COMP0086 Summative Assignment

Nov 14, 2022

Question 1

- (a) Our sample space for images is $\{0,1\}^D$, where each of our D dimensions can only take binary values (D being the number of pixels in the image). The exponential family best suited on this sample space is the D-dimensional multivariate Bernoulli distribution because it shares the same sample space. On the other hand, a D-dimensional multivariate Gaussian has the sample space \mathbb{R}^D , which does not match the sample space of our data. It is not immediately clear how the likelihood of an image of binary (discrete) values would be calculated under the continuous distribution of a multivariate Gaussian. Thus it would be inappropriate to model this dataset of images with a multivariate Gaussian.
- (b) For $\{\mathbf{x}^{(n)}\}_{n=1}^N$, a data set of N images, the joint likelihood (assuming images are independently and identically distributed) is the product of N, D-dimensional multivariate Bernoulli distributions:

$$P(\{\mathbf{x}^{(n)}\}_{n=1}^{N}|\mathbf{p}) = \prod_{n=1}^{N} P(\mathbf{x}^{(n)}|\mathbf{p})$$

Substituting the D-dimensional multivariate Bernoulli:

$$P(\{\mathbf{x}^{(n)}\}_{n=1}^{N}|\mathbf{p}) = \prod_{n=1}^{N} \prod_{d=1}^{D} p_d^{x_d^{(n)}} (1 - p_d)^{1 - x_d^{(n)}}$$

Taking the logarithm, we get the log likelihood:

$$\mathcal{L}(\{\mathbf{x}^{(n)}\}_{n=1}^{N}|\mathbf{p}) = \sum_{n=1}^{N} \sum_{d=1}^{D} [x_d^{(n)} \log(p_d) + (1 - x_d^{(n)}) \log(1 - p_d)]$$

Note that since the logarithm is a monotonically increasing function on \mathbb{R}_+ , the maximisers and minimisers of the likelihood do not change. Thus, to solve for the maximum likelihood estimate, \hat{p}_d , we can take the derivative of $\mathcal{L}(\{\mathbf{x}^{(n)}\}_{n=1}^N|\mathbf{p})$ with respect to p_d , the d^{th} element of \mathbf{p} :

$$\frac{\partial \mathcal{L}(\{\mathbf{x}^{(n)}\}_{n=1}^{N}|\mathbf{p})}{\partial p_{d}} = \sum_{n=1}^{N} \left(\frac{x_{d}^{(n)}}{p_{d}} - \frac{1 - x_{d}^{(n)}}{1 - p_{d}}\right)$$
$$\frac{\partial \mathcal{L}(\{\mathbf{x}^{(n)}\}_{n=1}^{N}|\mathbf{p})}{\partial p_{d}} = \frac{\sum_{n=1}^{N} x_{d}^{(n)}}{p_{d}} - \frac{\sum_{n=1}^{N} (1 - x_{d}^{(n)})}{1 - p_{d}}$$

and set the derivative to zero to solve for \hat{p}_d :

$$\frac{\sum_{n=1}^{N} x_d^{(n)}}{\hat{p}_d} - \frac{\sum_{n=1}^{N} (1 - x_d^{(n)})}{1 - \hat{p}_d} = 0$$

$$\sum_{n=1}^{N} x_d^{(n)} - \hat{p}_d \sum_{n=1}^{N} x_d^{(n)} - \hat{p}_d \cdot N + \hat{p}_d \sum_{n=1}^{N} x_d^{(n)} = 0$$

$$\hat{p}_d = \frac{1}{N} \sum_{n=1}^{N} x_d^{(n)}$$

Because we assume that each pixel is independent (we are taking the product of D one dimensional Bernoulli distributions), we can express the maximum likelihood for \mathbf{p} in vectorised form as $\hat{\mathbf{p}}^{MLE}$:

$$\hat{\mathbf{p}}^{MLE} = \frac{1}{N} \sum_{n=1}^{N} \mathbf{x}^{(n)}$$

(c) From Bayes' Theorem:

$$P(\mathbf{p}|\{\mathbf{x}^{(n)}\}_{n=1}^{N}) = \frac{P(\{\mathbf{x}^{(n)}\}_{n=1}^{N}|\mathbf{p})P(\mathbf{p})}{P(\{\mathbf{x}^{(n)}\}_{n=1}^{N})}$$

Taking the logarithm:

$$\mathcal{L}(\mathbf{p}|\{\mathbf{x}^{(n)}\}_{n=1}^{N}) = \mathcal{L}(\{\mathbf{x}^{(n)}\}_{n=1}^{N}|\mathbf{p}) + \mathcal{L}(\mathbf{p}) - \mathcal{L}(\{\mathbf{x}^{(n)}\}_{n=1}^{N})$$

Taking the derivative with respect to p_d :

$$\frac{\partial \mathcal{L}(\mathbf{p}|\{\mathbf{x}^{(n)}\}_{n=1}^{N})}{\partial p_{d}} = \frac{\partial \mathcal{L}(\{\mathbf{x}^{(n)}\}_{n=1}^{N}|\mathbf{p})}{\partial p_{d}} + \frac{\partial \mathcal{L}(\mathbf{p})}{\partial p_{d}}$$

where $\frac{\partial \mathcal{L}(\{\mathbf{X}^{(n)}\}_{n=1}^{N})}{\partial p_d} = 0$ because it doesn't depend on p_d .

We know from (b):

$$\frac{\partial \mathcal{L}(\{\mathbf{x}^{(n)}\}_{n=1}^{N}|\mathbf{p})}{\partial p_d} = \frac{\sum_{n=1}^{N} x_d^{(n)}}{p_d} - \frac{\sum_{n=1}^{N} (1 - x_d^{(n)})}{1 - p_d}$$

For the second term $\frac{\partial \mathcal{L}(\mathbf{p})}{\partial p_d}$, we start with $P(\mathbf{p})$, assuming each pixel to have an independent prior:

$$P(\mathbf{p}) = \prod_{d=1}^{D} P(p_d)$$

and assuming a Beta prior on each p_d :

$$P(\mathbf{p}) = \prod_{d=1}^{D} \frac{1}{B(\alpha, \beta)} p_d^{\alpha - 1} (1 - p_d)^{\beta - 1}$$

Taking the logarithm:

$$\mathcal{L}(\mathbf{p}) = \sum_{d=1}^{D} -\log(B(\alpha, \beta)) + (\alpha - 1)\log p_d + (\beta - 1)\log(1 - p_d)$$

Taking the derivative with respect to p_d :

$$\frac{\partial \mathcal{L}(\mathbf{p})}{\partial p_d} = \frac{(\alpha - 1)}{p_d} - \frac{(\beta - 1)}{1 - p_d}$$

Since we are only concerned with p_d , we are only left with a single element of the summation pertaining to p_d .

Combining, we have an expression for $\frac{\partial \mathcal{L}(\mathbf{p}|\{\mathbf{X}^{(n)}\}_{n=1}^{N})}{\partial p_d}$:

$$\frac{\partial \mathcal{L}(\mathbf{p}|\{\mathbf{x}^{(n)}\}_{n=1}^{N})}{\partial p_{d}} = \frac{\sum_{n=1}^{N} x_{d}^{(n)}}{p_{d}} - \frac{\sum_{n=1}^{N} (1 - x_{d}^{(n)})}{1 - p_{d}} + \frac{(\alpha - 1)}{p_{d}} - \frac{(\beta - 1)}{1 - p_{d}}$$
$$\frac{\partial \mathcal{L}(\mathbf{p}|\{\mathbf{x}^{(n)}\}_{n=1}^{N})}{\partial n_{d}} = \frac{(\alpha - 1) + \sum_{n=1}^{N} x_{d}^{(n)}}{n_{d}} - \frac{(\beta - 1) + \sum_{n=1}^{N} (1 - x_{d}^{(n)})}{1 - n_{d}}$$

To find the maximum a posteriori (MAP) estimate $\hat{p_d}$ set $\frac{\partial \mathcal{L}(\mathbf{p}|\{\mathbf{X}^{(n)}\}_{n=1}^N)}{\partial p_d} = 0$ and solve:

$$0 = \frac{(\alpha - 1) + \sum_{n=1}^{N} x_d^{(n)}}{\hat{p_d}} - \frac{(\beta - 1) + \sum_{n=1}^{N} (1 - x_d^{(n)})}{1 - \hat{p_d}}$$

$$0 = (1 - \hat{p_d})(\alpha - 1) + (1 - \hat{p_d}) \left(\sum_{n=1}^{N} x_d^{(n)}\right) - \hat{p_d}(\beta - 1) - \hat{p_d} \left(\sum_{n=1}^{N} (1 - x_d^{(n)})\right)$$

$$0 = (\alpha - \alpha \hat{p_d} + \hat{p_d} - 1) + \left(\sum_{n=1}^{N} x_d^{(n)} - \hat{p_d} \sum_{n=1}^{N} x_d^{(n)}\right) - (\hat{p_d}\beta - \hat{p_d}) - \left(\hat{p_d} \cdot N - \hat{p_d} \sum_{n=1}^{N} x_d^{(n)}\right)$$

Cancelling the $\hat{p}_d \sum_{n=1}^N x_d^{(n)}$ terms:

$$0 = \alpha - \alpha \hat{p_d} + \hat{p_d} - 1 + \sum_{n=1}^{N} x_d^{(n)} - \hat{p_d}\beta + \hat{p_d} - \hat{p_d} \cdot N$$
$$0 = \hat{p_d}(2 - \alpha - \beta - N) + \alpha - 1 + \sum_{n=1}^{N} x_d^{(n)}$$
$$\hat{p_d} = \frac{\alpha - 1 + \sum_{n=1}^{N} x_d^{(n)}}{(N + \alpha + \beta - 2)}$$

Due to independence of our likelihood and priors for each dimension, we can express the maximum a priori for \mathbf{p} in vectorised form as $\hat{\mathbf{p}}^{MAP}$:

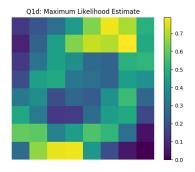
$$\hat{\mathbf{p}}^{MAP} = \frac{\alpha - 1 + \sum_{n=1}^{N} \mathbf{x}^n}{(N + \alpha + \beta - 2)}$$

(d&e) The Python code for MLE and MAP:

```
import matplotlib.pyplot as plt
import numpy as np
3
     {\tt def\_compute\_maximum\_likelihood\_estimate(x: np.ndarray)} \ -\!\!\!> \ np.ndarray:
6
           :param x: numpy array of shape (N, D) :return: MLE estimate """
10
           return np.mean(x, axis=0)
     def _compute_maximum_a_priori_estimate(
    x: np.ndarray, alpha: float, beta: float
14
     ) -> np.ndarray:
           Calculates MAP estimate of images
           :param x: numpy array of shape (N, D)
:param alpha: param of prior distribution
:param beta: param of prior distribution
:return: MAP estimate
"""
19
20
22
23
24
25
           n, = x.shape
           return (alpha - 1 + np.sum(x, axis=0)) / (n + alpha + beta - 2)
     def d(x: np.ndarray, figure_path: str, figure_title: str) -> None:
30
           Produces answers for question 1d :param x: numpy array of shape (N, D)
31
33
34
           :param figure_path: path to store figure
:param figure_title: figure title
35
36
           maximum_likelihood = _compute_maximum_likelihood_estimate(x)
38
           plt.figure()
            plt.imshow(
                 np.reshape(maximum_likelihood, (8, 8)),
41
                 interpolation="None",
42
           plt.colorbar()
           plt.axis("off")
plt.title(figure_title)
44
45
           plt.savefig(figure_path)
49
          x: np.ndarray, alpha: float, beta: float, figure_path: str, figure_title: str
50
51
     ) -> None:
           Produces answers for question 1e:param x: numpy array of shape (N, D):param alpha: param of prior distribution
55
56
           :param beta: param of prior distribution
:param figure_path: path to store figure
:param figure_title: figure title
58
59
           :return:
60
61
           maximum\_a\_priori = \_compute\_maximum\_a\_priori\_estimate(x, alpha, beta)
62
            plt.figure()
            plt.imshow(
64
                 np.reshape(maximum_a_priori, (8, 8)),
65
                 interpolation="None",
           plt.colorbar()
    resis("off")
67
           plt.axis("off")
plt.title(figure_title)
plt.savefig(f"{figure_path}.png")
69
70
71
72
73
74
75
76
77
78
79
            maximum\_likelihood = \_compute\_maximum\_likelihood\_estimate(x)
            plt.figure()
                 {\tt np.reshape(maximum\_a\_priori-maximum\_likelihood,\ (8\,,\ 8))}\,,
                 interpolation="None",
           plt.colorbar()
           plt.axis("off")
plt.title(f"MAP vs MLE")
80
            plt.savefig(f"{figure_path}-mle-vs-map.png")
```

src/solutions/q1.py

Displaying the learned parameters:



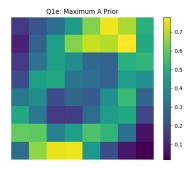


Figure 1: ML parameters

Figure 2: MAP parameters

Comparing the equations:

$$\hat{\mathbf{p}}^{MLE} = \frac{1}{N} \sum_{n=1}^{N} \mathbf{x}^{(n)}$$

and

$$\hat{\mathbf{p}}^{MAP} = \frac{\alpha - 1 + \sum_{n=1}^{N} \mathbf{x}^n}{(N + \alpha + \beta - 2)}$$

As the number of data points increases, $\hat{\mathbf{p}}^{MAP}$ approaches $\frac{1}{N}\sum_{n=1}^{N}\mathbf{x}^{(n)}$, the $\hat{\mathbf{p}}^{MLE}$. This makes sense because as our data set gets bigger, the effect of the prior diminishes. However, if a specific pixel in all of the images of our data set are white or all black, the MLE for that pixel would either be 1 or 0. This may not be representative of our intuitions about images, as there should be some non-zero probability of a pixel being black or white. By introducing an appropriate prior we can ensure that the probability of that pixel will never be exactly zero or one. In our case, with a Beta(3,3) prior on each pixel, our parameter values are biased to be closer to 0.5 and to never be at the extremities 0 and 1. We can see this in Figure 2 where the range of our parameters is smaller than the range of Figure 1 and doesn't include zero. Figure 3 visualises $\hat{\mathbf{p}}^{MAP} - \hat{\mathbf{p}}^{MLE}$ and we can see that for likelihoods greater than 0.5 in the MLE, the MAP has a lower value and for likelihoods less than 0.5, the MAP has a higher value, confirming our intuitions.

