Introduction to learning and analysis of big data
Exercise 2

Dr. Sivan Sabato

Fall 2021/2

Submission guidelines. **Please read and follow carefully**:

- The exercise is submitted in pairs.
- Submit via Moodle.
- The submission should include two separate files:
  1. A pdf file that includes your answers to all the questions;
  2. A zip file that includes your submitted code. The zip file should be named "ex2.zip". It should include a copy of the shell python file provided for this exercise in Moodle, with the required functions are implemented by you. **Do not change the name of this file!** In addition, the zip file may include other code files that are used by the shell file.
- The code files should be in the root of the zip archive, **not under a subdirectory**.
- Your python code should follow the course python guidelines (see the Moodle website).
- Resources on coding in python are also available in the Moodle website.
- Before you submit, **make sure that your code works in the course environment**, as explained in the guidelines. Specifically, **make sure that the test `simple_test` provided in the shell file works**.
- You may only use python modules that are explicitly allowed in the exercise or in the guidelines. If you are wondering whether you can use another module, ask a question in the exercise forum. No module containing machine learning algorithms will be allowed.
- For questions, use the exercise forum, or if they are not of public interest, send them via the course requests system.
- Grading: Q1: 15, Q2: 15, Q3: 15, Q4: 15, Q5: 10, Q6: 10, Q7: 20 (5 for (a), 5 for (b), 10 for (c)).

Question 1. Implement the soft-SVM algorithm that we learned in class in Python. The shell file "softsvm.py" is provided for this exercise in Moodle. It contains an empty implementation of the function required below. You should implement it and submit according to the submission instructions.

```
def softsvm(l, trainX, trainy)
```

The input parameters are:

- `l` - the parameter λ of the soft SVM algorithm.
- `trainX` - a 2-D matrix of size $m \times d$, where m is the sample size and d is the dimension of the examples. Row i in this matrix is a vector with d coordinates that describes an example x_i from the training sample.
- `trainy` - a column vector of length m. The i's number in this vector is the label $y_i \in \{-1, 1\}$ from the training sample.

The function returns the linear predictor `w` which is a column vector in $\mathbb{R}^d$.

- You may assume all the input parameters are legal.
- We will use the library `cvxopt` for our Quadratic Program solver.

Instructions for using `cvxopt`:

- First, you will need to define the matrices `H`, `u`, `A`, and `v` which correspond to the vectors and matrices with the same names in the quadratic programming problem you learned in class. Those matrices should be `cvxopt` matrices, check how to create `cvxopt` matrices or convert `numpy` arrays to `cvxopt` matrices here: `http://cvxopt.org/userguide/matrices.html`.
- In order to conserve memory, use sparse matrices when possible.
- Run `sol = cvxopt.solvers.qp(H, u, -A, -v)` to solve the quadratic programming problem. Here, we pass A and v with a minus sign, since this solver assumes the constraints are $Az \leq v$, while in class we assumed they were $Az \geq v$. The solution of the quadratic program is provided in `sol["x"]`.
- See the note at the end of the exercise regarding a possible error and how to solve it.

Question 2. In this question, you will run your soft SVM implementation on data from the MNIST dataset you saw in exercise 1. For this task, we took a subset of this dataset which include and digits 3 and 7, and the goal of the predictor is to distinguish between the two digits. You can load the dataset, which is already divided to train and test, from the file `ex2q2_mnist.npz` on the course website.

Run two experiments on this data set. In the first experiment, use a sample size of 100. To generate this small sample, draw it randomly from the provided training sample. Repeat the "small sample" experiment 10 times, and when you report the results, average over these 10 experiments, and plot also error bars which show the maximum and minimum values you got over all experiments. Run your soft-SVM implementation with each of the following values of λ: $\lambda = 10^n$, for $n \in \{1, \ldots, 10\}$.

