electron microscopy, 12th IEEE International Symposium on Biomedical Imaging (ISBI 2015).
[11] A. M.-C. So, J. Zhang, Y. Ye, On approximating complex quadratic optimization problems via semidefinite programming relaxations, Math. Program. 110 (1) (2007) 93–110.

[12] A.-C. So, Moment inequalities for sums of random matrices and their applications in optimization, Mathematical Programming 130 (1) (2011) 125–151.

[13] A. Naor, O. Regev, T. Vidick, Efficient rounding for the noncommutative grothendieck inequality, in: Proceedings of the Forty-fifth Annual ACM Symposium on Theory of Computing, STOC ’13, 2013, pp. 71–80.

[14] J. B. Keller, Closest unitary, orthogonal and Hermitian operators to a given operator, Mathematics Magazine 48 (4) (1975) 192–197.

[15] M. Grant, S. Boyd, CVX: Matlab software for disciplined convex programming, version 2.1, http://cvxr.com/cvx (Mar. 2014).

[16] H. R. Tüttüncü, C. K. Toh, J. M. Todd, Solving semidefinite-quadratic-linear programs using sdpt3, Mathematical Programming 95 (2) (2003) 189–217.

[17] J. Lee, Introduction to Smooth Manifolds, Graduate Texts in Mathematics, Springer, 2003.