Machine learning, big data and artificial intelligence – Fall 2019 – Homework 2

INSTRUCTIONS (PLEASE READ CAREFULLY!)

- In this homework you will work with a deep learning project of your choice. Details are given on the next page.
- The work should be carried out in groups of 3 students.
- You must hand in a plan specifying what you will do (in broad terms) and who will do what part of the project.
- You will produce a written report and an oral presentation of your project. Details are given on the pages below.
- The written reports must include a summary of who did what part.
- Your report should be concise and written in such a way that it is perfectly clear what has been done and why. **Do not** directly copy and paste software outputs. Present results using nicely formatted tables and graphs.
- You are **not allowed** to copy answers from other students, or from other sources. You are however allowed to *cite* other sources (e.g. books, webpages). Your report will be checked for plagiarism, both manually and using specialised software. Plagiarism will lead to you failing the course and will be reported to the Disciplinary Board, which may lead to suspension from the university. So **do not copy the work of others**.
- The **deadlines** for the second homework:
  - You should hand in your plan ahead of the seminar at 10.00 on Friday 13 December.
  - You should hand in the report with your solutions before 08.00 Thursday 9 January 2020.
  - You should give your oral presentation on Thursday 9 January 2020.

  The deadlines are strict and extensions will only be granted under exceptional circumstances.

Choosing a topic

The topic that you choose should go beyond what you have done in the seminars, but not be so difficult that three people cannot finish it in 40-60 hours of work. This is a small course project and not a thesis! Please consult the teaching staff to make sure that your project is at an appropriate level.

Five ideas for projects are listed below – feel free to choose one of these or to come up with an idea of your own:

1. **Featues engineering using neural networks.** Fit a neural network to a training set (e.g. some image data). Then extract the features from the network (that is, export the output from the second to last layer of the network, i.e. the data that is passed to the final regression/classification layer) and use these as features for other machine learning methods. That way you can investigate whether you can get even better performance by using the features created by the neural network in e.g. a random forest. Try different datasets and different machine learning methods and compare the results.

2. **Forecasting time series with neural networks.** In the recent M4 competition (`http://rpubs.com/fotpetr/m4competition`), a large number of models for forecasting time series were compared. Included were classic time series models, novel time series models, machine learning models and hybrids between these. The best model (the Smyl model) was a hybrid between classic exponential smoothing and a recurrent neural network. In this project, you will implement and compare some of the methods from the M4 competition (or similar methods) and compare their performance in forecasting different time series (using real data).

3. **Adversarial examples for images.** Pick a computer vision system of your choice (e.g. the VGG16 model used in the *Deep learning with R* book). Create example images that trick the network into misclassifying them, both manually (using Photoshop/GIMP/similar software, see e.g. Fig 1 in `https://arxiv.org/pdf/1711.04451.pdf`) and using a GAN (generative adversarial network, Chapter 8.5. of *Deep learning with R*).

4. **Adversarial examples for other systems.** In addition to computer vision, neural networks are used for many other applications. Examples include interpreting audio data and detecting URL:s that may imply that an email message is spam/fraud. Adversarial examples for these types of applications have not been studied to the same extent as adversarial examples for image data. Create adversarial examples for a neural network used for something that is not computer vision, either manually or using a GAN (generative adversarial network, Chapter 8.5. of *Deep learning with R*).

5. **Overfitting to the test set.** When we fit a large number of models to the same data (comparing different methods, tuning hyperparameters...) we run the

risk of *overfitting to the training data*. Competitions with e.g. the ImageNet data are examples of this. This has been discussed extensively online in recent months (e.g. `https://tinyurl.com/y4mxd5eb`). In this project, you will investigate this phenomenon in detail, using probability theory and simulations.

The written report

The written report should be no more than 6 pages long (excluding appendices), and should contain the following:

- An introduction to the problem that you have studied.
- A description of the methods/models you have used an what you did in the project.
- The results.
- A discussion of the results.
- A description of who did what part of the project.
- Citations to all sources that you used for the project.
- The code that you used (in an appendix, in a `monospaced` font).

Please note that how "good" your results are is uncorrelated with the mark for your report. We are looking for a well-planned project where you use sound methods and present the results clearly.

The oral presentation

The oral presentation should be 10 minutes long. In it, you should present the following (using a Beamer/PowerPoint presentation):

- A short introduction to the problem that you have studied.
- A short description of what you did in the project.
- The results.
- A brief discussion of the results.