In the second experiment, use a sample size of 1000, which you should also draw randomly from the training set. Run your soft-SVM implementation with each of the following values of λ: $\lambda = 10^n$, for $n \in \{1, 3, 5, 8\}$. To make the running time feasible, you should run this experiment only once for each value of λ.

(a) Submit a plot of the training error and test error of the small sample size results as a function of λ (plot λ on a logarithmic scale), with one line for the train error and another line for the test error. Each line should show an average of the 10 experiments, and error bars which show the maximum and minimum values you got over all experiments.

(b) Add to the plot the points describing the training error and test error of the large sample size. For this part, don't draw lines between the points in this case, only show each point individually, since you tested values of λ which are quite far away from each other.

(c) Based on what we learned in class, what would you expect the results to look like? Do the results you got match your expectations? In your answer address the following issues:

- Which sample size should get a smaller training error? What about test error? Do the results match your expectations?
- What should be the trend in the *training error* as a function of λ (decreasing/increasing/other)? Why? Do the results (for the small sample size) match your expectations?
- What should be the trend in the *test error* as a function of λ (decreasing/increasing/other)? Why? Do the results (for the small sample size) match your expectations?

Question 3. Implement the soft-margin kernel SVM routine described in class, using `cvxopt` quadratic problem solver you used in Question 1. The algorithm should use the Gaussian (RBF) kernel. Similar to question 1, you will implement the function `softsvmrbf` in the shell file "softsvmrbf.py" which is provided for this exercise in Moodle. function details:

```
def softsvmbf(l, sigma, trainX, trainy)
```

The input parameters are:

- `l` - the parameter λ of the soft SVM algorithm.
- `sigma` - the bandwidth parameter σ of the RBF kernel.
- `trainX` - a 2-D matrix of size $m \times d$, where m is the sample size and d is the dimension of the examples. Row i gives example $x_i \in \mathbb{R}^d$ from the training sample.
- `trainy` - a column vector of length m . The i's number in this vector is the label $y_i \in \{-1, 1\}$ from the training sample.

The function returns the column vector `alpha` $\in \mathbb{R}^m$ which describes the coefficients found by the algorithm.

Question 4. For this question, use the data file `ex2q4_data.npz` provided on the course website, which contains data points in the domain $\mathcal{X} = \mathbb{R}^2$ and labels in $\{-1, 1\}$, split into a training set and test set.

(a) We would like to use soft SVM to learn a predictor for this problem. Plot the points in the training set in $\mathbb{R}^2$, and color them by their label. Explain why it may be a better idea use kernel soft SVM and not linear soft SVM.

(b) Run your RBF soft SVM code on the training set. Perform 5-fold cross-validation to tune λ and σ. Try the values $\lambda \in \{1, 10, 100\}$ and $\sigma \in \{0.01, 0.5, 1\}$ — a total of 9 parameter pairs to try. Report the 9 average validation error values for each of the pairs (λ, σ). Report which pair was selected by the cross validation, rerun the training using this pair on the entire training set, and report the test error of the resulting classifier.

Repeat the procedure above using the linear (non-kernel) soft SVM code from Q1 on the given training set. In this case, you only need to choose λ since there is no σ parameter.

(c) Which approach (RBF or soft SVM) achieved a better validation error? Is it what you expected? Give one reason general reason why the RBF SVM might get a better validation error, and one reason why it might give a worse validation error, compared to the linear soft SVM approach.

(d) Set $\lambda = 100$ and consider $\sigma \in \{0.01, 0.5, 1\}$. For these values, run the soft-margin RBF SVM on the training set, and plot the resulting predictor in $\mathbb{R}^2$ as follows: Define a fixed region (roughly the region in which the training data resides), divide it into a fine grid, and color the grid points red or blue, depending on the label predicted by the classifier for each point. You can use the the function `matplotlib.pyplot.imshow` to plot this.

(e) Explain the difference between the three plots for the different σ values that you provided above. Base your answer on what we learned in class regarding the effect of σ on the formula of the separator generated by an RBF kernel.

