TENTALYDELSE EXAM QUESTIONS

Fält med fet text måste fyllas i Boxes with text in bold must be filled out

Kurskod Course code	DD2437
Kursnamn Course name	Artificial Neural Networks and Deep Architectures
Datum Date 20-10-2023	**Tid** Time 14-17
Språk Language	☐ Svenska ☑ English
Ansvarig lärare under tentamen Responsible teacher during the exam	Pawel Herman
Telefonnummer Phone number	0761893012
Tentan ska rättas (välj ett alternativ) The exam should be corrected (choose one option)	☑ i Canvas in Canvas ☐ Manuellt Manually

Antal sidor No. of pages 4	**Antal frågor** No. of questions 6
Betygskriterier Grading	A: >=42, B: [37, 41], C: [32, 36], D: [27, 31], E: [23, 26], F: <23
Tillåtna hjälpmedel - Om det här fältet är tomt så är inga hjälpmedel tillåtna. Endast de hjälpmedel som nämns här är tillåtna. Allowed aids - If this box is empty, no aids are allowed. Only the aids mentioned here are allowed.	You are allowed to use your own paper notes (not electronic) including printouts of your own digital notes (but not full printouts of all the lecture slides). A standard English-other language dictionary is also allowed.
Övrig information Other information	Use a separate sheet for each question. Brief and concrete answers are preferred by all means. Do NOT give several mutually conflicting answers to a question (ingen helgardering). If you do, the alternative with lowest score will be chosen. Please keep in mind that you are obliged to abide by the code of honor at EECS/KTH (https://www.kth.se/en/eecs/utbildning/hederskodex/inledning-1.17237).

Question 1 (11p)

In each case below, what type of problem/processing is this? Propose a neural network approach to address it. For your solution, give algorithm name, network topology, describe input and output (what kind of data, how many nodes etc), how training and model selection is done, what evaluation criteria are used to quantify the performance etc. Please use the following seven headers for your concise answer: I) Problem type (including representation of available data), II) Neural network type, III) Network architecture (inputs, outputs, topology etc.), IV) Training algorithm (including loss function), V) Model selection (here you can list key hyperparameters and briefly describe how you decide on their values, what data is used), VI) Performance evaluation (measure and how it is evaluated, what data is used) and VII) Challenges (please list any particular risks, concerns, potential issues and/or challenges you expect to face when solving the task).

a) In manufacturing it is important to control condition and wear of tools used in production processes. It helps maintain the quality of generated products but also prevents from costly failures and delays on the production line. Typically there are multiple sensor technologies used together with simple measurements made on a regular basis to systematically monitor how the tools are used. This should offer insights into risks underlying premature wear and decay of the tools. In the past, selected variables were particularly tracked and if their values crossed predefined thresholds, a warning signal was issued. This however led to a very high false positive rate of alarms. This was partly due to the fact that rather than readouts from individual sensors one should detect co-occurring patterns of activities reported by multiple sensors and measurements (multivariate patterns). In addition, one could expect that their sequence is a more reliable predictor of the oncoming tool failure (critical wear and decay). Your task is to devise a neural network approach.

b) As machines get more and more complex, mechanisms for self-diagnostics get more important. In an automated factory, a number of parameters (sensor values, data from micro-controller memories, etc) are constantly logged. Over time, the company has saved this data (now about 100000 entries) as well as corresponding labels describing the data. This label is either a collective descriptor ”normal operation” or, in case it was found out that the machine was not working properly, the type of error was saved. Your task is to use this data to construct an automated self-diagnostics system bearing in mind that the clear majority of available data characterise normal operation.

c) As part of multidisciplinary efforts towards self-driving devices there is a need to develop a system that can identify potentially hazardous road scenarios based on visual input obtained through multiple cameras. For that purpose, a convolutional neural network (CNN) based approach has been proposed. However, the availability of training data is limited (these are photos and videos collected in real-world traffic and then annotated with the level of risk for traffic hazard). More data is needed where some new scenarios could be made as various combinations (hybrid) of those available scenarios. Your task is to propose a neural network solution to this training data deficit.

Question 2 (4p)

For a Hopfield network with bipolar {1, -1} nodes and the following weight matrix, **W**:

$$\mathbf{W} = \begin{bmatrix} 0 & -1 & -2 & 3 & 4 \\ -1 & 0 & -1 & -2 & 3 \\ -2 & -1 & 0 & -1 & -2 \\ 3 & -2 & -1 & 0 & -1 \\ 4 & 3 & -2 & -1 & 0 \end{bmatrix}$$

please find two patterns that are fixed-point attractors. Show your synchronous mode calculations to prove that the proposed patterns are fixed points, assuming that the node output is 1 if the net input is greater or equal to 0.

Question 3 (10p)

You are requested by botanists to help them automatically categorise a large volume of deciduous trees based on photos of their leaves (when they fall down during the autumn time). A small subset (up to 5%) of a relatively large pool of available photos of various tree leaves is annotated with the names of the corresponding trees. A larger subset (including those samples that are labelled by tree names) of up to 70% of the available photo pool is annotated with 10 key morphological features such as type of lamina, shape, number of leaflets, regularity of the edge etc. (but not colour).