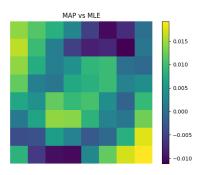


Figure 3: $\hat{\mathbf{p}}^{MAP} - \hat{\mathbf{p}}^{MLE}$

Priors can also help ensure numerical stability during calculations. The logarithm of zero is negative infinity, so having if the MLE is zero it can be problematic for log-likelihood calculations whereas MAP can ensure non-zero probabilities. Interestingly, when $\alpha = \beta = 1$, $\hat{\mathbf{p}}^{MLE} = \hat{\mathbf{p}}^{MAP}$. This is when the prior is a uniform distribution and so there is uniform bias on the location of \mathbf{p} and we recover the MLE.

On the other hand, a mis-specified prior can be problematic, as the estimated parameters might be skewed by the prior and not properly represent the underlying data generating process, this can result in parameter estimates that are 'worse' than using the MLE if our data set is limited in size.

Question 2

When all D components are generated from a Bernoulli distribution with $p_d = 0.5$, we have the likelihood function for model M_1 :

$$P(\{\mathbf{x}^{(n)}\}_{n=1}^{N}|\mathbf{p}^{(1)} = [0.5, 0.5, ..., 0.5]^{T}, M_{1}) = \prod_{n=1}^{N} \prod_{d=1}^{D} (0.5)^{x_{d}^{(n)}} (0.5)^{1-x_{d}^{(n)}}$$

Knowing that either $x_d^{(n)}$ or $1 - x_d^{(n)}$ will be 1 and the other zero, we can simplify $(0.5)^{x_d^{(n)}}(1 - 0.5)^{1-x_d^{(n)}}$ to 0.5:

$$P(\{\mathbf{x}^{(n)}\}_{n=1}^{N}|\mathbf{p}^{(1)} = [0.5, 0.5, ..., 0.5]^{T}, M_{1}) = \prod_{n=1}^{N} \prod_{d=1}^{D} (0.5)$$

$$P(\{\mathbf{x}^{(n)}\}_{n=1}^{N}|\mathbf{p}^{(1)} = [0.5, 0.5, ..., 0.5]^{T}, M_1) = 0.5^{N \cdot D}$$

When all D components are generated from Bernoulli distributions with unknown, but identical, p_d , we have the likelihood function for model M_2 :

$$P(\{\mathbf{x}^{(n)}\}_{n=1}^{N}|\mathbf{p}^{(2)} = [p_d, p_d, ..., p_d]^T, M_2) = \prod_{n=1}^{N} \prod_{d'=1}^{D} p_d^{x_{d'}^{(n)}} (1 - p_d)^{1 - x_{d'}^{(n)}}$$

When each component is Bernoulli distributed with separate, unknown p_d , we have the likelihood function for model M_3 :

$$P(\{\mathbf{x}^{(n)}\}_{n=1}^{N}|\mathbf{p}^{(3)} = [p_1, p_2, ..., p_D]^T, M_3) = \prod_{n=1}^{N} \prod_{d=1}^{D} p_d^{x_d^{(n)}} (1 - p_d)^{1 - x_d^{(n)}}$$

For each model M_i , we can marginalise out $\mathbf{p}^{(i)}$ to get $P(\{\mathbf{x}^{(n)}\}_{n=1}^N | M_i)$:

$$P(\{\mathbf{x}^{(n)}\}_{n=1}^{N}|M_i) = \int_0^1 \dots \int_0^1 P(\{\mathbf{x}^{(n)}\}_{n=1}^{N}|\mathbf{p}^{(i)}, M_i) P(\mathbf{p}^{(i)}|M_i) dp_1...dp_D$$

Given that the prior of any unknown probabilities is uniform, i.e. $P(\mathbf{p}^{(i)}|M_i) = 1$. We can simplify:

$$P(\{\mathbf{x}^{(n)}\}_{n=1}^{N}|M_i) = \int_0^1 \dots \int_0^1 P(\{\mathbf{x}^{(n)}\}_{n=1}^{N}|\mathbf{p}^{(i)}, M_i) dp_1 \dots dp_D$$

For M_1 :

$$P(\{\mathbf{x}^{(n)}\}_{n=1}^{N}|M_1) = \int_0^1 \dots \int_0^1 0.5^{N \cdot D} d\theta_1 \dots d\theta_D$$

We can remove the integrals:

$$P(\{\mathbf{x}^{(n)}\}_{n=1}^{N}|M_1) = (0.5)^{N \cdot D}$$

For M_2 , we have that all pixels share some probability p_d so we only need to integrate over a single variable p_d :

$$P(\{\mathbf{x}^{(n)}\}_{n=1}^{N}|M_2) = \int_0^1 \prod_{n=1}^{N} \prod_{d'=1}^{D} p_d^{x_{d'}^{(n)}} (1 - p_d)^{1 - x_{d'}^{(n)}} dp_d$$

Changing the products to sums:

$$P(\{\mathbf{x}^{(n)}\}_{n=1}^{N}|M_2) = \int_0^1 p_d^{\sum_{n=1}^{N} \sum_{d'=1}^{D} x_{d'}^{(n)}} (1 - p_d)^{\sum_{j=1}^{N} \sum_{d'=1}^{D} 1 - x_{d'}^{(n)}} dp_d$$

Rewriting:

$$P(\{\mathbf{x}^{(n)}\}_{n=1}^{N}|M_2) = \int_0^1 (p_d)^K (1 - p_{d'=1})^{N \cdot D - K} dp_d$$

where $K = \sum_{n=1}^{N} \sum_{d'=1}^{D} x_{d'}^{(n)}$.

This integral is the beta function:

$$P(\{\mathbf{x}^{(n)}\}_{n=1}^{N}|M_2) = \frac{K!(N \cdot D - K)!}{(N \cdot D + 1)!}$$

For M_3 , we need an integral for each p_d :

$$P(\{\mathbf{x}^{(n)}\}_{n=1}^{N}|M_3) = \int_0^1 \dots \int_0^1 \prod_{n=1}^N \prod_{d=1}^D p_d^{x_d^{(n)}} (1 - p_d)^{1 - x_d^{(n)}} dp_1 \dots dp_D$$

We can separate the integrals to only contain the relevant p_d :

$$P(\{\mathbf{x}^{(n)}\}_{n=1}^{N}|M_3) = \prod_{d=1}^{D} \left(\int_0^1 \prod_{n=1}^{N} p_d^{x_d^{(n)}} (1 - p_d)^{1 - x_d^{(n)}} dp_d \right)$$

Changing the products to sums:

$$P(\{\mathbf{x}^{(n)}\}_{n=1}^{N}|M_3) = \prod_{d=1}^{D} \left(\int_0^1 p_d^{\sum_{n=1}^{N} x_d^{(n)}} (1 - p_d)^{\sum_{n=1}^{N} 1 - x_d^{(n)}} dp_d \right)$$

In this case, we have the product of integrals where each evaluates to a beta function:

$$P(\{\mathbf{x}^{(n)}\}_{n=1}^{N}|M_3) = \prod_{d=1}^{D} \frac{K_d!(N-K_d)!}{(N+1)!}$$

where $K_d = \sum_{n=1}^N x_d^{(n)}$.

The posterior probability of a model M_i can be expressed:

$$P(M_i | \{\mathbf{x}^{(n)}\}_{n=1}^N) = \frac{P(\{\mathbf{x}^{(n)}\}_{n=1}^N | M_i) P(M_i)}{P(\{\mathbf{x}^{(n)}\}_{n=1}^N)}$$

We only have three models, so in this case the normalisation $P(\{\mathbf{x}^{(n)}\}_{n=1}^N)$ can be expressed as a sum:

$$P(M_i|\{\mathbf{x}^{(n)}\}_{n=1}^N) = \frac{P(\{\mathbf{x}^{(n)}\}_{n=1}^N|M_i)P(M_i)}{\sum_{i\in\{1,2,3\}}P(\{\mathbf{x}^{(n)}\}_{n=1}^N|M_i)P(M_i)}$$

Given that $P(M_i) = \frac{1}{3}$ for all $i \in \{1, 2, 3\}$:

$$P(M_i|\{\mathbf{x}^{(n)}\}_{n=1}^N) = \frac{P(\{\mathbf{x}^{(n)}\}_{n=1}^N|M_i)}{\sum_{i \in \{1,2,3\}} P(\{\mathbf{x}^{(n)}\}_{n=1}^N|M_i)}$$

Calculating the posterior probabilities of each of the three models having generated the data in binarydigits.txt using Python, we can show the values in the Table 1.

i	$P(M_i \{\mathbf{x}^{(n)}\}_{n=1}^N)$
1	1E-1924
2	1E-1858
3	1-(1E-1924)-(1E-1858)

Table 1: Posterior Probabilities

We can see that for models specified to have the same parameter value for all pixels, like M_1 , is very unlikely with the given data set. This makes sense because it is specifying models where the image is essentially blank (a uniform shade), which is not reflective of our digit images. Moreover, M_1 specifies a specific value of 0.5 for all the parameters whereas M_2 specifies any value for all the parameters as long as it's the same. So the model M_1 is just one possible model specified in M_2 and we can see this reflected in our probabilities when $P(M_2|\{\mathbf{x}^{(n)}\}_{n=1}^N) > P(M_1|\{\mathbf{x}^{(n)}\}_{n=1}^N)$.

The Python code for calculating the posterior probabilities of the three models:

```
import pandas as pd
      from scipy.special import betaln, logsumexp
 6
7
8
      \begin{array}{lll} \textbf{def} & \texttt{-log-p-d-given-m1} \, (\, x \colon \; \texttt{np.ndarray} \,) \; -\!\!\!> \; \textbf{float} : \end{array}
            Calculates log likelihood of model 1: param x: numpy array of shape (N, D): return: log likelihood """
10
11
            n, d = x.shape
13
14
            return n * d * np.log(0.5)
16
17
      def _log_p_d_given_m2(x: np.ndarray):
18
19
            Calculates log likelihood of model 2
            :param x: numpy array of shape (N, D)
:return: log likelihood
"""
20
21
22
            \begin{array}{ll} n\,,\;\;d=\,x\,.\,shape \\ k\,=\,np\,.\,sum(\,x\,)\,.\,astype\,(\,in\,t\,) \\ return\;\;betaln\,(\,k\,+\,1\,,\;n\,*\,d\,-\,k\,+\,1\,) \end{array}
23
24
25
26
27
28
      def _log_p_d_given_m3(x: np.ndarray):
            :param x: numpy array of shape (N, D) return: log likelihood
29
30
31
33
34
            n, = x.shape

k_d = np.sum(x, axis=0).astype(int)
            return logsumexp(betaln(k_d + 1, n - k_d + 1))
36
38
      def _log_p_model_given_data(x) -> np.ndarray:
            Calculates posterior log likelihood of models given image data
40
            :param x: numpy array of shape (N, D)
:return: posterior log likelihood
"""
41
42
44
            log_p_d_given_m = np.array(
45
                         -\log_{p}_{d}_{given_{m}}1(x),
                         log_p_d_given_m2(x),
log_p_d_given_m3(x),
47
48
49
50
51
            log_p_m_given_data = log_p_d_given_m - logsumexp(log_p_d_given_m)
            return log_p_m_given_data
55
      \begin{array}{lll} \texttt{def} & \texttt{c(x: np.ndarray, table\_path: str)} \ -\!\!\!> \ None: \end{array}
56
            Produces answers for question 2c
            :param x: numpy array of shape (N,\ D) :param table_path: path to store table posterior likelihoods
58
59
61
62
            log_p_m_given_data = _log_p_model_given_data(x)
            df = pd.DataFrame(
                   data=np.array(
                              np.arange(len(log-p-m-given_data)).astype(int) + 1,
[f"1E{int(x/np.log(10))}" for x in log-p-m-given_data[:-1]]
+ [
65
67
                                    f"1-\{'-'.join([f'(1E\{int(x/np.log(10))\})'|for x in log_p_m_given_data[:-1]])\}"
70
71
72
73
74
                  ).T.
                   columns=["Model", "P(M_i |D)"],
            df.set_index("Model", inplace=True)
df.to_csv(table_path)
```

src/solutions/q2.py

Question 3

(a) The likelihood for a model consisting of a mixture of K multivariate Bernoulli distributions can be expressed as the product across N data points:

$$P(\{\mathbf{x}^{(n)}\}_{n=1}^{N}|\theta) = \prod_{i=1}^{N} P(\mathbf{x}^{(n)}|\theta)$$

where $\{\mathbf{x}^{(n)}\}_{n=1}^{N}$ is our data set with $\mathbf{x}^{(n)} \in \mathbb{R}^{D \times 1}$ and $\theta = \{\pi, \mathbf{P}\}$ are our parameters, $\pi = [\pi_1, ..., \pi_K] \in \mathbb{R}^{K \times 1}$ our K mixing proportions $(0 \le \pi_k \le 1; \sum_k \pi_k = 1)$ and $\mathbf{P} \in \mathbb{R}^{D \times K}$ the K Bernoulli parameter vectors with elements p_{kd} denoting the probability that pixel d takes value 1 given mixture component k. We also assume the images are iid and that the pixels are independent of each other within each component distribution.

For each $P(\mathbf{x}^{(n)}|\theta)$:

$$P(\mathbf{x}^{(n)}|\theta) = \sum_{k=1}^{K} \pi_k \prod_{d=1}^{D} (p_{kd})^{x_d^{(n)}} (1 - p_{kd})^{1 - x_d^{(n)}}$$

The log-likelihood $\mathcal{L}(\mathbf{x}^{(n)}|\theta)$ can be expressed in vector form:

$$\mathcal{L}(\mathbf{x}^{(n)}|\theta) = \log \sum_{k=1}^{K} \pi_k \exp\left(\mathbf{x}^{(n)} \log(\mathbf{P}_k) + (1 - \mathbf{x}^{(n)}) \log(1 - \mathbf{P}_k)\right)$$

which can be further vectorised using Python scipy's logsumexp operation.

