PA Instruction

DSC 291/190: Trustworthy Machine Learning, SP'25
Instructor: Dr. Lily Weng

Instructions

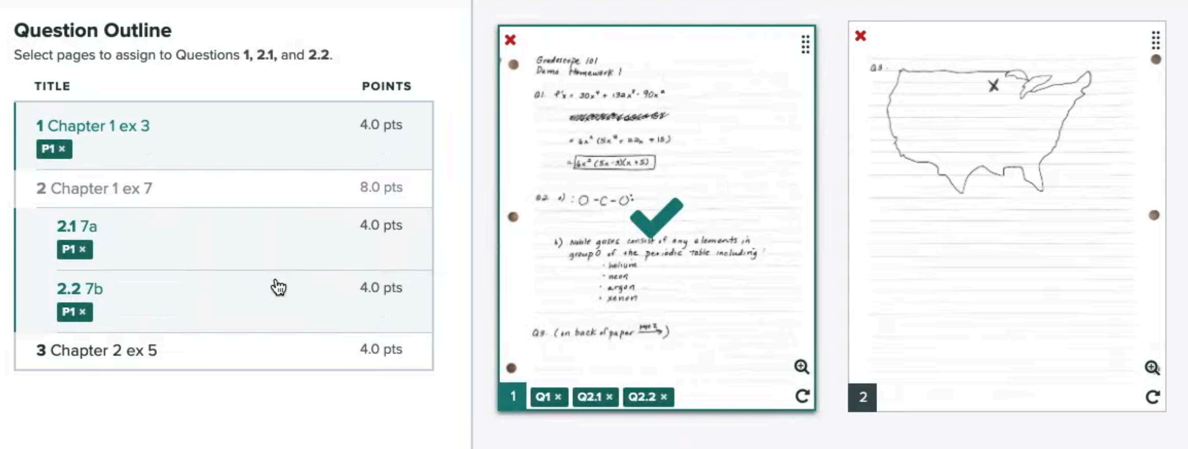
- You should do this PA individually. Collaboration is not allowed.
- The homework has to be submitted on Gradescope before the submission deadline.
- The submission deadline is **Thursday, April 24th, 2025 at 11:59 PM**. Delay per day gives a ***20% penalty***. If we do not receive your submission by **Tuesday, April 29th at 11:59 AM**, it will be graded as 0 pt.

HW Structure:

- This homework consists of 3 parts dealing with ***Vision Model Training and Evaluation***. Each part has its own dedicated Colab notebook which you can find in this zip.
- The 4 parts are as follows:
    1. Basic Vision Models [Experiments with MNIST] (55 points)
    2. Advanced Vision Models [Experiments with CIFAR10] (45 points)
    3. Training a Robust Model (10 points) – **Optional/Bonus**
- The first two parts are mandatory. The third part is for your own learning and is an optional question.
- Further instructions for each of the questions are given in their respective notebooks.

Submission Format:

- For each question:
    - You may choose to either use Colab or download the file as .ipynb and run it on your local machine as a Jupyter notebook.
    - Once you have completed your solutions, save the notebook as a PDF.
        - If using Colab do: Download the notebook from colab as a .ipynb file (File -> Download as -> .ipynb) and use `jupyter nbconvert --to PDF filename.ipynb --output output_filename.pdf` in the terminal.
            - Alternatively, you can open the .ipynb file in Jupyter and follow the next bullet point.
        - If using Jupyter do: *File -> Download as -> PDF via LaTeX*
    - **Make sure all your solutions are displayed in the pdf**. It's okay if the provided questions get cut off.
    - Look at the PDF file and make sure all your solutions are there, displayed correctly. The PDF is the only thing the grader can see.
- Once the PDF files are ready, merge them into one large PDF.
- Submit the final PDF on Gradescope as a group or individually.
    - In Gradescope, assign the pages of the solution pdf to the corresponding question number, as shown in this video tutorial or as shown in the screenshot below.



Question Outline

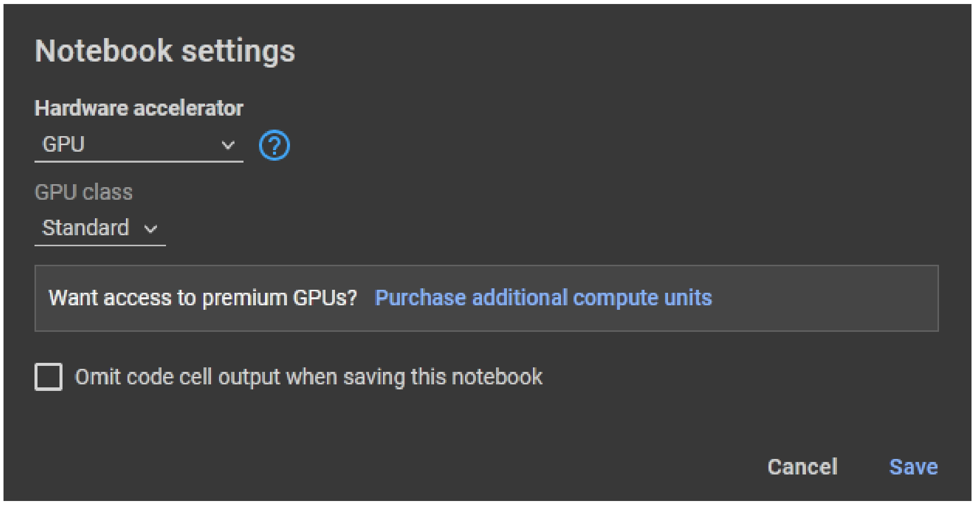
Select pages to assign to Questions **1**, **2.1**, and **2.2**.

TITLE	POINTS
1 Chapter 1 ex 3 P1 ×	4.0 pts
2 Chapter 1 ex 7	8.0 pts
2.1 7a P1 ×	4.0 pts
2.2 7b P1 ×	4.0 pts
3 Chapter 2 ex 5	4.0 pts

- Note that PDF of the solved notebooks is the only submission format. Do not submit python (.py) or notebook (.ipynb) extension files.
    - **Note that we do want you to show your code in the pdf (please don’t collapse the cells in Colab so that we can see and grade them).**

Enable GPU in Colab

- We highly recommend using a GPU in Colab for faster runtimes especially for Parts 2 and 3. To enable a GPU, go to Runtime → Change Runtime Type and select “GPU” in the dropdown list (as shown below) and click “Save”.



Notebook settings

Hardware accelerator: GPU

GPU class: Standard

Want access to premium GPUs? Purchase additional compute units

□ Omit code cell output when saving this notebook

- Note that there is a usage limit per day on Colab, so please test your code first without GPU (selecting “None” in the above dropdown list) and run your final code on GPU.
- Also note that Colab will disconnect the session if there is inactivity in the browser tab.