1 Supplementary Material

This will cover the proofs required for checking eigenvalues of a symmetric matrix, checking the symmetric generalised eigenvalue problem and the protocol for fingerprinting the covariance matrix.

1.1 Details of Theorem 3

We use the fact that $\lambda_i \leq \|A\|_2$, and $\|v_i\|_2 = 1$. We also have $\|r\|_2 \leq \frac{\sqrt{n}}{2}$ and $|\rho| \leq \frac{1}{2}$, and so;

$$\begin{aligned}
\|TA\widehat{v_i} - \widehat{\lambda}_i\widehat{v_i}\|_\infty &\leq \sqrt{n}\|TA\widehat{v_i} - \widehat{\lambda}_i\widehat{v_i}\|_2 \\
&= \sqrt{n}\|T^2Av_i + TAr - T^2\lambda_i v_i - T\rho v_i - T\lambda_i r - \rho r\|_2 \\
&\leq \sqrt{n}(T\|A\|_2\|r\|_2 + T|\rho|\|v_i\|_2 + T|\lambda_i|\|r\|_2 + |\rho|\|r\|_2) \\
&\leq Tn\|A\|_F + \frac{T\sqrt{n}}{2} + \frac{n}{4} \\
\|\widehat{v_i}^T\widehat{v_j} - T^2\delta_{ij}\|_\infty &\leq \sqrt{n}\|\widehat{v_i}^T\widehat{v_j} - T^2\delta_{ij}\|_2 \\
&\leq \sqrt{n}\|(Tv_i + r)^T(Tv_j + r) - T^2\delta_{ij}\|_2 \\
&\leq \sqrt{n}\|Tv_i^T r + Tr^T v_j + r^T r\|_2 \\
&\leq 2T\sqrt{n}\|r\|_2 + \sqrt{n}\|r\|_2^2 \\
&\leq Tn + \frac{n\sqrt{n}}{4}
\end{aligned}$$

1.2 Details of Theorem 4

First define $\widetilde{v_i} = \frac{\widehat{v_i}}{T}$, $\widetilde{\lambda}_i = \frac{\widehat{\lambda}_i}{T}$, so we have;

$$\frac{\|TA\widehat{v_i} - \widehat{\lambda}_i\widehat{v_i}\|_\infty}{T^2} = \|A\widetilde{v_i} - \widetilde{\lambda}_i\widetilde{v_i}\|_\infty \geq \frac{\|A\widetilde{v_i} - \widetilde{\lambda}_i\widetilde{v_i}\|_2}{\sqrt{n}}$$

As A is symmetric, we can write $A = VDV^T$, where V is the orthogonal matrix of eigenvectors, and D is the diagonal matrix of corresponding eigenvalues. Then (using $VV^T = I$)

$$\begin{aligned}
\|A\widetilde{v_i} - \widetilde{\lambda}_i\widetilde{v_i}\|_2 &= \|VDV^T\widetilde{v_i} - \widetilde{\lambda}_i\widetilde{v_i}\|_2 \\
&= \|V(D - \widetilde{\lambda}_i)V^T\widetilde{v_i}\|_2 \\
&= \|(D - \widetilde{\lambda}_i)V^T\widetilde{v_i}\|_2 \\
&\geq \min_j(|\lambda_j - \widetilde{\lambda}_i|)\|V^T\widetilde{v_i}\|_2 \\
&= \min_j(|\lambda_j - \widetilde{\lambda}_i|)\|\widetilde{v_i}\|_2 \\
&\geq \min_j(|\lambda_j - \widetilde{\lambda}_i|)\sqrt{1 - \frac{\sqrt{n}}{T} - \frac{n}{4T^2}} \\
&= \min_j(|\lambda_j - \widetilde{\lambda}_i|)\sqrt{1 - \frac{1}{2} - \frac{1}{16}} \quad \text{if } \sqrt{n} \leq \frac{T}{2} \\
&\geq \frac{\min_j(|\lambda_j - \widetilde{\lambda}_i|)}{2}
\end{aligned}$$