Moreover, the log-likelihood $\mathcal{L}(\{\mathbf{x}^{(n)}\}_{n=1}^N | \theta)$ can be expressed:

$$\mathcal{L}(\{\mathbf{x}^{(n)}\}_{n=1}^{N}|\theta) = \sum_{i=1}^{N} \left(\log \sum_{k=1}^{K} \pi_k \exp\left(\mathbf{x}^{(n)} \log(\mathbf{P}_k) + (1 - \mathbf{x}^{(n)}) \log(1 - \mathbf{P}_k)\right)\right)$$

(b) We know that:

$$P(A|B) \propto P(B|A)P(A)$$

Thus,

$$P(s^{(n)} = k | \mathbf{x}^{(n)}, \pi, \mathbf{P}) \propto P(\mathbf{x}^{(n)} | s^{(n)} = k, \pi, \mathbf{P}) P(s^{(n)} = k | \pi, \mathbf{P})$$

where $s^{(n)} \in \{1, ..., K\}$ a discrete hidden variable with $P(s^{(n)} = k | \mathbf{x}^{(n)}, \pi) = \pi_k$. Note that $P(s^{(n)} = k | \pi, \mathbf{P}) = P(s^{(n)} = k | \pi)$ as $s^{(n)}$ isn't dependent on \mathbf{P} .

Let \tilde{r}_{nk} be the unnormalised responsibility $P(\mathbf{x}^{(n)}|s^{(n)}=k,\pi,\mathbf{P})P(s^{(n)}=k|\pi,\mathbf{P})$. Using the mixture for component k, π_k and the likelihood function of component k:

$$\tilde{r}_{nk} = \pi_k \prod_{d=1}^{D} (p_{kd})^{x_d^{(n)}} (1 - p_{kd})^{1 - x_d^{(n)}}$$

Normalising across the components:

$$r_{nk} = \frac{\tilde{r}_{nk}}{\sum_{j=1}^{K} \tilde{r}_{nj}}$$

we have calculated $P(s^{(n)} = k | \mathbf{x}^{(n)}, \pi, \mathbf{P})$ for the E step of an EM algorithm. Moreover,

$$\log \tilde{r}_{nk} = \log \pi_k + \sum_{d=1}^{D} \left(x_d^{(n)} \log(p_{kd}) + (1 - x_d^{(n)}) \log(1 - \exp(\log(p_{kd}))) \right)$$

and

$$\log r_{nk} = \log \tilde{r}_{nk} - \log \sum_{i=1}^{K} \exp(\log \tilde{r}_{nj})$$

which can be vectorised as $\log \mathbf{r}$ calculated with $\log \pi$ and $\log \mathbf{P}$ using Python scipy's logsum exp operation.

(c) We know that the expectation log joint can be expressed:

$$\left\langle \sum_{n} \log P(\mathbf{x}^{(n)}, s^{(n)} | \pi, \mathbf{P}) \right\rangle_{q(\{s^{(n)}\})} = \sum_{n=1}^{N} q(s^{(n)}) \log P(\mathbf{x}^{(n)}, s^{(n)} | \pi, \mathbf{P})$$

Let this quantity be E. For each term of E:

$$q(s^{(n)}) = \mathbf{r}_n^T$$

and

$$\log P(\mathbf{x}^{(n)}, s^{(n)} | \pi, \mathbf{P}) = \log[P(\mathbf{x}^{(n)} | s^{(n)}, \pi, \mathbf{P})P(s^{(n)} | \pi, \mathbf{P})]$$

which is the vectorised version of $\log \tilde{r}_{nk}$ from part (b) so:

$$\log P(\mathbf{x}^{(n)}, s^{(n)} | \pi, \mathbf{P}) = \log(\pi) + \log(\mathbf{P})^T \mathbf{x}^{(n)} + \log(1 - \mathbf{P})^T (1 - \mathbf{x}^{(n)})$$

Combining:

$$E = \sum_{n} \mathbf{r}_{n}^{T} [\log(\pi) + \log(\mathbf{P})^{T} \mathbf{x}^{(n)} + \log(1 - \mathbf{P})^{T} (1 - \mathbf{x}^{(n)})]$$

To maximise with respect to π and \mathbf{P} for the M step, we want to take the derivative, set to zero, and solve for $\hat{\pi}$ and $\hat{\mathbf{P}}$.

For the k^{th} element of π :

$$\frac{\partial E}{\partial \pi_k} = \sum_{n} r_{nk} \frac{1}{\pi_k}$$

We can calculate the maximiser with:

$$\frac{\partial E}{\partial \pi_k} + \lambda = 0$$

where λ is a Lagrange multiplier ensuring that the mixing proportions sum to unity.

Thus,

$$\hat{\pi}_k = \frac{\sum_n r_{nk}}{N}$$

For the dk^{th} element of **P**:

$$\frac{\partial E}{\partial \mathbf{P}_{dk}} = \sum_{n} r_{nk} \frac{\partial}{\partial \mathbf{P}_{dk}} [x_d^{(n)} \log \mathbf{P}_{dk} + (1 - x_d^{(n)}) \log(1 - \mathbf{P}_{dk})]$$

Simplifying:

$$\frac{\partial E}{\partial \mathbf{P}_{dk}} = \sum_{n} r_{nk} \left(\frac{x_d^{(n)}}{\mathbf{P}_{dk}} - \frac{1 - x_d^{(n)}}{1 - \mathbf{P}_{dk}} \right)$$

Setting the derivative to zero:

$$\frac{\sum_{n} x_{d}^{(n)} r_{nk}}{\hat{\mathbf{P}}_{dk}} - \frac{\sum_{n} r_{nk} - \sum_{n} x_{d}^{(n)} r_{nk}}{1 - \hat{\mathbf{P}}_{dk}} = 0$$

Solving for $\hat{\mathbf{P}}_{dk}$:

$$\hat{\mathbf{P}}_{dk} \sum_{n} r_{nk} - \hat{\mathbf{P}}_{dk} \sum_{n} x_d^{(n)} r_{nk} = \sum_{n} x_d^{(n)} r_{nk} - \hat{\mathbf{P}}_{dk} \sum_{n} x_d^{(n)} r_{nk}$$

Thus,

$$\hat{\mathbf{P}}_{dk} = \frac{\sum_{n} x_d^{(n)} r_{nk}}{\sum_{n} r_{nk}}$$

We have the maximizing parameters for the expected log-joint

$$\arg \max_{\pi, \mathbf{P}} \left\langle \sum_{n} \log P(\mathbf{x}^{(n)}, s^{(n)} | \pi, \mathbf{P}) \right\rangle_{q(\{s^{(n)}\})}$$

thus obtaining an iterative update for the parameters π and **P** in the M-step of EM.

For numerical stability, we can compute the maximisation step for the MAP of \mathbf{P} , by solving for $\hat{\mathbf{P}}_{dk}^{MAP}$ with:

$$\frac{\partial E'}{\partial \mathbf{P}_{dk}} = 0$$

where

$$E' = \sum_{n=1}^{N} q(s^{(n)}) \log P(\mathbf{P}|\pi, \mathbf{x}^{(n)}, s^{(n)})$$

and from Bayes':

$$\log P(\mathbf{P}|\pi, \mathbf{x}^{(n)}, s^{(n)}) = \log P(\mathbf{x}^{(n)}, s^{(n)}|\pi, \mathbf{P}) + \log P(\mathbf{P}) - \log P(\mathbf{x}^{(n)}, s^{(n)}|\pi)$$

Assuming an independent Beta prior on each pixel of each component:

$$\log P(\mathbf{P}) = \sum_{k=1}^{K} \sum_{d=1}^{D} -\log(B(\alpha, \beta)) + (\alpha - 1)\log \mathbf{P}_{dk} + (\beta - 1)\log(1 - \mathbf{P}_{dk})$$

and

$$\frac{\partial \log P(\mathbf{P})}{\partial \mathbf{P}_{dk}} = \frac{(\alpha - 1)}{\mathbf{P}_{dk}} - \frac{(\beta - 1)}{1 - \mathbf{P}_{dk}}$$

Thus, the derivative can be expressed as:

$$\frac{\partial E'}{\partial \mathbf{P}_{dk}} = \sum_{n} \left(r_{nk} \left(\frac{\partial \log P(\mathbf{x}^{(n)}, s^{(n)} | \pi, \mathbf{P})}{\partial \mathbf{P}_{dk}} + \frac{\partial \log P(\mathbf{P})}{\partial \mathbf{P}_{dk}} \right) \right)$$

Substituting the appropriate expressions:

$$\frac{\partial E'}{\partial \mathbf{P}_{dk}} = \sum_{n} \left(r_{nk} \left(\frac{x_d^{(n)}}{\mathbf{P}_{dk}} - \frac{1 - x_d^{(n)}}{1 - \mathbf{P}_{dk}} + \frac{(\alpha - 1)}{\mathbf{P}_{dk}} - \frac{(\beta - 1)}{1 - \mathbf{P}_{dk}} \right) \right)$$

Simplifying:

$$\frac{\partial E'}{\partial \mathbf{P}_{dk}} = \frac{\sum_{n} r_{nk} (\alpha - 1 + x_d^{(n)})}{\mathbf{P}_{dk}} - \frac{\sum_{n} r_{nk} (\beta - x_d^{(n)})}{1 - \mathbf{P}_{dk}}$$

Setting $\frac{\partial E'}{\partial \mathbf{P}_{dk}} = 0$ we can calculate $\hat{\mathbf{P}}_{dk}^{MAP}$:

$$\sum_{n} r_{nk}(\alpha - 1 + x_d^{(n)}) - \hat{\mathbf{P}}_{dk} \sum_{n} r_{nk}(\alpha - 1 + x_d^{(n)}) = \hat{\mathbf{P}}_{dk} \sum_{n} r_{nk}(\beta - x_d^{(n)})$$

$$\hat{\mathbf{P}}_{dk}^{MAP} = \frac{\sum_{n} r_{nk} (x_d^{(n)} + \alpha - 1)}{(\alpha + \beta - 1)(\sum_{n} r_{nk})}$$

As a sense check, we can see when setting $\alpha = 1$ and $\beta = 1$ we recover $\hat{\mathbf{P}}_{dk}^{MLE}$ as we would expect. For the following parts, a Beta(2, 2) prior was used.

(d) Plotting the unnormalised posterior likelihood as a function of the iteration number for different k values:

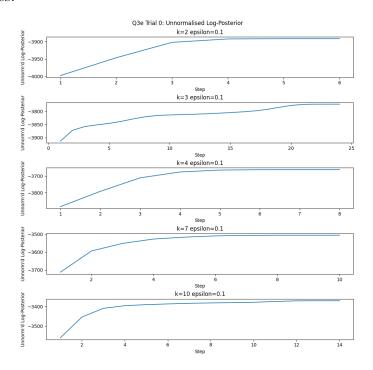


Figure 4: Log Likelihood vs Iteration Number

where *epsilon* is the stopping condition for when the unnormalised log posterior converges sufficiently. Note that the normalisation constant for the log posterior $\log P(\mathbf{x}^{(n)}, s^{(n)}|\pi)$ is intractable and so only the unnormalised portion $\log P(\mathbf{x}^{(n)}, s^{(n)}|\pi, \mathbf{P}) + \log P(\mathbf{P})$ was computed and reported.

Displaying the parameters found for $K \in \{2, 3, 4, 7, 10\}$:

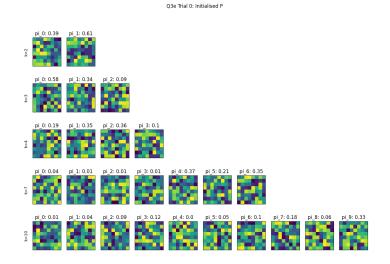


Figure 5: Randomly initialised parameters

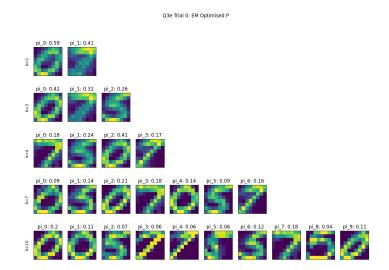


Figure 6: EM optimised parameters

The Python code for the EM algorithm:

```
from dataclasses import dataclass
from typing import List, Tuple
 3
       import matplotlib.pyplot as plt
      import numpy as np
from scipy.special import betaln, logsumexp
from sklearn.manifold import TSNE
       from src.constants import DEFAULT_SEED
10
      @dataclass
       class Theta:
             Data class containing the model parameters
             log-pi: the logarithm of the mixing proportions (1, k)
log-p_matrix: the logarithm of the probability where the (i,j)th element is the probability that
pixel j takes value 1 under mixture component i (d, k)
16
17
19
20
             log_pi: np.ndarray
             log_p_matrix: np.ndarray
22
24
             def pi(self) -> np.ndarray:
25
                   Calculates the mixing proportions :return: vector of mixing proportions (1, k)
30
                    return np.exp(self.log_pi)
31
33
34
             \begin{array}{ll} \textbf{def} & \texttt{p-matrix} \, (\, \, \texttt{self} \, ) \, \, -\!\!\!> \, \texttt{np.ndarray} \, ; \end{array}
                   Calculates the Bernoulli parameters :return: matrix Bernoulli parameters (d, k)
35
36
38
                    \begin{array}{lll} d\,, & k \,=\, s\,elf\,.\,log\,‐p\,‐m\,atrix\,.\,shape \\ image\_dimension \,=\, int\,(np\,.\,sqrt\,(d)\,) \end{array}
                    return np.exp(self.log_p_matrix).reshape(image_dimension, image_dimension, -1)
42
             def log_one_minus_p_matrix(self) -> np.ndarray:
44
                    Compute \log(1-P) where P=\exp(\log_-p\_matrix) :return: an array of the same shape as \log_-p\_matrix (d, k)
45
                   log_of_one = np.zeros(self.log_p_matrix.shape)
stacked_sum = np.stack((log_of_one, self.log_p_matrix))
weights = np.ones(stacked_sum.shape)
weights[1] = -1 # scale p matrix by -1 for subtraction
return np.array(logsumexp(stacked_sum, b=weights, axis=0))
49
50
53
54
             def log_pi_repeated(self, n: int) \rightarrow np.ndarray:
55
56
57
                    Repeats the log_pi vector n times along axis 0 :param n: number of repetitions :return: an array of shape (n, k) """
58
59
60
                    return np.repeat(self.log_pi, n, axis=0)
61
62
      \label{eq:def_init_params} \begin{array}{lll} def & \verb"-init_params" (k: int), & d: int) & -> & Theta: \end{array}
64
65
             Random initialisation of theta parameters (log_pi and log_p_matrix)
             :param k: Number of components
:param d: Image dimension (number of pixels in a single image)
:return: theta: the parameters of the model
66
67
70
71
72
73
74
                    log_pi=np.log(np.random.dirichlet(np.ones(k), size=1)), log_p_matrix=np.log(np.random.uniform(low=0, high=1, size=(d, k))),
       def _compute_log_component_p_x_i_given_theta(x: np.ndarray, theta: Theta) -> np.ndarray:
             Compute the unweighted probability of each mixing component for each image
             :param x: the image data (n, d)
80
              param theta: the parameters of the model
             :return: an array of the unweighted probabilities (n, k)
81
83
84
              return x @ theta.log_p_matrix + (1 - x) @ theta.log_one_minus_p_matrix
       \begin{array}{lll} \textbf{def} & \texttt{\_compute\_log\_p\_x\_i\_given\_theta} \, (x: & \texttt{np.ndarray} \, , & \texttt{theta:} & \texttt{Theta}) \, \to & \texttt{np.ndarray:} \end{array}
86
              Computes the log likelihood of each image in the dataset x
             :param x: the image data (n, d)::param theta: the parameters of the model :return: log_p_x_i=given_theta: a log_i likelihood array containing the log_i likelihood of each image (n, d)
89
91
             ,1)
             n\,,\ _{-}\,=\,x\,.\,s\,h\,a\,p\,e
```

```
94
                      log_component_probabilities = _compute_log_component_p_x_i_given_theta(
 95
                      x, theta
) # (n, k)
 96
  97
                      return np.array(
                                logsumexp(
 98
                                        log_component_probabilities + theta.log_pi_repeated(n), # scale each component by component probability
 99
100
                               )
            def \_compute\_log\_likelihood(x: np.ndarray, theta: Theta) \rightarrow float:
106
107
                      Computes the log likelihood of all images in the dataset x
108
                      :param x: the image data (n, d):param theta: the parameters of the model :return: \log_{p_x} 
109
                      return np.sum(_compute_log_p_x_i_given_theta(x, theta)).item()
114
            {\tt def} \  \  \, {\tt \_compute\_log\_prior} \, (
116
           theta: Theta, alpha-parameter: float, beta-parameter: float) -> float;
118
119
                      Compute the prior log probability of the P matrix under a Beta prior
                      :param theta: the parameters of the model
:param alpha_parameter: alpha parameter of the beta prior
:param beta_parameter: beta parameter of the beta prior
                      :return: log_p_of_p_matrix
124
126
                      return np.sum(
                               -betaln(alpha_parameter, beta_parameter)
+ (alpha_parameter - 1) * theta.log_p_matrix
+ (beta_parameter - 1) * theta.log_one_minus_p_matrix
                      ).item()
130
132
            def _compute_unnormalised_log_posterior_likelihood(
133
                     x: np.ndarray, theta: Theta, alpha_parameter: float, beta_parameter: float
            ) -> float:
136
                      Compute the unnormalised posterior log probability of the P matrix :param x: the image data (n,\ d) :param theta: the parameters of the model
137
138
139
                      :param alpha-parameter: alpha parameter of the beta prior
:param beta-parameter: beta parameter of the beta prior
140
141
                      :return: log_p_of_p_matrix
143
                      log_likelihood = _compute_log_likelihood(x, theta)
144
                      log_prior = _compute_log_prior(theta, alpha_parameter, beta_parameter)
return log_likelihood + log_prior
146
147
149
            \begin{array}{lll} \textbf{def} & \texttt{\_compute\_log\_e\_step} \ (x: & \texttt{np.ndarray} \ , & \texttt{theta:} \ \textbf{Theta}) \ -\!\!\!\!> \ \texttt{np.ndarray} \ : \end{array}
                      Compute the e step of expectation maximisation
                      :param x: the image data (n, d):param theta: the parameters of the model
                      :return: an array of the log responsibilities of k mixture components for each image (n,\,k)
154
                      log_r_unnormalised = _compute_log_component_p_x_i_given_theta(x, theta)
                      log_r_normaliser = logsumexp(log_r_unnormalised, axis=1)
log_responsibility = log_r_unnormalised - log_r_normaliser[:, np.newaxis]
157
                      return log_responsibility
160
161
            def _compute_log_pi_hat(log_responsibility: np.ndarray) -> np.ndarray:
163
                      Compute the log of the maximised mixing proportions:param_log_responsibility: an array of the log responsibilities of k mixture components for each image
                       (n, k)
                      :return: an array of the maximised log mixing proportions (1, \boldsymbol{k}) """
166
167
                                = log_responsibility.shape
168
                      return (logsumexp(log_responsibility, axis=0) - np.log(n)).reshape(1, -1)
170
            def _compute_log_p_matrix_hat(
                      x: np.ndarray,
log_responsibility: np.ndarray,
\begin{array}{c} 173 \\ 174 \end{array}
                      alpha_parameter: float,
beta_parameter: float,
\begin{array}{c} 176 \\ 177 \end{array}
            ) \rightarrow np.ndarray:
                      Compute the log of the maximised pixel probabilities
                      :param x: the image data (n, d)
180
                        param log_responsibility: an array of the log responsibilities of k mixture components for each image
181
                      (n, \kappa):param alpha-parameter: alpha parameter of the beta prior:param beta-parameter: beta parameter of the beta prior:return: an array of the maximised pixel probabilities for each component (d, k)"""
182
183
184
186
                     n, d = x.shape
_, k = log_responsibility.shape
187
```

```
188
              189
190
191
192
              ) # (n, d, k)
194
              \label{log_p_matrix_unnormalised_posterior} \begin{array}{l} log\_nexp(\\ log\_responsibility\_repeated \;,\; b=(x\_repeated \; + \; alpha\_parameter \; - \; 1) \;,\; axis=0 \end{array}
195
              ) # (d, k)
196
              \label{logpmatrix_normaliser_posterior} \begin{array}{l} log\_p\_matrix\_normaliser\_posterior = logsumexp( \\ log\_responsibility\_repeated \,, \, b=(alpha\_parameter \, + \, beta\_parameter \, - \, 1) \,, \, axis=0 \\ ) \ \# \ (d\,, \, k) \end{array}
108
199
200
201
202
              log_p_matrix_normalised_posterior = (
203
                    log_p_matrix_unnormalised_posterior - log_p_matrix_normaliser_posterior
                  # (d,
204
                            k)
205
              return log_p_matrix_normalised_posterior
206
207
208
       def _compute_log_m_step(
              x: np.ndarray,
log_responsibility: np.ndarray,
209
210
              alpha_parameter: float,
beta_parameter: float,
       ) -> Theta:
213
              Compute the m step of expectation maximisation :param x: the image data (n, d) :param log_responsibility: an array of the log responsibilities of k mixture components for each image
216
217
               (n, k)
              :param alpha-parameter: alpha parameter of the beta prior :param beta-parameter: beta parameter of the beta prior :return: thetas optimised after maximisation step """
219
220
222
                    log_pi=_compute_log_pi_hat(log_responsibility),
log_p_matrix=_compute_log_p_matrix_hat(
                          x, log_responsibility, alpha_parameter, beta_parameter
226
228
229
       def _run_expectation_maximisation(
              x: np.ndarray,
theta: Theta,
232
              alpha_parameter: float,
beta_parameter: float,
max_number_of_steps: int,
233
              epsilon: float,
236
237
       ) -> Tuple [Theta, np.ndarray, List [float]]:
              Run the expectation maximisation algorithm
              :param x: the image data (n, d) :param theta: initial theta parameters
240
              :param alpha_parameter: alpha parameter of the beta prior
:param beta_parameter: beta parameter of the beta prior
:param max_number_of_steps: the maximum number of steps to run the algorithm
242
243
244
              :param epsilon: the minimum required change in log posterior, otherwise the algorithm stops early :return: a tuple containing the optimised thetas, the log responsibilities,

and the log log-posteriors at each step of the algorithm
245
247
248
              log_responsibility = None
              log_posteriors = []
for _ in range(max_number_of_steps):
250
              for _ in range(max_number_of_steps):
    log_responsibility = _compute_log_e_step(x, theta)
    theta = _compute_log_m_step(
253
254
                         x, log_responsibility, alpha_parameter, beta_parameter
256
                    log_posteriors.append(
258
                          _compute_unnormalised_log_posterior_likelihood(
259
                                x, theta, alpha_parameter, beta_parameter
260
261
262
                         check for early stopping
                    if len(log_posteriors) > 1:
    if (log_posteriors[-1] - log_posteriors[-2]) < epsilon:
        break
264
265
266
267
              return theta, log_responsibility, log_posteriors
268
269
       def _visualise_p_matrix(
     thetas: List[Theta], ks: List[int], figure_title: str, figure_path: str
270
       ) -> None:
273
              Visualises the P matrix for different thetas and ks:param thetas: list of Theta instances:param ks: list of k values used for each Theta:param figure_title: name of figure
276
278
              :param figure_path: path to store figure
              :return:
279
             n = len(ks)
281
282
             m = np.max(ks)
```

```
283
               fig = plt.figure()
284
               fig.set_figwidth(15)
285
               fig.set\_figheight(10)
               for i, k in enumerate(ks):
for j in range(k):
286
287
                           ax = plt.subplot(n, m, m * i + j + 1)
ax.imshow(
    thetas[i].p_matrix[:, :, j],
    interpolation="None",
288
289
200
291
203
                             ax.tick_params(
                                   axis="x",
which="both",
294
295
296
                                   bottom=False ,
                                   top=False,
298
                             ax.tick_params (
300
                                   axis="y",
which="both",
301
                                   left=False,
302
303
                                   right=False,
304
                            ax.xaxis.set_ticklabels([])
305
                            ax.yaxis.set_ticklabels([])
ax.yaxis.set_ticklabels([])
ax.set_title(f"pi_{j}: {np.round(thetas[i].pi[0, j], 2)}")
306
307
308
                             if j == 0:
               ax.set_ylabel(f"{k=}")
fig.suptitle(figure_title)
plt.savefig(figure_path)
309
310
311
313
       def _visualise_responsibility_clusters(
    log_responsibilities: List[np.ndarray],
314
315
               ks: List[int],
figure_title: str,
316
318
               \label{figure_path:str} \texttt{figure_path:} \ \ \mathbf{str} \ ,
319
        ) -> None:
320
              Visualise responsibility vectors of images using TSNE for different k values :param log_responsibilities: list of log responsibilities for different ks :param ks: list of k values used for each Theta :param figure_title: name of figure :param figure_path: path to store figure
321
322
324
325
               :return:
327
328
              n = len(ks)
               fig = plt.figure()
fig.set_figwidth(5 * n)
fig.set_figheight(5)
330
331
               for i, k in enumerate(ks):
if k > 2:
332
                            # use TSNE when
                                                       we have more than 2 dimensions
335
                            embedding = TSNE(
                                   n_{-components}=2,
                                    learning_rate="auto",
                                   init="random", perplexity=10,
338
339
                                    random_state=DEFAULT_SEED,
340
                            ).fit_transform(log_responsibilities[i])
341
                                                                                  sponsibility vectors without dimensionality reduction
343
                            # otherwise we can visualise
                     embedding = np.exp(log_responsibilities[i])
ax = plt.subplot(1, n, i + 1)
ax.scatter(embedding[:, 0], embedding[:, 1])
344
346
                     ax.set_title(f" {k=}
               fig.suptitle(figure_title)
plt.savefig(figure_path, bbox_inches="tight")
349
350
        def _plot_log_posteriors (
352
               log_posteriors: List[List[float]],
ks: List[int],
epsilon: float,
353
354
355
356
               figure_title: str,
357
               figure_path: str,
        ) -> None:
              Plot log posteriors as a function of EM iteration for different ks: param log-posteriors: list of vectors, each representing the log posterior during EM for a specific k: param ks: list of k values used for each Theta
360
361
               :param epsilon: value used for early stopping of EM :param figure_title: name of figure
363
364
365
               :param figure_path: path to store figure
               :return:
366
367
               fig , ax = plt.subplots(len(ks), 1, constrained_layout=True) fig .set_figwidth(10) fig .set_figheight(10)
368
369
370
              fig.set_rignergnt(10)
for i, k in enumerate(ks):
    ax[i].plot(np.arange(1, len(log_posteriors[i]) + 1), log_posteriors[i])
    ax[i].set_xlabel("Step")
    ax[i].set_ylabel(f"Unnorm'd Log_Posterior")
    ax[i].set_title(f"{k=} {epsilon=}")
373
374
375
               plt.suptitle (figure_title)
               plt.savefig(figure_path)
```

```
380
          def e(
381
382
                 x: np.ndarray,
383
                  alpha_parameter: float,
                 beta_parameter: float,
number_of_trials: int,
384
385
                 ks: List[int],
epsilon: float,
max_number_of_steps: int,
386
387
                 figure_path: str, figure_title: str,
380
390
391
         ) -> None:
392
                 Produces answers for question 3e:param x: numpy array of shape (N, D)
393
394
                 :param x: numpy array of snape (N, D)
:param alpha-parameter: alpha parameter of the beta prior
:param beta-parameter: beta parameter of the beta prior
:param number-of-trials: number of trails to run EM
:param ks: k values to use for each trial
:param epsilon: value used for early stopping of EM
395
396
397
399
                  :param max_number_of_steps: maximum number of steps during EM :param figure_title: base name of figures :param figure_path: base paths to store figure
400
401
402
                 :return:
403
404
405
                 n, d = x.shape
np.random.seed(DEFAULT_SEED)
for i in range(number_of_trials):
    init_thetas: List[Theta] = []
    em_thetas: List[Theta] = []
    log_posteriors: List[List[float]] = []
    log_responsibilities: List[np.ndarray] = []
    for j, k in enumerate(ks):
        init_theta = _init_params(k, d)
        em_theta_log_responsibility_log_poste
                 n, d = x.shape
406
407
408
409
410
411
412
                                  {\tt em\_theta}\;,\;\; {\tt log\_responsibility}\;,\;\; {\tt log\_posterior}\; =\; {\tt \_run\_expectation\_maximisation}\; (
414
415
                                          theta=init_theta ,
alpha_parameter=alpha_parameter ,
beta_parameter=beta_parameter ,
417
418
419
                                          epsilon=epsilon,
420
                                          max_number_of_steps=max_number_of_steps,
421
422
                                  init_thetas.append(init_theta)
423
                                 em_thetas.append(em_theta)
log_responsibilities.append(log_responsibility)
424
425
                                  log-posteriors.append(log-posterior)
426
                          _visualise_p_matrix (
428
                                 init_thetas .
429
                                 figure_title=f"{figure_title} Trial {i}: Initialised P", figure_path=f"{figure_path}-{i}-initialised-p.png",
431
432
                          _visualise_p_matrix(
433
                                 em_thetas, ks,
434
435
                                 figure_title=f"{figure_title} Trial {i}: EM Optimised P", figure_path=f"{figure_path}-{i}-optimised-p.png",
436
437
                          _visualise_responsibility_clusters(
log_responsibilities,
439
440
                                 figure_title=f"{figure_title} Trial {i}: TSNE Responsibility Visualisation", figure_path=f"{figure_path}-{i}-tsne.png",
442
443
                          _plot_log_posteriors(
log_posteriors,
445
446
448
                                  figure_title=f"{figure_title} Trial {i}: Unnormalised Log-Posterior", figure_path=f"{figure_path}-{i}-log-pos.png",
449
450
451
```