Question 5. For a given training sample $S = ((x_1, y_1), \ldots, (x_m, y_m))$, consider the following **modified version** of the soft-SVM optimization problem:

$$\text{Minimize}_{w \in \mathbb{R}^d} \lambda \|w\|^2 + \sum_{i=1}^{m} \left(\ell^h(w, (x_i, y_i)) \right)^2,$$

where $\ell^h(w, (x_i, y_i)) = \max\{0, 1 - y_i \langle w, x_i \rangle\}$ is the *hinge loss* defined in class.

Express this optimization problem as a quadratic program in the form we learned in class, using the following steps:

(a) Write a minimization problem with constraints that is equivalent to the problem above but uses only a quadratic/linear objective and linear constraints, using auxiliary variables similar to the ξ_i used in the soft-SVM implementation.

(b) Write what H,u,A,v in the definition of a Quadratic Program should be set to so as to solve the minimization problem you wrote above.

Question 6. **The representer theorem.** Consider the following optimization objective, where $\mathcal{X} = \mathbb{R}^d$ and $\mathcal{Y} = \{-1, 1\}$, and we assume that $r \in \mathbb{R}$ is some (not necessarily positive) real value.

$$\text{Minimize}_{w \in \mathbb{R}^d} r\|w\|_2^4 + \sum_{i=1}^{m} \exp^{|\langle w, x_i \rangle - y_i|}$$

Find the **exact** set of values of r such that the Representer Theorem holds for this objective function. Prove that this is indeed the correct set of values.

Question 7. **Kernel functions.** Consider a space of examples $\mathcal{X} = \mathbb{R}^d$. Let $x, x' \in \mathcal{X}$.

(a) Prove that the following function *cannot be* a kernel function for any feature mapping:

$$K(x, x') := -x(1)x'(1).$$

Hint: consider the case of $x = x'$.

(b) Prove that the following function *cannot be* a kernel function for any feature mapping:

$$K(x, x') := (x(1) + x(2))(x'(3) + x'(4)).$$

Hint: what property of inner products does this function violate? How can you prove it?

(c) Convert the Perceptron algorithm to a *kernel-Perceptron* algorithm. This is a version of the Perceptron algorithm that works in the feature space F generated by ψ. Instead of getting the sample points $(x_1, \ldots, x_m)$, it gets as input the Gram matrix G, where $G_{i,j} = K(x_i, x_j) \equiv \langle \psi(x_i), \psi(x_j) \rangle$. In addition, instead of outputting $w \in \mathbb{R}^d$, it outputs $\alpha(1), \ldots, \alpha(m)$ such that $w = \sum_{i=1}^{m} \alpha(i)\psi(x_i)$.

A note on the error:
"`ValueError: Rank(A) < p or Rank([P; A; G]) < n`"
from `covxopt`:
`covxopt` expects the matrix `H` in a quadratic program to be positive definite, that is: to have only non-negative eigenvalues.
However, due to numerical inaccuracies in calculations, when some eigenvalues are very close to zero (though still positive), `covxopt` might think they are negative (e.g. a tiny amount smaller than zero). You can check this by running "`numpy.linalg.eigvals(H)`" (make sure that `H` is a numpy array) and see the eigenvalues of the matrix `H`. If they are very close to zero, either positive or negative, this explains why you are getting this error.
To avoid this issue, if you have it, the solution is to add to the diagonal of the matrix a **small** positive value, let's call it ϵ. If you add ϵ to the diagonal, all the eigenvalues grow by ϵ, so if one of the eigenvalues was too close to zero for python to work with, it will now be a little larger so that python is not confused thinking it's negative. However, adding anything to the matrix might change the result, and if you add a large number to the diagonal it might change the result too much. So the best strategy is to add the smallest value that works, so that on the one hand python doesn't get confused, and on the other hand the results don't change significantly.