So if we consider $\epsilon > 0$, and wish to ensure that $\min_j(|\lambda_j - \widetilde{\lambda}_i|) < \epsilon$, i.e. there is a (true) eigenvalue close to the approximate eigenvalue, then we can choose a T based on

$$\begin{aligned}
\min_j(|\lambda_j - \widetilde{\lambda}_i|) &\leq 2\|A\widetilde{v}_i - \widetilde{\lambda}_i\widetilde{v}_i\|_2 \\
&\leq 2\sqrt{n}\|A\widetilde{v}_i - \widetilde{\lambda}_i\widetilde{v}_i\|_\infty \\
&\leq \frac{2\sqrt{n}\|TA\widehat{v}_i - \widehat{\lambda}_i\widehat{v}_i\|_\infty}{T^2} \\
&\leq \frac{2n\sqrt{n}\|A\|_F}{T} + \frac{n}{T} + \frac{n\sqrt{n}}{2T^2} \qquad \text{(using Theorem 3)}
\end{aligned}$$

As T tends to infinity, this bound positively approaches 0, as such, for any $\epsilon > 0$ we can find a T s.t. the error in $\mathbb{R}$ of $\min_j(|\lambda_j - \widetilde{\lambda}_i|)$ will be ϵ.

1.3 Details of Theorem 8

The Cholesky Decomposition allows us to solve the symmetric generalised eigenvalue problem for $A, B \in \mathbb{F}_q^{n\times n}$, with A symmetric, and B symmetric positive semi-definite;

$$\text{Find } V, D \in \mathbb{R}^{n\times n} \text{ such that } AV = BVD$$

We do this by finding the Cholesky Decomposition of B, L and then performing finding the eigenvalues of the symmetric matrix $C = L^{-1}A(L^{-1})^T$ to get matrices V', D' with $CV' = V'D'$. $D = D'$, and $V = L^{-1}V'$ are the solutions we desire.
With our approximations, we use our matrix inversion and Cholesky Decomposition protocols to find, using scaling factor T_1, we have that $\hat{C}$ will be in $\mathbb{F}_{qT_1}^{n\times n}$.

$$\hat{C} = \widehat{(\hat{L})^{-1}} A \widehat{(\hat{L})^{-1}}^T$$

So we have

$$\begin{aligned}
\hat{L}\hat{L}^T &= T_1^2 B + E_1 \qquad E_1 \in \left[-\frac{n\|B\|_F}{2T_1}, \frac{n\|B\|_F}{2}\right]^{n\times n} \\
\hat{L}\widehat{(\hat{L})^{-1}} &= T_1 I + E_2 \qquad E_2 \in \left[-n\|\hat{B}\|_F - \frac{n^2}{4}, n\|\hat{B}\|_F + \frac{n^2}{4}\right]^{n\times n}
\end{aligned}$$

If we receive approximate eigenpairs, $\hat{U}, \hat{D}$ with diagonal $\hat{\lambda}$, of $\hat{C}$ from the helper, with scaling factor T giving error ϵ^δ, satisfying

$$\begin{aligned}
\|T\hat{C}\widehat{U} - \widehat{D}\widehat{U}\|_{\max} &\leq \left\lceil Tn\|C\|_F + \frac{T\sqrt{n}}{2} + \frac{n}{4}\right\rceil \\
\|\widehat{U}^T\widehat{U} - T^2 I\|_{\max} &\leq \left\lceil T\sqrt{n} + \frac{n}{4}\right\rceil
\end{aligned}$$

Let $D^\delta, U^\delta \in \mathbb{R}^{n\times n}$ be the true eigenvalues and eigenvectors of $\hat{C}$. So

$$\hat{C}U^\delta = U^\delta D^\delta$$

We know that $\|TD^\delta - \hat{D}\|_{\max}$ will be at most $T\epsilon^\delta$. Furthermore let $\hat{L}^T V^\delta = U^\delta$, so

$$\begin{aligned}
\hat{C}U^\delta &= U^\delta D^\delta \\
\widehat{(\hat{L})^{-1}} A \widehat{(\hat{L})^{-1}}^T \hat{L}^T V^\delta &= \hat{L}^T V^\delta D^\delta \\
\hat{L}\widehat{(\hat{L})^{-1}} A \widehat{(\hat{L})^{-1}}^T \hat{L}^T V^\delta &= \hat{L}\hat{L}^T V^\delta D^\delta \\
(T_1 I + E_2) A (T_1 I + E_2)^T V^\delta &= (T_1^2 B + E_1) V^\delta D^\delta \\
\left(A + \frac{E_2 A + A E_2^T + E_2 E_2^T}{T_1^2}\right)^T V^\delta &= \left(B + \frac{E_2}{T_1^2}\right) V^\delta D^\delta
\end{aligned}$$