src/solutions/q3.py

(e) Running the algorithm a few times starting from randomly chosen initial conditions and visualising the parameters:

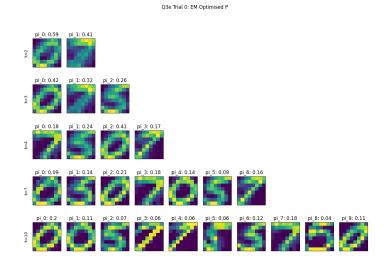


Figure 7: EM optimised parameters: Trial 0

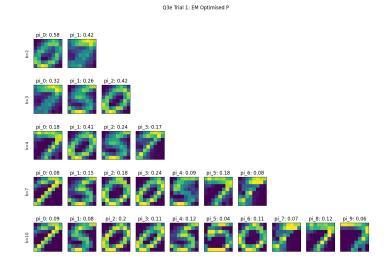


Figure 8: EM optimised parameters: Trial 1

Q3e Trial 2: EM Optimised P

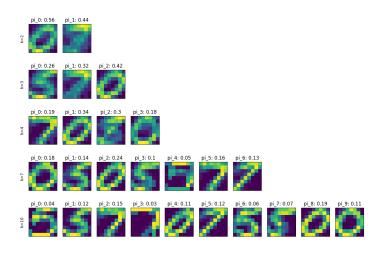


Figure 9: EM optimised parameters: Trial 2

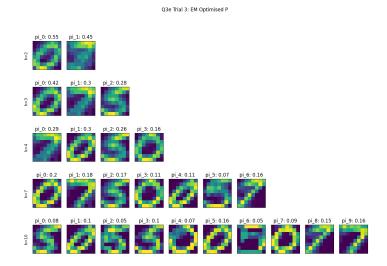


Figure 10: EM optimised parameters: Trial 3

For smaller k, we can visually see that we obtain very similar solutions (a seven and a zero for k = 2). For k = 3, we get one each of zero, seven, and five, but in different permutations for different trials. However for higher K, we see that this may not always be the case. For Trial 1 of k = 10, we have three 5's whereas in Trial 3 we have four 5's. Interestingly, different clusters of the same digits can be different, representing different variants of the written digit (i.e. a slanted zero, a slightly slanted zero, and a symmetric zero).

Moreover, looking at the responsibilities of each mixture component, we can see that when k is relatively small they are relatively evenly distributed. However for k = 7 and especially k = 10, we can see some components have very small or zero probability (i.e. π_3 of trial 2). It will be unlikely for those components to represent very distinct clusters (i.e. the parameters for π_2 and π_3 are very similar in trial 2) This can be verified when we perform a TSNE visualisation of the responsibility vector for each of the images (Note that for k = 2, just the responsibility vector is plotted because it is two dimensional). We can see that for large k, qualitatively the number of clusters no longer matches the k value, indicating that some mixtures are redundant. For example for k = 7 and k = 10 we can only qualitatively see three to five clusters with TSNE.

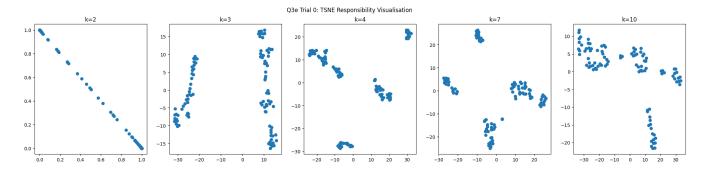


Figure 11: TSNE Visualisation of Image responsibilities: Trial 0

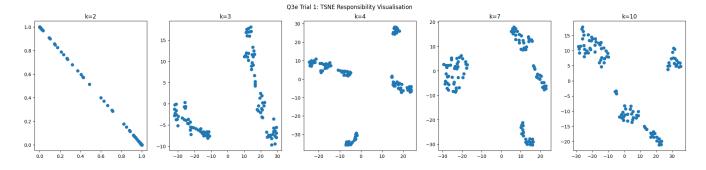


Figure 12: TSNE Visualisation of Image responsibilities: Trial 1

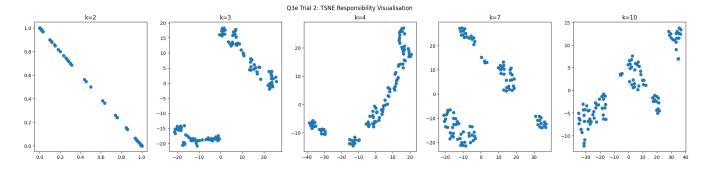


Figure 13: TSNE Visualisation of Image responsibilities: Trial 2

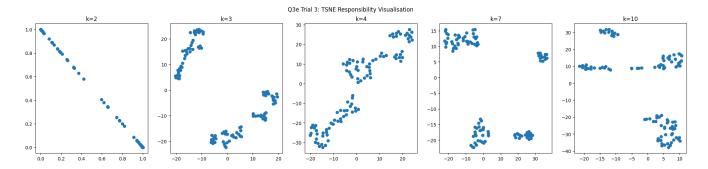


Figure 14: TSNE Visualisation of Image responsibilities: Trial 3

Improvements to the model could include searching for an optimal k by maximising the log posterior with regularisation on the magnitude of k to balance maximising log posterior with minimising model complexity. Additionally, adding a prior on the responsibility components can be helpful to ensure a more even distribution across mixture components unlike the components visualised here. This could help promote more meaningful clusters as k increases. Moreover, more experimentation for choosing better priors can be helpful to find better separation between mixtures. Finally, increasing the size of our data set (i.e. more images) and resolution of our images (i.e. more pixels) can help the model better understand the distinguishing nuances of different mixtures and provide better clustering, although the number of images and the resolution should scale together to ensure that the model doesn't learn the noise in the higher resolution images. This is assuming we are able to scale our computing resources. Finally, given that we know that there are ten digits and our current data set only includes a subset of these digits, we can also expand our data set to include all ten digits. Hopefully, for k = 10, we will then be able to achieve a unique digit for each mixing component, rather than variations of repeated digits as we see now.

Question 5

(a) The formulae for the ML estimates of $P(s_i = \alpha | s_{i-1} = \beta) = \Psi(\alpha, \beta)$:

$$\Psi(\alpha,\beta) = \frac{N_{\alpha,\beta}}{N_{\beta}}$$

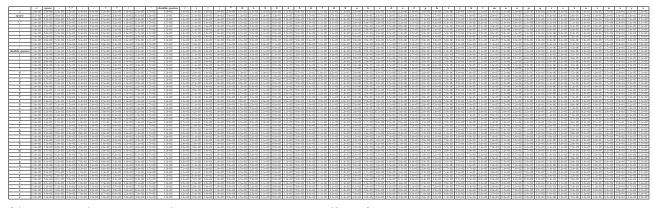
where $N_{\alpha,\beta}$ is the count of the number of occurrences of the pair (α,β) , where β is followed by $s\alpha$ in the text and N_{β} is the number of occurrences of β . Moreover to ensure ergodicity, a one was added to each $N_{\alpha,\beta}$. This was also taken into account for the normaliser N_{β} .

Moreover, the stationary distribution ϕ can be calculated using the power method:

- (i) Initialise any $\phi^{(0)} \in \mathbb{R}^{53 \times 1}$ and $\sum_i \phi_i^{(0)} = 1$
- (ii) Repeat $\phi^{(i+1)} = \Psi \phi^{(i)}$
- (iii) Terminate when $\phi^{(i+1)-\phi^{(i)}<\epsilon}$

where $\Psi \in \mathbf{R}^{53 \times 53}$ containing the transition probabilities, $\Psi_{i,j} = P(s_j | s_i)$ where s_i is the i^{th} symbol and s_j is the j^{th} symbol, and ϵ is some small number indicating sufficient convergence of the distribution to be considered stationary. The function $\phi(\gamma)$ is simply the index of symbol γ in the vector ϕ .

The transition matrix Ψ :



(Apologies for the tiny font, latex was being difficult)

The invariant distribution ϕ :

Symbol	Probability
=	1.7e-05
space	1.7e-01
-	6.1e-04
	1.2e-02
;	3.9e-04
:	2.9e-04
<u> </u>	6.0e-04
?	4.7e-04
- /	1.9e-05
/	7.7e-03
,	1.9e-05
double quotes	2.4e-05
(2.4e-03 2.3e-04
)	2.2e-04
r	1.7e-05
1	1.7e-05
*	1.1e-03
0	6.9e-05
1	1.4e-04
2	6.0e-05
3	3.4e-05
4	2.3e-05
	3.2e-05
5 6	3.2e-05
7	
8	2.8e-05
9	7.6e-05 2.6e-05
a a	6.6e-02
b b	
С	1.1e-02
	2.0e-02 3.8e-02
d	
e f	1.0e-01 1.8e-02
	1.6e-02
g h	5.4e-02
i	
j	5.6e-02 8.5e-04
J k	6.4e-03
1	3.1e-02
	2.0e-02
m	5.9e-02
n	6.2e-02
0	
P	1.5e-02
q	7.7e-04
r	4.7e-02
s	5.2e-02
t	7.2e-02
u	2.1e-02
V	8.5e-03
W	1.9e-02
X	1.4e-03
У	1.5e-02
Z	7.4e-04

(b) The latent variables $\sigma(s)$ for different symbols s are not independent. This is because by choosing an encoding for one symbol $e = \sigma(s)$, the encoding for a second symbol $\sigma(s')$ cannot be e. We have 53 symbols but only 52 degrees of freedom, because once we have defined the encoding for 52 symbols, the encoding for the 53^{rd} symbol cannot be chosen. Thus, there exists a dependence between $\sigma(s)$ for different symbols s.

The joint probability of the encrypted text $e_1e_2\cdots e_n$ given σ :

$$P(e_1, e_2, ..., e_n | \sigma) = \phi(\gamma = \sigma^{-1}(e_1)) \prod_{i=2}^n \psi(\alpha = \sigma^{-1}(e_i), \beta = \sigma^{-1}(e_{i-1}))$$

because σ is the encoding function, mapping a symbol s into the encoded symbol e, we require σ^{-1} the decoding function mapping the encoded symbol e back to s.

(c) The proposal probability $S(\sigma \to \sigma')$ depends on the permutations of σ and σ' . Our proposal generating process restricts us to choose a proposal σ' that differs from σ only at two spots:

$$\sigma'(s^i) = \sigma(s^j)$$

$$\sigma'(s^j) = \sigma(s^i)$$

for any two symbols s^i and s^j of the 53 possible symbols $(s^i \neq s^j)$.

Therefore, if the above doesn't hold for σ' , $S(\sigma \to \sigma') = 0$. From σ there are $\binom{53}{2}$ possible proposal σ' 's with the above property. Because we are assuming a uniform prior distribution over σ 's, the transition probability of a σ' that satisfies the above property is $S(\sigma \to \sigma') = \frac{1}{\binom{53}{2}}$.

The MH acceptance probability is given as:

$$A(\sigma \to \sigma'|\mathcal{D}) = \min\{1, \frac{S(\sigma' \to \sigma)P(\sigma'|\mathcal{D})}{S(\sigma \to \sigma')P(\sigma|\mathcal{D})})\}$$

because $S(\sigma \to \sigma')$ is the conditional transition probability of σ' given σ and \mathcal{D} is our encrypted text $e_1, e_2, ..., e_n$.

 $S(\sigma \to \sigma') = S(\sigma' \to \sigma)$ for all σ and σ' that differ only at two spots because the probability in this case will always be $\frac{1}{\binom{53}{2}}$, we can simplify:

$$A(\sigma \to \sigma' | \mathcal{D}) = \min\{1, \frac{P(\sigma' | \mathcal{D})}{P(\sigma | \mathcal{D})}\}$$

From Bayes' Theorem:

$$P(\sigma|\mathcal{D}) = \frac{P(\mathcal{D}|\sigma)P(\sigma)}{\sum_{\sigma'} P(\mathcal{D}|\sigma')P(\sigma')}$$

We are assuming a uniform prior for σ , so $P(\sigma)$ is a constant and we can simplify further:

$$A(\sigma \to \sigma'|\mathcal{D}) = \min\{1, \frac{P(\mathcal{D}|\sigma')}{P(\mathcal{D}|\sigma)}\}$$

This is the acceptance probability for a given proposal σ' . The expression for $P(\mathcal{D}|\sigma)$ is $P(e_1, e_2, ..., e_n|\sigma)$ described in the previous part.

