Improving Robustness of Deep-Learning-Based Image Reconstruction - Supplementary Material

Proof of Theorem 1:
For the inverse problem of recovering the true x from the measurement $y = Ax$, goal is to design a robust linear recovery model given by $\hat{x} = BAx$

The min-max formulation to get robust model for a linear set-up:

$$\min_B \max_{\delta:\|\delta\|_2\leq\epsilon} \mathbb{E}_{x\in D}\|BAx - x\|^2 + \lambda\|B(Ax+\delta) - x\|^2$$

$$\min_B \max_{\delta:\|\delta\|_2\leq\epsilon} \mathbb{E}_{x\in D}(1+\lambda)\|BAx - x\|^2 + \lambda\|B\delta\|^2 + 2\lambda(B\delta)^T(BAx - x) \tag{1}$$

Since the data is normalized, i.e., $\mathbb{E}(x) = 0$ and $cov(x) = I$. This makes the above optimization problem as:

$$\min_B \max_{\delta:\|\delta\|_2\leq\epsilon} \mathbb{E}_{x\in D}(1+\lambda)\|(BA - I)x\|^2 + \lambda\|B\delta\|^2$$

$$\min_B \max_{\delta:\|\delta\|_2\leq\epsilon} \mathbb{E}_{x\in D}(1+\lambda)tr(BA - I)xx^T(BA-I)^T + \lambda\|B\delta\|^2 \tag{2}$$

Since, $\mathbb{E}(tr(\cdot)) = tr(\mathbb{E}(\cdot))$, the above problem becomes:

$$\min_B \max_{\delta:\|\delta\|_2\leq\epsilon} (1+\lambda)tr(BA - I)(BA-I)^T + \lambda\|B\delta\|^2$$

$$\min_B \max_{\delta:\|\delta\|_2\leq\epsilon} (1+\lambda)\|BA - I\|_F^2 + \lambda\|B\delta\|^2 \tag{3}$$

Using SVD decomposition of $A = USV^T$ and $B = MQP^T$

$$\min_{M,Q,P:M^TM=I,P^TP=I,Q \text{ is diag}} \max_{\delta:\|\delta\|\leq\epsilon} (1+\lambda)\|MQP^TUSV^T - I\|_F^2 + \lambda\|MQP^T\delta\|^2 \tag{4}$$

Since, only the second term is dependent on δ, maximizing the second term with respect to δ:
We have $\|MQP^T\delta\| = \|QP^T\delta\|$ since M is unitary. Given Q is diagonal, $\|QP^T\delta\|$ w.r.t. δ can be maximized by having $P^T\delta$ vector having all zeros except the location corresponding to the $\max_i Q_i$. Since, $\|P^T\delta\| = \|\delta\|$, again because P is unitary, so to maximize within the ϵ-ball, we will have $P^T\delta = \epsilon[0,..,0,1,0,..,0]$ where 1 is at the $\arg max_i Q_i$ position. This makes the term to be:

$$\max_{\delta:\|\delta\|_2\leq\epsilon} \|MQP^T\delta\|^2 = \epsilon^2(\max_i Q_i)^2$$

Substituting the above term in Equation 4:

$$\min_{M,Q,P:M^TM=I,P^TP=I,Q \text{ is diag}} (1+\lambda)\|MQP^TUSV^T - I\|_F^2 + \lambda\epsilon^2(\max_i Q_i)^2$$

$$\min_{M,Q,P:..} (1+\lambda)tr(MQP^TUSV^T - I)(MQP^TUSV^T - I)^T + \lambda\epsilon^2(\max_i Q_i)^2$$

$$\min_{M,Q,P:..} (1+\lambda)tr(MQP^TUS^2U^TPQM^T - 2MQP^TUSV^T + I) + \lambda\epsilon^2(\max_i Q_i)^2$$

$$\min_{M,Q,P:..} (1+\lambda)tr(P^TUS^2U^TPQ^2 - 2MQP^TSV^T + I) + \lambda\epsilon^2(\max_i Q_i)^2 \tag{5}$$

For the above equation, only the second term depends on M, minimizing the second term w.r.t. M keeping others fixed:

$$\min_{M:M^TM=I} tr(-2MQP^TUSV^T)$$

Since, this is a linear program with the quadratic constraint, relaxing the constraint from $M^TM = I$ to $M^TM \leq I$ won't change the optimal point as the optimal point will always be at the boundary i.e. $M^TM = I$

$$
\begin{aligned}
\min_{M:M^TM\leq I} tr(-2MQP^TUSV^T) & \text{ which is a convex program} \\
\text{Introducing the Lagrange multiplier matrix } K \text{ for the constraint} \\
\mathcal{L}(M,K) = tr(-2MQP^TUSV^T + K(M^TM - I)) \\
\text{Substituting } G = QP^TUSV^T \text{ and using stationarity of Lagrangian} \\
\Delta L_M = M(K+K^T) - G^T = 0 \implies ML = G^T \text{ where } L = K+K^T \\
\text{Primal feasibility: } M^TM \leq I. \text{ Optimal point at boundary } \implies \mathrm{M}^TM = I
\end{aligned}
$$

