Covariance Sensitivity Proofs

March 9, 2020

Lemma 1. *The covariance matrix of X may be written as*

$$\frac{1}{n-1}\sum_{i=1}^{n}(X_i-\mu)(X_i-\mu)^T.$$

Proof.

$$\frac{1}{n-1}\sum_{i=1}^{n}(X_i-\mu)(X_i-\mu)^T = \frac{1}{n-1}\sum_{i=1}^{n}\begin{bmatrix} x_{1i}-\mu_1 \\ x_{2i}-\mu_2 \\ \vdots \\ x_{mi}-\mu_m \end{bmatrix}\begin{bmatrix} x_{1i}-\mu_1 & x_{2i}-\mu_2 & \cdots & x_{mi}-\mu_m \end{bmatrix}$$

$$= \frac{1}{n-1}\sum_{i=1}^{n}\begin{bmatrix} (x_{1i}-\mu_1)(x_{1i}-\mu_1) & (x_{1i}-\mu_1)(x_{2i}-\mu_2) & \cdots & (x_{1i}-\mu_1)(x_{mi}-\mu_m) \\ (x_{2i}-\mu_1)(x_{1i}-\mu_1) & (x_{2i}-\mu_1)(x_{2i}-\mu_2) & \cdots & (x_{2i}-\mu_1)(x_{mi}-\mu_m) \\ \vdots & \vdots & \ddots & \vdots \\ (x_{mi}-\mu_1)(x_{1i}-\mu_1) & (x_{mi}-\mu_1)(x_{2i}-\mu_2) & \cdots & (x_{mi}-\mu_1)(x_{mi}-\mu_m) \end{bmatrix}$$

$$= \begin{bmatrix} \frac{1}{n-1}\sum_{i=1}^{n}(x_{1i}-\mu_1)(x_{1i}-\mu_1) & \frac{1}{n-1}\sum_{i=1}^{n}(x_{1i}-\mu_1)(x_{2i}-\mu_2) & \cdots & \frac{1}{n-1}\sum_{i=1}^{n}(x_{1i}-\mu_1)(x_{mi}-\mu_m) \\ \frac{1}{n-1}\sum_{i=1}^{n}(x_{2i}-\mu_1)(x_{1i}-\mu_1) & \frac{1}{n-1}\sum_{i=1}^{n}(x_{2i}-\mu_1)(x_{2i}-\mu_2) & \cdots & \frac{1}{n-1}\sum_{i=1}^{n}(x_{2i}-\mu_1)(x_{mi}-\mu_m) \\ \vdots & \vdots & \ddots & \vdots \\ \frac{1}{n-1}\sum_{i=1}^{n}(x_{mi}-\mu_1)(x_{1i}-\mu_1) & \frac{1}{n-1}\sum_{i=1}^{n}(x_{mi}-\mu_1)(x_{2i}-\mu_2) & \cdots & \frac{1}{n-1}\sum_{i=1}^{n}(x_{mi}-\mu_1)(x_{mi}-\mu_m) \end{bmatrix}$$

which is the covariance matrix of X. □

Lemma 2.

$$\sum_{i=1}^{n}(X_i-\mu)=0.$$

Proof.

$$
\begin{aligned}
\sum (X_i - \mu) &= \sum_{i=1}^{n} \left(\begin{bmatrix} x_{1i} \\ x_{2i} \\ \vdots \\ x_{mi} \end{bmatrix} - \begin{bmatrix} \mu_1 \\ \mu_2 \\ \vdots \\ \mu_m \end{bmatrix} \right) \\
&= \sum_{i=1}^{n} \begin{bmatrix} x_{1i} - \mu_1 \\ x_{2i} - \mu_2 \\ \vdots \\ x_{mi} - \mu_m \end{bmatrix} \\
&= \begin{bmatrix} \sum_{i=1}^{n} (x_{1i} - \mu_1) \\ \sum_{i=1}^{n} (x_{2i} - \mu_2) \\ \vdots \\ \sum_{i=1}^{n} (x_{mi} - \mu_m) \end{bmatrix} \\
&= \begin{bmatrix} n\mu_1 - n\mu_1 \\ n\mu_2 - n\mu_2 \\ \vdots \\ n\mu_m - n\mu_m \end{bmatrix} \\
&= 0
\end{aligned}
$$

□

Corollary 1.

$$\sum_{i=1}^{n} (X_i - \mu)^T = 0.$$

by identical proof construction.

1 Neighboring Definition: Change One

1.1 ℓ_1-sensitivity

Theorem 1. *Let $F(X)$ be the covariance matrix of X without the normalization factor of $n-1$. Let M_i be a maximum bound on $x_i \in X_i$, and let m_i be a minimum bound on $x_i \in X_i$. Then each entry f_{ij} of this matrix has sensitivity bounded above by*

$$\frac{2(n-1)}{n}(M_i - m_i)(M_j - m_j)$$

Proof. Let X' be defined as

$$X' = \begin{bmatrix} X'_1 & \cdots & X'_m \end{bmatrix}^T$$

where

$$X'_i = X_i \cup \{y_i\}.$$

I.e., each row i has a single additional observation y_i in X' that it does not have in X. Let X'' be defined in the same way as X', except with a different point $\{y'_i\}$ added to each row of X. This proof, which is essentially an extension of the proof of variance sensitivity, will use the definition of "neighboring databases" in which databases are neighboring if they have a single point changed. I.e., X' and X'' are neighboring databases.

