Bachelor in Data Science and Artificial Intelligence May 2025
Unsupervised Learning
Dr.-Ing. Michael Wand

Midterm Project: Anomaly Detection with the Autoencoder Framework

In this project, you will implement an anomaly detection system using the Autoencoder framework. You will perform the implementation (using what we have developed so far in the lecture and the exercises), you will do parameter tuning and system evaluation, and you will write a short report on your results.

The entire project will be graded and will contribute 25% of the final grade of the course "Unsupervised Learning". Please find all details in the paragraphs below.

The Task:
Please create a dataset for anomaly detection as follows:

- Take the MNIST dataset in the form which has been posted on iCorsi (MNIST.npz).
- Split both training and test data in the following way: 1) all samples corresponding to target "8", 2) all samples corresponding to target 4", 3) all the rest. Now you have 6 datasets (train/8, train/4, train/rest, test/8, test/4, test/rest).
- The data corresponding to targets 8 and 4 is to be considered anomalous, all other data is considered normal. **You cannot use the dataset train/4. You can use the dataset test/4 only for the final evaluation** (see below).

Build an autoencoder using PyTorch (you can use the solutions from the past exercise sessions). The autoencoder can be trained *only* on the dataset train/rest. Evaluate the autoencoder on the datasets test/rest and test/8 (we can call them the *development* datasets), if you did everything right, the reconstruction cost should be higher on the test/8 dataset than on the test/rest dataset. **Use the reconstruction cost as an anomaly score and optimize the quality of the anomality detection.** For evaluation, use any of the measures which were presented in the lecture.

When you have fixed all parameters (e.g. the autoencoder topology, the anomaly threshold), run the system again, testing on the held-out dataset test/4 (the *evaluation* dataset). The result of this step is the key evaluation parameter, and also the key parameter which goes into your final report.

The final report:
Please write a report on your work**,** to be handed in together with the source code. The report should be around 3-4 pages long, and should contain the following sections:

- Introduction (1-2 paragraphs on the task)
- Data and Methods (1-2 paragraphs on the data corpus, including information on how the data was split, some paragraphs on your neural network topology, training, anomaly scoring, parameters which you attempt to optimize)
- Experiments and Results (on the *development* set, e.g. reconstruction accuracy for different NN topologies, tuning the anomaly score, ROC curve, possibly an image of the reconstruction, etc.)
- Evaluation and Conclusion (1-2 paragraphs, final score on the *evaluation* dataset)

Grading, Rules, Instructions:
You can talk about the task to your fellow students, but please do not share your implementation or

your report. Plagiarism in the source code or the report will be penalized with a grade of 0 and might be reported to the faculty.

Submit the source code (as a Python script or an Jupyter Notebook) *and* the report on iCorsi. The deadline is **May 31, 2025, 23:59.**

I will grade your work based on the following scheme, where both items are equally weighted:

- experiments (do your experiments make sense, is data used correctly, are results correctly interpreted)
- report (structure, style, readability, understandability)

I will not grade you on the quality of the Anomaly Detection itself, but it should become clear from the report that you made a reasonable effort to tune the system.

For a passing grade (4), please describe the optimization of **at least one parameter**. For medium grade (5), you should make a discernible effort to obtain a good result, and you should describe your work in a comprehensible manner. For a top grade (6), you should perform a couple of well-structured experiments, and your report should have a good scientific style.

The most important information:
You are *absolutely welcome* to ask questions to me about the system, and it's also OK to talk to your fellows, as long as you do not directly share source code or your reports. In fact, we will dedicate the next exercise sessions to this, and I suggest that you start working on the project as soon as possible, so that we can talk about the implementation in the next week, and about the report in the week before the deadline. I will give you feedback and try to help you to improve your work. But *please* ask, I am here to help!