Homework 4 – Machine Learning (CS4342, Whitehill, Spring 2021)

1. **Support Vector Machines: Implementation [40 points]**: In this problem you will implement a class called `SVM4342` that supports both training and testing of a linear, hard-margin support vector machine (SVM). In particular, you should flesh out the two methods `fit` and `predict` that have the same API as the other machine learning tools in the `sklearn` package.

   (a) `fit`: Given a matrix $\mathbf{X}$ consisting of n rows (examples) by m columns (features)[1] as well as a vector $\mathbf{y} \in \{-1, 1\}^n$ consisting of labels, optimize the hyperplane normal vector $\mathbf{w}$ and bias term b to maximize the margin between the two classes, subject to the constraints that each data point be on the correct side of the hyperplane (hard-margin SVM). To do so, you should harness an off-the-shelf quadratic programming (QP) solver from the `cvxopt` Python package. The template file already includes code showing how to use it – just pass in the relevant matrices and vectors as `numpy` arrays. The trick is in setting up the variables to encode the SVM **objective** and **constraints** correctly, as described in lecture. Then, store the optimized values in `self.w` and `self.b` because you'll need them later.

   (b) `predict`: Given a matrix $\mathbf{X}$ of test examples, and given the pre-trained `self.w` and `self.b`, compute and return the corresponding test labels.

   Your code will be evaluated based both on the accuracy of the predicted test labels in several tests (you can see the exact test code we'll be running in the template file), as well as the difference between the hyperplane parameters compared to their ideal values.

   Note: as shown in the template, you can calculate the ideal values using the off-the-shelf `sklearn` SVM solver. Note that, since the SVM in this package is, by default, a soft-margin SVM, we have to "force" it to be hard-margin by making the cost penalty C very large.

Submit your Python code in a file called `homework4_WPIUSERNAME1.py`.

[1] To be consistent with the notation I've used in the lecture slides, $\mathbf{X}$ in this assignment would actually need to be called $\mathbf{X}^\top$. The reason I call it $\mathbf{X}$ here is to be consistent with the `sklearn` package.