(d) Reporting the current decryption of the first 60 symbols after every 100 iterations:

MH Iteration	
100	er pl losrua= drk po=a bstra=dita lad=n pl -df:a= udba pa no
200	er nl loiruah drw noha bitrahdsta ladhp nl xdymah udba na po
300 400	er nl loiruav srw nova bitravsdta lasvp nl xsymav usba na po er vd dsir,an orw vsna bitranolta daony vd uophan ,oba va ys
500	er c, ,sirdan or. csna bitranolta ,aony c, uophan doba ca ys
700	en ck kyindar on. cyra bitnarolta kaors ck uophar doba ca sy en pk klindar on. plra bitnaroyta kaors pk uochar doba pa sl
800	en p, ,londar in. plra botnariyta ,airs p, fichar diba pa sl en pu ulondar in. plra botnariyta uairs pu fichar diba pa sl
900	en pu ulondar in. plra botnariyta uairs pu fichar diba pa sl
1100	en pl luondar in. pura botnariyta lairs pl fighar diba pa su en pl luondar in. pura cotnarixta lairs pl fighar dica pa su
1200	en pk kuondar inl pura comnarixma kairs pk fighar dica pa su
1300	en ck kuondar inl cura pomnarixma kairs ck fighar dipa ca su en ck koundar inl cora pumnarixma kairs ck fighar dipa ca so
1500	en ck koundar inl cora vumnarixma kairs ck fithar diva ca so
1600 1700	en ck koundar inl cora vumnarixma kairs ck fithar diva ca so
1800	an ck kounder inl core vumnerixme keirs ck fither dive ce so an ck kounler ind core vumnerixme keirs ck fither live ce so
1900	an ck kounler ind core vumnerixme keirs ck fither live ce so
2000	an ck kounler ind core vumnerixme keirs ck fither live ce so an ck kounler ind core vumnerixme keirs ck fither live ce so
2200	an ck kounler ind core vunnerixme keirs ck fither live ce so
2300	an ck kounger ind core vumnerixme keirs ck fither give ce so
2400 2500	an ck kounger ind core vulnerixle keirs ck fither give ce so an mk kounger ind more vulnerixle keirs mk fither give me so
2600	an mk kounger ind more vulneriple keirs mk fither give me so
2700 2800	an mk kounger ind more vulneriple keirs mk fither give me so an mk kounger ind more vulneriple keirs mk fither give me so
2900	an mk kounger ind more vulneriple keirs mk fither give me so
3000 3100	an mk kounger ind more vulneriple keirs mk fither give me so
3200	an mf founger ind more vulneriple feirs mf kither give me so an mf founger ind more vulneriple feirs mf kither give me so
3300	an mf founger ind more vulneriple feirs mf kither give me so
3400 3500	an mf founger ind more vulneriple feirs mf kither give me so an mf founger ind more vulneriple feirs mf kither give me so
3600	an mf founger ind more vulneriple feirs mf kither give me so
3700 3800	an mf founger ind more vulneriple feirs mf kither give me so an mf founger ind more vulneriple feirs mf kither give me so
3900	in mf founger and more vulneraple fears mf kather gave me so
4000	in mf founger and more vulneraple fears mf kather gave me so
4100 4200	in mf founger and more vulneraple fears mf kather gave me so in mf founger and more vulnerable fears mf kather gave me so
4300	in mf founger and more vulnerable fears mf kather gave me so
4400 4500	in mf founger and more vulnerable fears mf yather gave me so in mf founger and more vulnerable fears mf yather gave me so
4600	in mf founger and more vulnerable fears mf yather gave me so
4700 4800	in mf founger and more vulnerable fears mf yather gave me so in mf founger and more vulnerable fears mf yather gave me so
4900	in mf founger and more vulnerable fears mf yather gave me so
5000	in mf founger and more vulnerable fears mf yather gave me so
5100 5200	in mf founger and more vulnerable fears mf yather gave me so in mf founger and more vulnerable fears mf yather gave me so
5300	in my younger and more vulnerable years my father gave me so
5400 5500	in my younger and more vulnerable years my father gave me so in my younger and more vulnerable years my father gave me so in my younger and more vulnerable years my father gave me so
5600	in my younger and more vulnerable years my father gave me so
5700 5800	in my younger and more vulnerable years my father gave me so in my younger and more vulnerable years my father gave me so
5900	in my younger and more vulnerable years my father gave me so
6000	in my younger and more vulnerable years my father gave me so in my younger and more vulnerable years my father gave me so
6200	in my younger and more vulnerable years my father gave me so
6300 6400	in my younger and more vulnerable years my father gave me so in my younger and more vulnerable years my father gave me so
6500	in my younger and more vulnerable years my father gave me so in my younger and more vulnerable years my father gave me so
6600	in my younger and more vulnerable years my father gave me so
6700 6800	in my younger and more vulnerable years my father gave me so in my younger and more vulnerable years my father gave me so
6900	in my younger and more vulnerable years my father gave me so
7000 7100	in my younger and more vulnerable years my father gave me so in my younger and more vulnerable years my father gave me so
7200	in my younger and more vulnerable years my father gave me so
7300 7400	in my younger and more vulnerable years my father gave me so
7500	in my younger and more vulnerable years my father gave me so in my younger and more vulnerable years my father gave me so
7600	in my younger and more vulnerable years my father gave me so
7700 7800	in my younger and more vulnerable years my father gave me so in my younger and more vulnerable years my father gave me so
7900	in my younger and more vulnerable years my father gave me so
8000 8100	in my younger and more vulnerable years my father gave me so in my younger and more vulnerable years my father gave me so
8200	in my younger and more vulnerable years my father gave me so
8300 8400	in my younger and more vulnerable years my father gave me so
8500	in my younger and more vulnerable years my father gave me so in my younger and more vulnerable years my father gave me so
8600	in my younger and more vulnerable years my father gave me so
8700 8800	in my younger and more vulnerable years my father gave me so in my younger and more vulnerable years my father gave me so
8900	in my younger and more vulnerable years my father gave me so
9000	in my younger and more vulnerable years my father gave me so
9200	in my younger and more vulnerable years my father gave me so in my younger and more vulnerable years my father gave me so
9300	in my younger and more vulnerable years my father gave me so
9400 9500	in my younger and more vulnerable years my father gave me so in my younger and more vulnerable years my father gave me so
9600	in my younger and more vulnerable years my father gave me so
9700 9800	in my younger and more vulnerable years my father gave me so in my younger and more vulnerable years my father gave me so
9900	in my younger and more vulnerable years my father gave me so
10000	in my younger and more vulnerable years my father gave me so

The corresponding σ :

s	$\sigma(s)$
=	[
space	X
-	h
,	,
;	1
<u>:</u> !	n
?	r e
	f
/	b
;	3
double quotes	5
(4
)	9
ĺ	i
i	0
*	1
0	z
1	m
2	С
3	/
4	;
5	
6	*
7	k
8	:
9	q
a)
b	2 - 7
c	
d	7
e	
f	0
g	s !
h i]
j	(
k	8
1	у
m	v
n	d
0	=
P	space
q	6
r	g
S	t
t	double quotes
u	P
v	j
W	a
х	u
У	?
z	W
	•

To help with chain initialisation, 10000 different σ 's were first randomly and independently sampled. The σ with the best log-likelihood was chosen as the starting point for the MH chain and the algorithm was then run for 10000 iterations. Moreover, ten different trials of this was performed, where the trial with the best log-likelihood was displayed. The decrypted message for each of the ten trials:

Trial	Decryption
-0	itedcecoutl featpedof eyunt fa.n ec afredcevas, felay ed ero
1	in my younger and more vulnerable years my father gave me so
2	in cy yomnker and core vmlnerable years cy father kave ce so
- 3	is hy ytoswer asd htre volseraule yearm hy fanger wave he mt
4	in my younger and more vulnerable years my father gave me so
5	"5407""0""][4)81094307]180(['4819*'80""891207""0:96=810)9(807802]"
6	"542)(2(]94""18234=2)]812:9'4183*'12(13862)(2[307182""3:12)126]"
7	ioadcaclyon earowadle agy.o erk. ac retadcafrsu eanrg ad atl
- 8	in my younker and more vulnerable years my father kave me so
- 0	in my younker and more vulnerable years my father lave me so