It is first useful to determine how $f(X')$ compares to $f(X)$. Let Y be the vector of all the $\{y_i\}$ observations in X'. Then,

$$F(X') = \sum (X_i - \mu')(X_i - \mu')^T + (Y - \mu')(Y - \mu')^T.$$

The first of the sums inside this expression may be expanded to give

$$\begin{aligned}
\sum (x_i - \mu')(x_i - \mu')^T &= \sum ((x_i - \mu) + (\mu - \mu'))((x_i - \mu) + (\mu - \mu'))^T \\
&= \sum (x_i - \mu)(x_i - \mu)^T + (\mu - \mu') \sum (x_i - \mu)^T + \sum (x_i - \mu)(\mu - \mu')^T \\
&\quad + \sum (\mu - \mu')(\mu - \mu')^T \\
&= \sum (x_i - \mu)(x_i - \mu)^T + (\mu - \mu') \sum (x_i - \mu)^T + \sum (x_i - \mu)(\mu - \mu')^T \\
&\quad + n(\mu - \mu')(\mu - \mu')^T \\
&= \sum (x_i - \mu)(x_i - \mu)^T + n(\mu - \mu')(\mu - \mu')^T \\
&= F(X) + n(\mu - \mu')(\mu - \mu')^T,
\end{aligned}$$

where the second-to-last line is due to cancellations of the middle two terms by Lemma 2 and Corollary 1. So,

$$F(X') = F(X) + n(\mu - \mu')(\mu - \mu')^T + (Y - \mu')(Y - \mu')^T. \tag{1.1}$$

Looking at the two expressions inside the parentheses of Eq. 1.1, note first that

$$n(\mu - \mu')(\mu - \mu')^T$$

is an $m \times m$ matrix with ijth entry

$$\begin{aligned}
x_{ij} &= n(\mu_i - \mu'_i)(\mu_j - \mu'_j) \\
&\leq n \left(\frac{M_i - m_i}{n+1} \right) \left(\frac{M_j - m_j}{n+1} \right) \\
&= \frac{n}{(n+1)^2} (M_i - m_i)(M_j - m_j).
\end{aligned} \tag{1.2}$$

The second term,

$$(Y - \mu')(Y - \mu')^T,$$

is also an $m \times m$ matrix, with ijth entry

$$\begin{aligned}
x_{ij} &= (y_i - \mu'_i)(y_j - \mu'_j) \\
&= \left(y_i - \frac{n\mu_i + y_i}{n+1} \right) \left(y_j - \frac{n\mu_j + y_j}{n+1} \right) \\
&= \frac{n^2}{(n+1)^2} (y_i - \mu_i)(y_j - \mu_j) \\
&\leq \frac{n^2}{(n+1)^2} (M_i - m_i)(M_j - m_j).
\end{aligned} \tag{1.3}$$

Let f_{ij} be the ijth entry of the $m \times m$ matrix output by F. Then plugging the bounds in Eq. 1.2 and Eq. 1.3 back into Eq. 1.1 gives

$$
\begin{aligned}
f_{ij}(X') &\leq f_{ij}(X) + \frac{n}{(n+1)^2}(M_i - m_i)(M_j - m_j) + \frac{n^2}{(n+1)^2}(M_i - m_i)(M_j - m_j) \\
&= f_{ij}(X) + \frac{n}{(n+1)^2}(M_i - m_i)(M_j - m_j)(n+1) \\
&= f_{ij}(X) + \frac{n}{n+1}(M_i - m_i)(M_j - m_j). \qquad (1.4)
\end{aligned}
$$

Since we'd really like to consider the sensitivity of $f(X')$, it makes sense to redefine n based on the size of X' rather than of X, i.e. redefine n to be $n+1$. Then,

$$
f_{ij}(X') = f_{ij}(X) + \frac{n-1}{n}(M_i - m_i)(M_j - m_j). \qquad (1.5)
$$

Now, consider two neighboring databases X' and X''. Say X' may still be written as $X \cup \{y\}$, and X'' may be similarly written as $X \cup \{z\}$. It then follows from Eq. 1.5, using the triangle inequality, that

$$
\left| f_{ij}(X') - f_{ij}(X'') \right| \leq \frac{2(n-1)}{n}(M_i - m_i)(M_j - m_j).
$$

$\square$

Corollary 2. *The sample covariance has sensitivity*

$$
\frac{2}{n}(M_i - m_i)(M_j - m_j).
$$

Proof. This follows directly from the above theorem, re-inserting the normalization factor of $n-1$. $\square$

1.2 ℓ_2-sensitivity

2 Neighboring Definition: Add/Drop One

2.1 ℓ_1-sensitivity

2.2 ℓ_2-sensitivity