By using the eigenvalue perturbation theory [Trefethen and Bau III (1997)], we can say that there exists $V \in \mathbb{R}^{n\times n}$, $D \in \mathbb{R}^{n\times n}$ with diagonal λ, so

$$\lambda_i = \lambda_i^\delta + {v_i^\delta}^T \left(\frac{E_2 A + A E_2^T + E_2 E_2^T}{T_1^2} - \lambda_i^\delta \frac{E_1}{T_1^2}\right) v_i^\delta$$

So

$$\begin{aligned}
|\lambda_i - \lambda_i^\delta| &= |{v_i^\delta}^T \left(\frac{E_2 A + A E_2^T + E_2 E_2^T}{T_1^2} - \lambda_i^\delta \frac{E_1}{T_1^2}\right) v_i^\delta| \\
&\le \left\|{v_i^\delta}^T\right\|_2 \left\|\left(\frac{E_2 A + A E_2^T + E_2 E_2^T}{T_1^2} - \lambda_i^\delta \frac{E_1}{T_1^2}\right)\right\|_2 \|v_i^\delta\|_2 \\
&\le \left\|\frac{E_2 A + A E_2^T + E_2 E_2^T - \lambda_i^\delta E_1}{T_1^2}\right\|_2 \\
&\le \frac{\|E_2 A\|_2 + \left\|A E_2^T\right\|_2 + \left\|E_2 E_2^T\right\|_2 + \left\|\lambda_i^\delta E_1\right\|_2}{T_1^2} \\
&\le \frac{2\|E_2\|_2 \|A\|_2 + \|E_2\|_2^2 + \|\hat{C}\|_2 \|E_1\|_2}{T_1^2} \\
&\le \frac{2n\left(n\|B\|_2 + \frac{n^2}{4}\right)\|A\|_2 + n^2\left(n\|B\|_2 + \frac{n^2}{4}\right)^2 + \|\hat{C}\|_2 n\left(\frac{n\|B\|_2}{2}\right)}{T_1^2} \\
&\le \frac{\left(2n^2\|B\|_2 + \frac{n^3}{2}\right)\|A\|_2 + \left(n^4\|B\|_F^2 + \frac{\|B\|_2 n^5}{2} + \frac{n^6}{16}\right) + \left(\frac{\|\hat{C}\|_2 n^2 \|B\|_2}{2}\right)}{T_1^2} \\
&\le \frac{\left(2n^2\|\hat{B}\|_2 + \frac{n^3}{2}\right)\|A\|_2 + \left(n^4\|\hat{B}\|_2^2 + \frac{\|B\|_2 n^5}{2} + \frac{n^6}{16}\right) + \left(\frac{\|\hat{C}\|_2 n^2 \|B\|_2}{2}\right)}{T_1^2} \\
&\le \frac{32n^2\|B\|_2\|A\|_2 + 8n^3\|A\|_2 + 16n^4\|B\|_2^2 + 8\|B\|_F n^5 + n^6 + 8\|\hat{C}\|_2 n^2 \|B\|_2}{T_1^2}
\end{aligned}$$

As, $A, B \in \mathbb{F}_q$, we have $\|A\|_2, \|B\|_2 \leq qn$, $\|\hat{C}\|_2 \leq qnT_1$

$$\begin{aligned}|\lambda_i - \lambda_i^\delta| &\leq \frac{32n^2(nq)^2 + 8n^3nq + 16n^4(nq)^2 + 8nqn^5 + n^6 + 8qnT_1n^2nq}{T_1^2} \\ &\leq \frac{32n^4q^2 + 8n^4q + 16n^6q^2 + 8n^6q + n^6 + 8qnT_1n^3q}{T_1^2} \\ &\leq \frac{8n^4(4q^2+q) + n^6(16q^2+8q+1) + 8qnT_1n^3q}{T_1^2} \\ &\leq \frac{q^3n^4}{T_1}\end{aligned}$$