The Python code for the MH sampler:

```
from typing import Dict, List, Tuple
3
     import numpy as np
import pandas as pd
     from sklearn.preprocessing import normalize
     from src.constants import DEFAULT_SEED
     def _convert_to_scientific_notation(x: float) -> str:
10
           Convert value to string in scientific notation
           :param x: value to convert
:return: string of x in scientific notation
"""
13
14
           return "\{:.1e\}".format(float(x))
19
     class Decrypter:
           \begin{array}{lll} def & \_\_init\_\_(self \;,\; decryption\_dict \colon \; Dict[\,str \;,\; \,str \,]\,) \; -\!\!> \; None \colon \\ \end{array}
20
                Decrypter containing the mapping a symbol to its encrypted symbol : param decryption_dict:
22
24
25
                 self.decryption_dict = decryption_dict
26
           def decrypt(self, encrypted_message: str) -> str:
                Decrypts an encrypted message using the decryption dictionary
30
                 : param\ encrypted\_message:\ the\ encrypted\ message\ to\ decrypt
                 :return: decrypted message
33
34
                return \ "".join([self.decryption\_dict[x] \ for \ x \ in \ encrypted\_message])
35
           def table(self) -> pd.DataFrame:
36
                Generate table containing symbol decryptions :return: pandas table of decryptions """
38
                decrpyter_table = pd.DataFrame(
    self.decryption_dict.items(), columns=["s", "sigma(s)"]
42
                decrpyter_table [decrpyter_table == ""] = "space"
decrpyter_table [decrpyter_table == '"'] = "double quotes"
return decrpyter_table.set_index("s")
44
45
     class Statistics:
           def __init__(
    self ,
50
51
                training_text: str,
symbols: List[str],
invariant_stopping_epsilon: float = 5e-20,
55
56
57
           ) -> None:
                Statistics for text
                :param training_text: training text for calculating transition and invariant probability :param symbols: symbols in the training text :param invariant_stopping_epsilon: stopping condition for constructing the invariant distribution
58
59
60
61
62
                self.training_text = training_text
                 self.symbols = symbols
                self.num.symbols = len(symbols)
self.symbols_dict = self._construct_symbols_dictionary(symbols)
self.transition_matrix = self._construct_transition_matrix(
64
67
                      {\tt training\_text}\ ,\ {\tt self.symbols\_dict}
69
70
71
72
73
74
75
76
                 self.invariant_distribution = self._approximate_invariant_distribution(
                      invariant_stopping_epsilon
                 self.log_transition_matrix = np.log(self.transition_matrix)
                 self.log_invariant_distribution = np.log(self.invariant_distribution)
           def list_of_symbols_for_df(self) -> List[str]:
                Replace certain symbols to prepare for dataframe :return: list of symbols with some replacements ""
                x = self.symbols.copy()
                83
84
                return x
86
           @property
           def transition_table(self) -> pd.DataFrame:
                Generate a table containing transition probabilities :return: transition probabilities
89
91
                df_transitions = pd.DataFrame(
92
                      data=self.transition_matrix
94
                      columns=self.list_of_symbols_for_df,
```

```
95
96
                 df_transitions.index = self.list_of_symbols_for_df
                 return df_transitions.applymap(_convert_to_scientific_notation)
97
98
aa
           def invariant_distribution_table(self) -> pd.DataFrame:
100
                Generate a table containing invariant distribution probabilities return: invariant distribution probabilities
104
                df =
                     pd . DataFrame (
106
                           data = self.invariant_distribution.reshape(1, -1),
107
108
                           columns = self.list_of_symbols_for_df,
                      .applymap(_convert_to_scientific_notation)
110
                      .transpose()
                      .reset_index()
                df.columns = ["Symbol", "Probability"]
return df.set_index("Symbol")
114
           @staticmethod
           \label{lem:def_construct_symbols_dictionary(symbols: List[str]) -> Dict[str, int]:} \\
                 Construct a dictionary mapping each symbol to an integer to index the transition matrix
                and the invariant distribution :param symbols: list of symbols to map :return: symbol to integer mapping """
124
                return \ \{k \colon \ v \ for \ v \,, \ k \ in \ enumerate (\, symbols \,) \,\}
126
           def _construct_transition_matrix(
           self, text: str, symbols_dict: Dict[str, int]
128
130
                Constructs the transition matrix for a given text :param text: string to calculate transition matrix with
                 :param symbols_dict: dictionary mapping symbol to a dictionary
134
                :return:
                # initialise with ones to ensure ergodicity
transition_matrix = np.ones((self.num_symbols, self.num_symbols))
for i in range(1, len(text));
136
138
                140
142
144
                \textcolor{return}{\texttt{return}} \hspace{0.2cm} \texttt{transition\_matrix}
145
           def _approximate_invariant_distribution (
147
                self, invariant_stopping_epsilon: float
148
           ) -> np.ndarray:
                Approximate the invariant distribution with the power method :param invariant_stopping_epsilon: stopping condition for constructing the invariant distribution :return: the invariant distribution as a vector (number of symbols, 1)
150
154
                {\tt invariant\_distribution} \ = \ {\tt np.zeros} \, (\, (\, {\tt self.num\_symbols} \, , \ 1) \, )
                previous_invariant_distribution = invariant_distribution.copy()
156
                # make sure it's a proper distribution that sums to one
158
                invariant_distribution [0] = 1
                while (
    np.linalg.norm(invariant_distribution - previous_invariant_distribution)
161
                     > invariant_stopping_epsilon
163
                      previous_invariant_distribution = invariant_distribution.copy()
164
                invariant_distribution = self.transition_matrix @ invariant_distribution return invariant_distribution
165
166
168
           def log_transition_probability(self, alpha: str, beta: str) -> float:
169
                Look up the log probability of the transition from symbol alpha to beta :param alpha: symbol that is being transitioned from :param beta: symbol that is being transitioned to :return: probability of transition """
172
                return self.log_transition_matrix[
    self.symbols_dict[beta], self.symbols_dict[alpha]
176
178
179
           def log_invariant_probability(self, gamma: str) -> float:
180
                Look up the log probability of a symbol with respect to the invariant distribution
181
                :param gamma: symbol to query
:return: log probability of the symbol
182
183
184
185
                return self.log_invariant_distribution[self.symbols_dict[gamma]].item()
186
           def compute_log_probability(self, text: str) -> float:
187
                Compute the log probability of a given text containing symbols
189
                :param text: text to compute log probability for
190
```

```
191
                   :return: log probability of the text
192
                   \begin{split} \log_{\texttt{probability}} &= \texttt{self.log\_invariant\_probability} \, (\texttt{text} \, [0]) \\ \text{for } i & \text{in } \texttt{range} \, (1, \, \, \texttt{len} \, (\texttt{text})) \colon \\ & \text{log\_probability} \, +\! = \, \texttt{self.log\_transition\_probability} \, (\texttt{text} \, [\, i \, ] \, , \, \, \texttt{text} \, [\, i \, - \, 1]) \end{split}
194
195
                   return log_probability
196
197
198
       class MetropolisHastingsDecryption:
    def __init__(self , symbols: List[str]):
    """
199
200
201
                   Metropolis Hastings MCMC for Decryption :param symbols: set of symbols to decrypt
202
203
204
205
                   self.symbols = symbols
206
207
             def generate_random_decrypter(self) -> Decrypter:
208
209
                   Generates a random decrypter
                   :return: a Decrypter instantiation
210
212
                   return Decrypter (
213
                                self.symbols[i]: self.symbols[x]
                                for i, x in enumerate
                                     np.random.permutation(np.arange(len(self.symbols)))
216
218
219
                   )
220
             @staticmethod
             \begin{array}{ll} \textbf{def} & \texttt{generate\_proposal\_decryption} \, (\, \texttt{decrypter} \, \colon \, \, \texttt{Decrypter} \, ) \, \, \, \to \, \, \texttt{Decrypter} \, : \\ \end{array}
222
223
                   Generate a proposal decrypter by randomly swapping two of the decryption mappings : param decrypter: the decrypter used to generate the proposal
224
                    :return: a proposal decrypter
226
                   x1 = np.random.choice(list(decrypter.decryption_dict.keys()))
                   x2 = np.random.choice(list(decrypter.decryption_dict.keys()))
proposal_decryption = decrypter.decryption_dict.copy()
proposal_decryption[x2], proposal_decryption[x1] = (
230
                          decrypter.decryption_dict[x1], decrypter.decryption_dict[x2],
233
234
                    return Decrypter (proposal_decryption)
236
237
              @staticmethod
             def _choose_decrypter(
    statistics: Statistics,
238
                    encrypted_message: str,
current_decrypter: Decrypter,
240
241
                   proposal_decrypter: Decrypter,
243
             ) -> Decrypter:
244
                   Choose between the current and proposal decrypter
                   :param statistics: Statistics instantiation for calculating log probabilities :param encrypted_message: the encrypted message
246
248
                    :param current_decrypter: the current decrypter
249
                    :param proposal_decrypter: the proposal decrypter
                   :return:
251
                   # calculate log probabilities
current_log_probability = statistics.compute_log_probability(
254
                         text=current_decrypter.decrypt(encrypted_message),
                   proposal_log_probability = statistics.compute_log_probability(
    text=proposal_decrypter.decrypt(encrypted_message),
257
258
                   )
                   # calculate acceptance probability
acceptance_probability = np.min(
260
261
262
                          [1, np.exp(proposal_log_probability - current_log_probability)]
263
264
                   # choose decrypter using the acceptance probability
                   return np.random.choice(
265
                         [current_decrypter, proposal_decrypter],
p=[1 - acceptance_probability, acceptance_probability],
266
268
269
              def _find_good_starting_decrypter(
271
                   self, statistics: Statistics,
                    encrypted_message: str
274
                   number\_start\_attempts: int,
             ) -> Decrypter:
276
                   Find a good starting decrypter for the sampler by choosing the one with the best log likelihood :param statistics: Statistics instantiation for calculating log probabilities
277
                   :param number_start.attempts: number of possible starting decrypters to check :return: the best starting decrypter for the sampler
279
280
282
                    best_log_likelihood = -np.float("inf")
283
                    best_decrypter = None
285
                    for _ in range(number_start_attempts):
                          decrypter = self.generate_random_decrypter()
286
```

```
288
                               statistics.compute_log_probability(
                                    text=decrypter.decrypt(encrypted_message)
289
290
291
                              > best_log_likelihood
292
                        ):
293
                              best_decrypter = decrypter
204
                  return best_decrypter
295
             def run (
297
                   self,
                   encrypted_message: str.
298
                   statistics: Statistics,
299
300
                   number_of_mh_loops: int
                   number_start_attempts: int,
301
302
                   log_decryption_interval: int,
303
             log_decryption_size: int ,
) -> Tuple[Decrypter , List[str]]:
304
305
                  Run the sampler with two steps:
306
                        1. find a good starting decrypter for the sampler 2. run the sampler
307
308
                   :param encrypted_message: the encrypted message
                  :param encrypted_message: the encrypted message
:param statistics: Statistics instantiation for calculating log probabilities
:param number_of_mh_loops: number of loops to run the metropolis hastings sampler
:param number_start_attempts: number of possible starting decrypters to check
:param log_decryption_interval: number of samples between logging the decrypted message
:param log_decryption_size: number of symbols to decrypt when logging the decrypted message
:return: a tuple containing the decrypter found from the sampler and the logged decryption message
"""
309
310
311
312
314
315
317
                  decrypter = self._find_good_starting_decrypter(
    statistics, encrypted_message, number_start_attempts
318
319
                  logged_decryption_message = [
    decrypter.decrypt(encrypted_message)[:log_decryption_size]
320
321
322
                   for i in range(1, number_of_mh_loops + 1):
    if (i + 1) % log_decryption_interval == 0:
323
                              logged_decryption_message.append(
    decrypter.decrypt(encrypted_message)[:log_decryption_size]
325
326
                         proposal_decrypter = self.generate_proposal_decryption(decrypter)
decrypter = self._choose_decrypter(
328
329
330
                             statistics, encrypted_message, decrypter, proposal_decrypter
331
332
                  return decrypter, logged_decryption_message
333
334
335
       def _construct_decryptions_table(
336
            decryption_messages: List[str], decryption_interval: int, columns: List[str]
       ) -> pd.DataFrame:
337
             decrypted_message_iterations_table = pd.DataFrame(
339
                         np.arange(0, len(decryption_messages)) * decryption_interval,
340
                         decryption_messages ,
342
343
             ).transpose()
             decrypted_message_iterations_table.columns = columns
344
345
             return decrypted_message_iterations_table.set_index(columns[0])
347
348
       def a(
             symbols: List[str],
             training_text: str,
transition_matrix_path: str,
350
351
             invariant_distribution_path: str ,
353
       ) -> None:
354
             Produces answers for question 5a
            :param symbols: symbols in the training text
:param training.text: training text for calculating transition and invariant probability
:param transition_matrix_path: path to store transition matrix
:param invariant_distribution_path: path to store invariant distribution
356
357
358
359
             :return:
360
361
             statistics = Statistics (
362
                  training_text ,
364
                  symbols,
365
366
             statistics.transition_table.to_csv(transition_matrix_path)
367
             statistics.invariant_distribution_table.to_csv(invariant_distribution_path, sep="|")
368
369
370
       def d(
371
             encrypted_message: str,
             symbols: List[str],
             training_text: str ,
number_trials: int ,
374
             number_of_mh_loops: int ,
             number_start_attempts: int
             log_decryption_interval: int,
378
             log_decryption_size: int,
             trial_decryptions_table_path: str,
379
             decryptor_table_path: str
381
             decrypted_message_iterations_table_path: str,
382
      ) -> None:
```

```
383
384
              Produces answers for question 5d
             Produces answers for question 5d
:param encrypted_message: the encrypted message
:param symbols: symbols in the training text
:param training_text: training text for calculating transition and invariant probability
:param number_trials: number of times to restart and run the sampler
:param number_of_mh_loops: number of loops to run the metropolis hastings sampler
:param number_start_attempts: number of possible starting decrypters to check
:param log_decryption_interval: number of samples between logging the decrypted message
:param log_decryption_size: number of symbols to decrypt when logging the decrypted message
:param trial_decryptions_table_path: path to store decryption messages for each trial
:param decrypted_message_iterations_table_path: path to store logged decryption messages
:return:
385
386
387
388
389
390
391
303
394
395
              :return:
396
397
398
              statistics = Statistics (
399
                    training_text ,
400
                    symbols,
401
              np.random.seed (DEFAULT_SEED)
402
403
              metropolis_hastings_decryption = MetropolisHastingsDecryption(symbols)
              decrypters: List[Decrypter] = []
log_likelihoods: List[float] = []
logged_decryption_messages: List[List[str]] = []
404
405
406
              407
408
409
410
411
412
                           number_of_mh_loops,
413
                           number_start_attempts ,
log_decryption_interval ,
414
415
                           log_decryption_size,
416
                     decrypters.append(decrypter)
                     log_likelihoods.append(
418
                           statistics.compute_log_probability(decrypter.decrypt(encrypted_message))
419
420
                     logged_decryption_messages.append(logged_decryption_message)decryption_messages.append(
421
422
                           decrypter.decrypt(encrypted_message)[:log_decryption_size]
424
              df_trial_decryptions = _construct_decryptions_table(
425
                    decryption.messages=[x[:log_decryption_size] for x in decryption_messages], decryption_interval=1, columns=["Trial", "Decryption"],
426
427
428
429
              df_trial_decryptions.to_csv(trial_decryptions_table_path, sep="|")
430
431
432
              # sort trials by log likelihood
              433
435
437
                     decryption_interval=log_decryption_interval
438
                    columns=["MH Iteration",
                                                            "Current Decryption"],
439
              df_logged_decryptions.to_csv(decrypted_message_iterations_table_path, sep="|")
440
```

src/solutions/q5.py

- (e) When some values of $\Psi(\alpha, \beta) = 0$, this affects the ergodicity of the chain. An ergodic chain is one that is irreducible (i.e. all possible transitions between symbols, including to itself, have probability greater than zero). If $\Psi(\alpha, \beta) = 0$, this means that there is zero probability that β will transition to α , breaking our definition. To restore ergodicity, we can add a small transition probability between all symbols of the chain. This essentially acts as a prior, stating that the probability of a symbol to transition to any other symbol (including itself) should never be zero.
- (f) If we were to use symbol probabilities alone for decoding, the joint probability would be:

$$P(e_1, e_2, ..., e_n | \sigma) = \prod_{i=1}^n P(\sigma^{-1}(e_i))$$

the product of the likelihoods of the decoded letters. In this case, the optimal decoding would simply replace the most frequent symbols in the encrypted message with the most frequent symbols in the training text. This decoding approach is much more difficult because each letter is assumed to be independent of its neighbours. For a first order Markov chain, we exploit the structure of language by considering pairs of letters. Assuming that as the training text size approaches infinity and the size of the encrypted message also approaches infinity, that the two will have the same symbol frequency and that the probability of each symbol is unique, (i.e. two different symbols can't have the same frequency), then using symbol probabilities alone should theoretically work by matching symbol probabilities. However, in practise it would be unlikely to be able to make these assumptions about symbol frequencies, especially with the finite size of our training set and encrypted message.

A second-order chain should also work in theory. However, with this approach it is probably practically more difficult for finding a suitable decoding. This is because our transition tensor would contain N^3 elements, where N is the number of symbols, to account for all possible second order transitions. Our training text would need to increase quadratically to maintain the same ratio of possible transitions to example transitions (number of first order transitions in a text of length N is N-1 and second order its N-2). This can also introduce sparsity (as in small non-zero probabilities in many entries) in our transition matrix despite our ability to maintain ergodicity with small probabilities to prevent non-zero entries. However, the log-likelihood of many areas of σ space might be very small or all just the same, when all the transition probabilities are just the offset probability (added to maintain ergodicity). Navigating this space will be much more difficult for the sampler as the space could be relatively flat.

For an encryption scheme where two symbols map to the same encrypted value:

$$\exists \alpha, \beta, \sigma(\alpha) = \sigma(\beta), \alpha \neq \beta$$

this approach can become much more complicated. Our σ is no longer as easily inverted and therefore for each duplicate mapping, we would have to integrate out the probability for the two possible decrypted symbols when computing the log-likelihood. Moreover, generating proposal encodings is not as simple as swapping the encryption for two symbols. This is because we do not know which two symbols map to the same encrypted symbol and simply swapping would preserve the same collision mapping of the current encoding. Moreover, the number of proposal σ' 's will depend on how many duplicates exist in the current σ .

Thus $S(\sigma \to \sigma')$ would no longer be symmetric, complicating the acceptance probability calculation as it would be dependent on the σ and σ' . Overall, this approach could work but would require many changes to accommodate for these complications. Integrating out collision mappings in the log-likelihood, non-symmetric proposal probabilities, and a much larger σ space because duplicates are allowed, means that it will take much longer for the sampler to find a reasonable σ .

If we used this approach for Chinese with ≥ 10000 symbols, we would be attempting to solve the same problem but with $N \geq 10000$ instead of N=53. Similar to the second order Markov chain, although this is theoretically possible, it would require a transition matrix of size $\geq 10000^2$ which is quite impractical and we'd run into similar problems as for second order Markov Chains. An alternative set up could be with using Chinese phonetics, for which there are much fewer than 10000, however this would require a mapping from a phonetic to an encrypted phonetic.

Question 7

(a) To find the local extrema of the function f(x,y) = x+2y subject to the constraint $y^2+xy=1$, first we define g(x,y):

$$g(x,y) = y^2 + xy - 1$$

where g(x,y) = 0 is an equivalent representation of the given constraint.