Because of the problem is convex, the local minima is the global minima which satisfies the two conditions: Stationarity of Lagrangian ($ML = G^T$) and Primal feasibility ($M^TM = I$). By the choice of $M = V$, and $L = SU^TPQ$, both these conditions are satisifed implying $M = V$ is the optimal point.
Substituting $M = V$ in Equation 5, we get:

$$
\begin{aligned}
\min_{Q,P:..} (1+\lambda)tr(P^TUS^2U^TPQ^2 - 2VQP^TUSV^T + I) + \lambda\epsilon^2(\max_i Q_i)^2 \\
\min_{Q,P:..} (1+\lambda)tr(P^TUS^2U^TPQ^2 - 2QP^TUS + I) + \lambda\epsilon^2(\max_i Q_i)^2 \\
\min_{Q,P:..} (1+\lambda)\|QP^TUS - I\|_F^2 + \lambda\epsilon^2(\max_i Q_i)^2
\end{aligned} \tag{6}
$$

Denote the i-th column of $C = U^TP$ by c_i and the entries in Q are in decreasing order (as entries in S are in increasing order) and the largest entry q_m in Q, has multiplicity m, the Equation 6 becomes:

$$
\min_{C,Q}(1+\lambda)\sum_{i=1}^{m}\|q_mSc_i - e_i\|^2 + \lambda\epsilon^2q_m^2 + (1+\lambda)\sum_{i=m+1}^{n}\|q_iSc_i - e_i\|^2 \tag{7}
$$

If we consider the last term i.e. $i > m$, it can be minimized by setting $c_i = e_i$ which is equivalent to choose $P_i = U_i$ and $q_i = 1/s_i$. This makes the last term ($= 0$), using $h = \lambda\epsilon^2/(1+\lambda)$, making the Equation 7 as:

$$
\begin{aligned}
\min_{C,Q}\sum_{i=1}^{m}(c_i^TSq_m^2Sc_i - 2e_i^Tq_mSc_i + e_i^Te_i) + hq_m^2 \\
\min_{C,Q} q_m^2(\sum_{i=1}^{m}c_i^TS^2c_i + h) - 2q_m\sum_{i=1}^{m}S_iC_{ii} + \sum_{i=1}^{m}e_i^Te_i
\end{aligned}
$$

The above term is upward quadratic in q_m, minima w.r.t. q_m will occur at $q_m^* = \frac{\sum_{i=1}^m S_iC_{ii}}{(\sum_{i=1}^m c_i^TS^2c_i + h)}$, which will make the quadratic term as $\sum_{i=1}^m e_i^Te_i - \frac{(\sum_{i=1}^m S_iC_{ii})^2}{(\sum_{i=1}^m c_i^TS^2c_i + h)}$, which has to be minimized w.r.t C

$$
\begin{aligned}
\min_C \sum_{i=1}^{m} e_i^Te_i - \frac{(\sum_{i=1}^m S_iC_{ii})^2}{(\sum_{i=1}^m c_i^TS^2c_i + h)} \\
\max_C \frac{(\sum_{i=1}^m S_iC_{ii})^2}{(\sum_{i=1}^m c_i^TS^2c_i + h)} \\
\max_C \frac{(\sum_{i=1}^m S_iC_{ii})^2}{\sum_{i=1}^m S_i^2C_{ii}^2 + \sum_{j\neq i} S_j^2C_{ij}^2 + h}
\end{aligned} \tag{8}
$$

Since $C = U^TP \implies C_{ij} = u_i^Tp_j \implies \|C_{ij}\| \leq 1$. To maximize the term given by the Equation 8, we can minimize the denominator by setting the term $C_{ij} = 0$, which makes the matrix C as diagonal.
Divide the matrix U and P into two parts: one corresponding to $i \leq m$ and another $i > m$, where i represents the column-index of $C = U^TP$.

Let $U = [U_1|U_2]$ and $P = [P_1|P_2]$. From above, we have $P_2 = U_2$ for $i > m$, making $P = [P_1|U_2]$.

$$U^T = \begin{bmatrix} U_1^T \\ \hline U_2^T \end{bmatrix} \text{ and } P = [P_1|U_2]$$
$$U^T P = \begin{bmatrix} U_1^T P_1 & U_1^T U_2 \\ U_2^T P_1 & U_2^T U_2 \end{bmatrix} = \begin{bmatrix} U_1^T P_1 & \mathbf{0} \\ U_2^T P_1 & I \end{bmatrix}$$

Since, $U^T P$ is diagonal, we have $U_2^T P_1 = \mathbf{0}$, $U_1^T P_1 = \Gamma$ where Γ is diagonal. Also, we have $P_1^T P_1 = I$. Only way to satisfy this would be making $P_1 = U_1$ which makes $P = U$ and $C = I$. It also results in

$$q_m^* = \frac{\sum_{i=1}^m S_i}{\sum_{i=1}^m S_i^2 + h}, \text{ where, } h = \epsilon^2 \frac{\lambda}{1+\lambda} \tag{9}$$

Hence, the resulting B would be of the form MQP^T where:

$$M = V, P = U \text{ and },\tag{10}$$
$$Q = \begin{bmatrix} q_m^* & 0 & \dots & 0 \\ 0 & q_m^* & .. & 0 \\ \vdots & \vdots & \vdots & \vdots \\ \vdots & \vdots & \vdots & \vdots \\ 0 & \dots & 1/s_{m+1} & .. \\ \vdots & \vdots & \vdots & \vdots \\ \vdots & \vdots & \vdots & \vdots \\ 0 & \dots & 0 & 1/s_n \end{bmatrix} \tag{11}$$