Crypto project

Name: Yihang Yan, Tomas Gudmundsson, Nathaniel Stein

1

Jacobi method

In order to find eigenvalues and eigenvectors of the covariance matrix, A, we use the Jacobi method. The method finds the largest element below the diagonal in the matrix at location (l, k) and simulates a rotation with A as follows:

$$A' = P^T \cdot A \cdot P \tag{1}$$

where P,A,A' have the form:

$$P = \begin{bmatrix} c_{ll} & s_{kl} \\ -s_{lk} & c_{kk} \end{bmatrix}, A = \begin{bmatrix} A_{ll} & A_{kl} \\ A_{lk} & A_{kk} \end{bmatrix}, A' = \begin{bmatrix} A'_{ll} & A'_{kl} \\ A'_{lk} & A'_{kk} \end{bmatrix} \tag{2}$$

and P represents a plane rotation of angle θ and has the diagonal values except c_{ll} and c_{kk} as 1 and other values as 0. The values c and s are the cosine and sine of the rotation angle. We will use the notation P_{pq} to denote a rotation that affects rows and columns p and q of A.

Note that the matrix multiplication $\left(P^T \cdot A\right)$ changes only rows p and q whereas the $(A \cdot P)$ changes columns p and q. This is because it makes a difference whether a matrix is multiplied before or after A.

In order for P to satisfy eq. 1 we expand the matrix multiplication as follows with $c_{ll} = c_{kk} = c$ and $s_{lk} = s_{kl} = s$:

$$\begin{aligned}
\begin{bmatrix} A'_{ll} & A'_{kl} \\ A'_{lk} & A'_{kk} \end{bmatrix} &= \begin{bmatrix} c & s \\ -s & c \end{bmatrix} \cdot \begin{bmatrix} A_{ll} & A_{kl} \\ A_{lk} & A_{kk} \end{bmatrix} \cdot \begin{bmatrix} c & -s \\ s & c \end{bmatrix} \\
&= \begin{bmatrix} c \cdot A_{ll} + s \cdot A_{lk} & c \cdot A_{kl} + s \cdot A_{kk} \\ -s \cdot A_{ll} + c \cdot A_{lk} & -s \cdot A_{kl} + c \cdot A_{kk} \end{bmatrix} \cdot \begin{bmatrix} c & -s \\ s & c \end{bmatrix} \\
&= \begin{bmatrix} c^2 \cdot A_{ll} + cs \cdot A_{lk} + cs \cdot A_{kl} + s^2 \cdot A_{kk} & -cs \cdot A_{ll} - s^2 \cdot A_{lk} + c^2 \cdot A_{kl} + cs \cdot A_{kk} \\ -cs \cdot A_{ll} + c^2 \cdot A_{lk} - s^2 \cdot A_{kl} + cs \cdot A_{kk} & s^2 \cdot A_{ll} - cs \cdot A_{lk} - cs \cdot A_{kl} + c^2 \cdot A_{kk} \end{bmatrix} \\
&= \begin{bmatrix} c^2 \cdot A_{ll} + 2cs \cdot A_{lk} + s^2 \cdot A_{kk} & (c^2 - s^2) \cdot A_{kl} + cs \cdot (A_{kk} - A_{ll}) \\ (c^2 - s^2) \cdot A_{lk} + cs \cdot (A_{kk} - A_{ll}) & c^2 \cdot A_{kk} - 2cs \cdot A_{lk} + s^2 \cdot A_{ll} \end{bmatrix}
\end{aligned} \tag{3}$$

In order to make the non diagonal element in this matrix as 0 we will examine the non diagonal equation as follows:

$$A'_{lk} = (c^2 - s^2) \cdot A_{lk} + cs(A_{kk} - A_{ll}) = 0 \tag{4}$$

Hence it follows that:

$$\frac{c^2 - s^2}{cs} = \frac{A_{ll} - A_{kk}}{A_{lk}} \tag{5}$$

and we can define a rotation angle as follows:

$$\theta = cot(2\phi) = \frac{c^2 - s^2}{2cs} = \frac{A_{ll} - A_{kk}}{2A_{lk}} \tag{6}$$

and by letting $t = s/c$ we can rewrite the equation above as:

$$2cs\theta = c^2 - s^2 <=> t^2 + 2t\theta - 1 = 0 \tag{7}$$

which has the solutions:

$$t = \begin{cases} -\theta + \sqrt{\theta^2 + 1} \\ -(\theta + \sqrt{\theta^2 + 1}) \end{cases} \tag{8}$$