If we have that $q \geq 20$, $n \geq 3$ and $T_1 \geq n^2$. We also have

$$|T\lambda_i^\delta - \hat{\lambda}_i| \leq T\epsilon^\delta$$

So

$$\begin{aligned}|T\lambda_i - \hat{\lambda}_i| &\leq |T\lambda_i - T\lambda_i^\delta| + |T\lambda_i^\delta - \hat{\lambda}_i| \\ &\leq T\left(\frac{q^3n^4}{T_1} + \epsilon^\delta\right)\end{aligned}$$

If we want $\frac{|T\lambda_i - \hat{\lambda}_i|}{T}$ to be equal to ϵ we must choose T_1 such that

$$\frac{|T\lambda_i - \hat{\lambda}_i|}{T} \leq \frac{q^3n^4}{T_1} + \epsilon^\delta$$

Therefore, to get the generalised eigenvalues to an error of ϵ we must choose T, T_1 such that

$$\begin{aligned}T &= \frac{q^2n^{\frac{5}{2}}}{\epsilon^\delta} \geq \frac{qn^{\frac{3}{2}}\|\hat{C}\|}{\epsilon^\delta} \\ T_1 &= \frac{q^3n^4}{\epsilon - \epsilon^\delta}\end{aligned}$$

Where $\epsilon^\delta < \epsilon$.
If we take $\epsilon^\delta = \frac{\epsilon}{2}$, then we have

$$\begin{aligned}T &= \frac{2q^2n^{\frac{5}{2}}}{\epsilon} \\ T_1 &= \frac{2q^3n^4}{\epsilon}\end{aligned}$$

And our total protocol is therefore, assuming $q > n$, $\left(n^2\log\left(q^3n^4/\epsilon\right), \log\left(q^3n^4/\epsilon\right)\right)$.

1.4 Fingerprinting the Covariance Matrix

This algorithm provides a $\left(d^2\log(qn), \log(qn)\right)$ −protocol for verification that A is indeed the covariance matrix scaled by n. The costs come from scaling by n and receiving $A \in \mathbb{F}_{qn}^{d\times d}$.

References

Lloyd N Trefethen and David Bau III. *Numerical linear algebra*, volume 50. Siam, 1997.

Algorithm 1: Streaming Annotated CovarianceFingerprint

Input : $S \in \mathbb{F}_q^{d\times n}$

Output: $f_x(A) = f_x\left((n-1)Cov(S)\right)$ or $\perp$

Choose $x \in_R \mathbb{F}$

Whilst Streaming S column by column;

for $S_j^{\downarrow}$ *with* $j = 0$ **to** $n-1$ **do**

  Construct the sum of each of these $f^v_{x^n}(S_j^{\downarrow})$, $f^v_x(S_j^{\downarrow})$, $f^v_{x^n}(S_j^{\downarrow})f^v_x(S_j^{\downarrow})$, $\sum_{i=0}^{d-1} S_{ij}x^n$ and $\sum_{i=0}^{d-1} S_{ij}x^{ni}$ individually

$f_x(A) = \sum_j f^v_{x^n}(S_j^{\downarrow})f^v_x(S_j^{\downarrow}) - \left[\sum_j \sum_{i=0}^{d-1} S_{ij}x^n\right]\left[\sum_j f^v_{x^n}(S_j^{\downarrow})\right] - \left[\sum_j \sum_{i=0}^{d-1} S_{ij}x^{ni}\right]\left[\sum_j f^v_x(S_j^{\downarrow})\right] + n\left[\sum_j \sum_{i=0}^{d-1} S_{ij}x^n\right]\left[\sum_j \sum_{i=0}^{d-1} S_{ij}x^{ni}\right]$

Receive $\widehat{A}$ from the helper

Check

  $f_x(A) == f_x(\widehat{A})$