We can therefore construct the optimisation problem:

$$\min_{\mathbf{x}} f(\mathbf{x})$$

such that $g(\mathbf{x}) = 0$ and $\mathbf{x} := [x, y]^T$.

We can calculate $\nabla f(\mathbf{x})$:

$$\nabla f(\mathbf{x}) = \left[\frac{\partial}{\partial x}(x+2y), \frac{\partial}{\partial y}(x+2y)\right]^T$$

$$\nabla f(\mathbf{x}) = [1, 2]^T$$

and calculating $\nabla g(\mathbf{x})$:

$$\nabla g(\mathbf{x}) = \left[\frac{\partial}{\partial x}(y^2 + xy - 1), \frac{\partial}{\partial y}(y^2 + xy - 1)\right]^T$$

$$\nabla g(\mathbf{x}) = [y, 2y + x]^T$$

Solving the constraint optimisation problem with Lagrange multipliers, we set up the equations:

$$\nabla f(\mathbf{x}) + \lambda \nabla g(\mathbf{x}) = \mathbf{0}$$

and

$$g(\mathbf{x}) = 0$$

Giving us the three equations:

$$1 + \lambda y = 0$$

$$2 + \lambda(2y + x) = 0$$

$$y^2 + xy - 1 = 0$$

Substituting $y = \frac{-1}{\lambda}$ from the first equation into the second equation:

$$2 + \lambda(2(\frac{-1}{\lambda}) + x) = 0$$

$$x = 0$$

Solving for y in our third equation with x = 0:

$$y^2 - 1 = 0$$

We see that $y = \pm 1$ and from the first equation $\lambda \mp 1$.

The local extrema are (x=0,y=1) when $\lambda=-1$ and (x=0,y=-1) when $\lambda=1$.

(b)

(i) Given that $g(a) = \ln(a)$, we want to transform this to the form f(x, a) = 0 where x = g(a):

$$x = \ln(a)$$
$$\exp(x) - a = 0$$

Thus,

$$f(x,a) = \exp(x) - a$$

(ii) We know that for Newton's method's

$$x_{n+1} = x_n - \frac{f(x_n)}{f'(x_n)}$$

where $f(x_n) = \exp(x_n) - a$

We can calculate:

$$f'(x) = \frac{\partial f(x, a)}{\partial x} = \exp(x)$$

Assuming we can evaluate $\exp(x)$, our update equation is:

$$x_{n+1} = x_n - \frac{\exp(x_n) - a}{\exp(x_n)}$$

Simplifying:

$$x_{n+1} = x_n + \frac{a}{\exp(x_n)} - 1$$

we have our update equation in Newton's algorithm for this problem.

Question 8

(a) For:

$$\sup_{\{\mathbf{X}\in\mathbb{R}^n\}}R_A(\mathbf{x})$$

where $R_A(\mathbf{x}) = \frac{\mathbf{x}^T \mathbf{A} \mathbf{x}}{\|\mathbf{x}\|^2}$, we want to show that a maximum is attained.

To do this, we will first show that the above optimisation can be equivalently formulated as:

$$\sup_{\left\{\mathbf{x}\in\mathbb{R}^n\big|\,\|\mathbf{x}\|=1\right\}}R_A(\mathbf{x})$$

We begin by considering any $\mathbf{w} \in \mathbb{R}^n$ and let $\mathbf{x} = \frac{\mathbf{w}}{\|\mathbf{w}\|}$. Because $\|\mathbf{x}\| = 1$ we can substitute:

$$\sup_{\left\{\mathbf{X}\in\mathbb{R}^{n}\big|\|\mathbf{X}\|=1\right\}}R_{A}(\mathbf{x}) = \sup_{\left\{\frac{\mathbf{W}}{\|\mathbf{W}\|}\in\mathbb{R}^{n}\big|\|\frac{\mathbf{W}}{\|\mathbf{W}\|}\|=1\right\}} \frac{\mathbf{w}^{T}\mathbf{A}\mathbf{w}\|\mathbf{w}\|^{2}}{\|\mathbf{w}\|^{2}\mathbf{w}^{T}\mathbf{w}}$$

where $\|\mathbf{x}\|^2 = \mathbf{x}^T \mathbf{x}$.

The set $\left\{\frac{\mathbf{w}}{\|\mathbf{w}\|} \in \mathbb{R}^n \mid \|\frac{\mathbf{w}}{\|\mathbf{w}\|}\| = 1\right\}$ contains all $\mathbf{w} \in \mathbb{R}^n$ so we can rewrite:

$$\sup_{\left\{\mathbf{x} \in \mathbb{R}^n \mid \|\mathbf{x}\| = 1\right\}} R_A(\mathbf{x}) = \sup_{\left\{\mathbf{w} \in \mathbb{R}^n\right\}} \frac{\mathbf{w}^T \mathbf{A} \mathbf{w} \|\mathbf{w}\|^2}{\|\mathbf{w}\|^2 \mathbf{w}^T \mathbf{w}}$$

We can simplify the expression:

$$\sup_{\left\{\mathbf{x} \in \mathbb{R}^n \middle| \|\mathbf{x}\| = 1\right\}} R_A(\mathbf{x}) = \sup_{\left\{\mathbf{w} \in \mathbb{R}^n\right\}} \frac{\mathbf{w}^T \mathbf{A} \mathbf{w}}{\mathbf{w}^T \mathbf{w}}$$

$$\sup_{\left\{\mathbf{x}\in\mathbb{R}^n\big|\|\mathbf{x}\|=1\right\}}R_A(\mathbf{x})=\sup_{\left\{\mathbf{w}\in\mathbb{R}^n\right\}}R_A(\mathbf{w})$$

and recover our original optimisation problem by letting $\mathbf{x} = \mathbf{w}$, showing that it is equivalent to the supremum over the unit sphere. Assuming the set containing the unit sphere is compact, the extreme value theory of calculus states that $\sup_{\{\mathbf{X} \in \mathbb{R}^n | \|\mathbf{X}\| = 1\}} R_A(\mathbf{x})$ is attained so equivalently $\sup_{\{\mathbf{X} \in \mathbb{R}^n\}} R_A(\mathbf{x})$ is attained as required.

(b) We can now reformulate the optimisation as:

$$\sup_{\left\{\mathbf{X} \in \mathbb{R}^n \middle| \|\mathbf{X}\| = 1\right\}} \frac{\mathbf{x}^T \mathbf{A} \mathbf{x}}{\|\mathbf{x}\|^2}$$

Because $\|\mathbf{x}\| = 1$, we can equivalently write:

$$\sup_{\left\{\mathbf{X} \in \mathbb{R}^n \middle| \|\mathbf{X}\| = 1\right\}} \mathbf{x}^T \mathbf{A} \mathbf{x}$$

Thus, showing $R_A(\mathbf{x}) \leq \lambda_1$ will be equivalent to showing $\mathbf{x}^T \mathbf{A} \mathbf{x} \leq \lambda_1$ for $||\mathbf{x}|| = 1$. We know that for all $\mathbf{x} \in \mathbb{R}^n$:

$$\mathbf{x} = \sum_{i=1}^{n} (\xi_i^T \mathbf{x}) \xi_i$$

so we can write:

$$\mathbf{x}^T \mathbf{A} \mathbf{x} = \Big(\sum_{i=1}^n (\xi_i^T \mathbf{x}) \xi_i^T \Big) \mathbf{A} \Big(\sum_{i=1}^n (\xi_i^T \mathbf{x}) \xi_i \Big)$$

Given that ξ_i are eigenvectors of **A** corresponding to eigenvalues λ_i :

$$\mathbf{x}^T \mathbf{A} \mathbf{x} = \left(\sum_{i=1}^n (\xi_i^T \mathbf{x}) \xi_i^T \right) \left(\sum_{i=1}^n \lambda_i (\xi_i^T \mathbf{x}) \xi_i \right)$$

Given that the eigenvectors ξ_i form an orthonormal basis, we know that $\xi_i^T \xi_j = 0$ when $i \neq j$ and $\xi_i^T \xi_j = 1$ when i = j, so:

$$\mathbf{x}^T \mathbf{A} \mathbf{x} = \sum_{i=1}^n \lambda_i (\xi_i^T \mathbf{x})^2$$

From our above reformulation with the unit sphere, we know that $\|\mathbf{x}\|^2 = 1$ so $\|\mathbf{x}\|^2 = \sum_{j=1}^n x_i^2 = \sum_{j=1}^n (\xi_j \mathbf{x})^2 = 1$. Thus the quantity $\sum_{i=1}^n \lambda_i (\xi_i^T \mathbf{x})^2$ is a weighted average of λ_i 's, which is always less than or equal to the largest λ_i value so:

$$\mathbf{x}^T \mathbf{A} \mathbf{x} = \sum_{i=1}^n \lambda_i (\xi_i^T \mathbf{x})^2 \le \lambda_1$$

where λ_1 is the largest eigenvalue of eigenvalues λ_i . Therefore, $R_A(\mathbf{x}) \leq \lambda_1$ as required.

(c) Given that $\mathbf{x} \in span\{\xi_{k+1},...,\xi_n\}$, we can rewrite \mathbf{x} :

$$\mathbf{x} = \sum_{i=k+1}^{n} (\xi_i^T \mathbf{x}) \xi_i$$

Using the same argument as in (b) we can bound $\mathbf{x}^T \mathbf{A} \mathbf{x}$:

$$\mathbf{x}^T \mathbf{A} \mathbf{x} = \sum_{i=k+1}^n \lambda_i (\xi_i^T \mathbf{x})^2 \le \max \{\lambda_{k+1}, ..., \lambda_n\}$$

But given that the maximum eigenvalue λ_1 is not contained in $\{\lambda_{k+1},...,\lambda_n\}$:

$$\max\{\lambda_{k+1},...,\lambda_n\} < \lambda_1$$

and therefore $R_A(\mathbf{x}) < \lambda_1$ as required.

Appendix 1: constants.py

```
import os

DATA_FOLDER = "data"

BINARY_DIGITS_FILE_PATH = os.path.join(DATA_FOLDER, "binarydigits.txt")

MESSAGE_FILE_PATH = os.path.join(DATA_FOLDER, "message.txt")

SYMBOLS_FILE_PATH = os.path.join(DATA_FOLDER, "symbols.txt")

TRAINING_TEXT_FILE_PATH = os.path.join(DATA_FOLDER, "war_and_peace.txt")

OUTPUTS_FOLDER = "outputs"

DEFAULT_SEED = 0
```

src/constants.py

Appendix 2: main.py

```
import os
 3
       import numpy as np
       from src.constants import (
   BINARY_DIGITS_FILE_PATH,
   MESSAGE_FILE_PATH,
               OUTPUTS_FOLDER,
              SYMBOLS_FILE_PATH
              TRAINING_TEXT_FILE_PATH,
12
13
       from src.solutions import q1, q2, q3, q5
       if __name__ == "_
                                       _main__
              if not os.path.exists(OUTPUTS_FOLDER):
    os.makedirs(OUTPUTS_FOLDER)
16
17
18
              x = np.loadtxt(BINARY_DIGITS_FILE_PATH)
19
              os.makedirs(Q1_OUTPUT_FOLDER):

os.makedirs(Q1_OUTPUT_FOLDER):
20
21
23
24
                      figure_path=os.path.join(Q1_OUTPUT_FOLDER, "q1d.png"), figure_title="Q1d: Maximum Likelihood Estimate",
26
29
30
                      alpha=3,
31
                      figure_path=os.path.join(Q1_OUTPUT_FOLDER, "q1e"), figure_title="Q1e: Maximum A Prior",
34
35
              os.makedirs(Q2.OUTPUT_FOLDER) os.makedirs(Q2.OUTPUT_FOLDER)
37
38
              \tt q2.c(x,\ table\_path=os.path.join(Q2\_OUTPUT\_FOLDER,\ "q2c.csv"))
40
41
              # Question 5
Q3_OUTPUT_FOLDER = os.path.join(OUTPUTS_FOLDER, "q3")
if not os.path.exists(Q3_OUTPUT_FOLDER):
    os.makedirs(Q3_OUTPUT_FOLDER)
43
44
46
47
48
                      alpha_parameter=2,
49
                     beta_parameter=2,
number_of_trials=4
50
51
52
                      ks = [2, 3, 4, 7, 10],

epsilon = 1e-1,
                      max_number_of_steps=int(1e2)
                      \label{eq:continuous}  figure\_path=os.path.join\left(Q3\_OUTPUT\_FOLDER,\ "q3e"\right), \\  figure\_title="Q3e",
54
56
57
58
              of os.path.exists (Q5_OUTPUT_FOLDER, "q5")
if not os.path.exists (Q5_OUTPUT_FOLDER):
    os.makedirs (Q5_OUTPUT_FOLDER)
60
              with open(TRAINING-TEXT-FILE_PATH) as fp:
training.text = fp.read().replace("\n", "").lower()
with open(SYMBOLS-FILE_PATH) as fp:
symbols = fp.read().split("\n")
with open(MESSAGE_FILE_PATH) as fp:
66
                      encrypted_message = fp.read()
68
              q5.a(
69
                     symbols,
70
71
                      transition\_matrix\_path = os.path.join (Q5\_OUTPUT\_FOLDER, ~~q5a-transition.csv"), invariant\_distribution\_path = os.path.join (Q5\_OUTPUT\_FOLDER, ~~q5a-invariant.csv"), \\
73
74
75
76
77
78
79
              q5.d(
                      encrypted_message,
                      symbols,
                      training_text , number_trials=10,
                      number_of_mh_loops=int(1e4),

number_start_attempts=int(1e4),
80
                      log_decryption_interval=100,
82
                      \label{log_decryption_size} \begin{split} \log_{-\text{decryption_size}} = & 60, \\ \text{trial\_decryptions\_table\_path} = & \text{os.path.join} \left( \text{Q5\_OUTPUT\_FOLDER}, \ "\ \text{q5d-trials.csv"} \right), \end{split}
                      decryptor_table_path=os.path.join(Q5.OUTPUT_FOLDER, "q5d-decrypter.csv"),
decrypted_message_iterations_table_path=os.path.join(
Q5.OUTPUT_FOLDER, "q5d-iterations.csv"
85
```

main.py