The first solution can be written more succinctly as

$$t = -\theta + \sqrt{\theta^2 + 1} = \frac{\left(-\theta + \sqrt{\theta^2 + 1}\right)\left(-\theta + \sqrt{\theta^2 + 1}\right)}{\theta + \sqrt{\theta^2 + 1}} = \frac{-\theta^2 + \theta^2 + 1}{\theta + \sqrt{\theta^2 + 1}} = \frac{1}{\theta + \sqrt{\theta^2 + 1}} \tag{9}$$

and same for the second solution if $\theta < 0$. Generally we can write:

$$t = \frac{sign(\theta)}{|\theta| + \sqrt{1 + \theta^2}} \tag{10}$$

and since $t = s/c$ we now have:

$$c = \frac{1}{\sqrt{t^2 + 1}}, \quad s = t \cdot c \tag{11}$$

Now when we know how to set these variables for the rotations to work we need to look at three scenarios to update the matrix when a rotation is performed:

i) Set value at location (l,k) as 0

ii) Change diagonal values at locations (l,l) and (k,k)

iii) Change values on rows l and k and columns l and k except (l,l) and (k,k)

For scenario i) we simply set the value of A'_{lk} as 0. However, for scenario ii) we will look at the top left and bottom right elements in eq. 3 to gather equations to set the diagonal elements A'_{kk} and A'_{ll} . We have:

$$A'_{kk} = c^2 \cdot A_{kk} - 2cs \cdot A_{lk} + s^2 \cdot A_{ll} \tag{12}$$

From eq. 4 (because $A'_{lk} = 0$) we can isolate A_{ll} as

$$A_{ll} = A_{kk} - A_{lk}\frac{s^2 - c^2}{cs} \tag{13}$$

and since $c^2 + s^2 = 1$ we simplify eq 12. as:

$$\begin{aligned}
A'_{kk} &= c^2 \cdot A_{kk} - 2cs \cdot A_{lk} + s^2 \cdot A_{ll} \\
&= c^2 \cdot A_{kk} - 2cs \cdot A_{lk} + s^2 \left(A_{kk} - A_{lk}\frac{s^2 - c^2}{cs} \right) \\
&= (c^2 + s^2) \cdot A_{kk} - s \left(2c + \frac{s^2 - c^2}{c} \right) A_{lk} \\
&= (c^2 + s^2) \cdot A_{kk} - \frac{s}{c} \left(2c^2 + s^2 - c^2 \right) A_{lk} \\
&= A_{kk} - \frac{s}{c} \left(c^2 + s^2 \right) A_{lk} \\
&= A_{kk} - t \cdot A_{lk}
\end{aligned} \tag{14}$$

Similarly we have:

$$A'_{ll} = A_{ll} + t \cdot A_{lk} \tag{15}$$

For scenario iii) we can look at top of eq 3. and note that if we consider an element A_{rk} when we perform rotation around A_{lk} that only the last two matrices will change the result since the first matrix changes rows l and k and does not have effect on row r. The last matrix changes columns l and k and therefore changes the resulting matrix. Multiplying through these matrices gives us the equations:

$$\begin{cases} A'_{rk} = cA_{rk} - sA_{rl} \\ A'_{rl} = cA_{rl} + sA_{rp} \end{cases} \tag{16}$$

Lets look at A'_{rk} which can be represented as:

$$
\begin{aligned}
A'_{rk} &= cA_{rk} - sA_{rl} \\
&= \left(1 - \frac{(1-c)(1+c)}{1+c}\right) A_{rk} - sA_{rl} \\
&= \left(1 - \frac{1-c^2}{1+c}\right) A_{rk} - sA_{rl} \\
&= \left(1 - \frac{s^2}{1+c}\right) A_{rk} - sA_{rl} \\
&= A_{rk} - s\left(A_{rl} + \frac{s}{1+c} A_{rk}\right) \\
&= A_{rk} - s\left(A_{rl} + \tau A_{rk}\right)
\end{aligned} \tag{17}
$$

where

$$\tau = \frac{s}{1+c} \tag{18}$$

Similarly we have

$$A'_{rl} = A_{rl} + s\left(A_{rk} + \tau A_{rl}\right) \tag{19}$$

To summarise we set values of elements in rows r and l and columns r and l as follows:

i) $A_{lk} = 0$

ii) $\begin{cases} A'_{kk} = A_{kk} - t \cdot A_{lk} \\ A'_{ll} = A_{ll} + t \cdot A_{lk} \end{cases}$

iii) $\begin{cases} A'_{rk} = A_{rk} - s\left(A_{rl} + \tau A_{rk}\right), & r \neq k, r \neq l \\ A'_{rl} = A_{rl} + s\left(A_{rk} + \tau A_{rl}\right), & r \neq k, r \neq l \end{cases}$

where

$$s = t \cdot c, \quad t = \frac{sign(\theta)}{|\theta| + \sqrt{1+\theta^2}}, \quad \tau = \frac{s}{1+c}, \quad \theta = \frac{A_{ll} - A_{kk}}{2A_{kl}}$$