You should effectively address two main tasks. **First**, propose a neural network approach to automated morphological labelling of the remaining part of the available photos. **Second**, as a follow-up, propose an end-to-end neural network based system for categorising leaves (not for naming their corresponding trees) based on their photos. In this second task bear in mind that *i)* we do not really know how many categories exist and what they represent, *ii)* categorising does not mean any hard grouping (groups could be overlapping), and *iii)* even though there could be new photos taken in the future that represent a new category, it would be valuable to know how different or similar they are to the categories identified before. In handling these **two** tasks, make sure that your answer accounts for the following aspects:

- a simple description of the proposed architecture (please motivate) with key hyperparameters and a suggestion for choosing their values (model selection)
- a brief description of the learning algorithms involved, how would you use (which data partitions) and potentially preprocess the data?
- a list of key problems, challenges and potential risks/issues that you envisage (suggest briefly how they could be handled or how the risks could be minimised, if applicable)
- for the second task, please elaborate on the process of identifying similarities for a hypothetical new input photo (especially if the categories can be considered as overlapping), briefly describe the process starting from feeding input image sample and ending with a form of inference or visualisation about the similarities
- how would you ensure that your approach is robust, e.g. not particularly sensitive to the colour of leaves, their position in the photo or the colour of the photo background?

Question 4 (6p)

Reservoir computing (echo state network, liquid state machine) offers the functionality of processing temporal/sequential data. One of the central components of such networks is reservoir. Explain briefly what it is and describe its key properties that promote good performance in sequence classification tasks. What is meant behind the statement that training echo state networks is fast? What kind of training is it?

What are the fundamental differences in solving the problem of sequence mapping or sequence discrimination between echo state networks and typical (vanilla) recurrent neural networks (RNN) or long short-term memory (LSTM) networks? Also, what functional deficit of standard RNN units do LSTMs address? What features of LSTM units are of special importance in this regard?

Question 5 (7p)

For new brain-like hardware architectures it is desirable to rely on new forms of computer memory. In particular, one does not only want to store information but also wants to perform direct computations on it, e.g. so that one could retrieve memories not by a reference/pointer to a specific memory location - memory address (as in classical von Neumann architectures) but by actual reference/cue to the desirable memory content (especially if it tolerates incomplete or noisy cue). Naturally, it is required that such a memory system should be capable of robust learning of new patterns and storing the existing ones.

Please answer the following questions in the given order:

i) Which neural network architecture could you propose as a prototype for such a memory system? and what would be the recommended learning approach?

ii) How would you make the network store particular memory patterns? What would be the input to your network and what type of data representation (encoding) would you use? How would actual learning work (to store desirable information in the network's memory)?

iii) What does the network memory capacity (the number of patterns it can reliably store and recall) depend on? How would you measure the capacity? How would you invest extra research effort or computational/algorithmic developments to enhance the capacity (robustness)?

iv) How would your network behave when new memories are to be acquired in the situation where the network capacity has approached the upper limit?

v) What would be key problems and challenges with this kind of form of memory (please explain and motivate).

Question 6 (8p)

Your task is to help gardeners protect their plants from intruding wildlife. Since hardware and equipment resources are rather limited, it is recommended that your solution should rely on the data acquired by a microphone placed centrally in the garden coupled with cheap digital signal processing (DSP) units that filter audio signals and convert them to time-frequency representation (a spectrogram by means of moving-window Fourier transform). As a result, a 10-sec-long signal from the microphone is represented by a 30-by-10 matrix normalized to [0, 1] (20 seconds are divided into 10 non-overlapping 2-sec intervals of spectral power in 30 frequency bands where each matrix element represents normalised power in that frequency band). You get this matrix once every 20 seconds, and your system is so fast that you easily complete all your operations in less than 0.1 seconds, after which your system does nothing until it gets a new input. You treat each input independently so there is no need to consider sequences. You have collected real-world data from intruding rabbits, deer, cats, dogs and humans and in total you have 352000 labelled samples. The idea is that your neural network based approach should classify a 20-sec-long sound signal into one of three classes: animals considered as intruders threatening the plants (rabbits, deer etc.), animals that do not tend to cause much trouble (cats, dogs, etc.) and humans harmless to garden plants. It is assumed that your system has to deal with only a single "intruder" at a time (so there are no cases with multiple animals simultaneously intruding a garden).

Describe how you design your neural network approach. In particular, please fill in the table:

A. Problem type that is addressed and a neural network architecture (name, the number of nodes in the layers)	
B. Training algorithm (name) and any data pre-processing, include information on the recommended data representations/encoding for inputs and outputs	
C. Data usage – how data is used for training, validation and/or model selection etc.	
D. Key hyperparameters, how is model selection conducted	
E. Loss function and/or systems level performance metric	
F. How the neural network is used in the production cycle, i.e. how the predictions are made and/or the network's output is interpreted/evaluated/visualised/utilised	
G. Potential challenges and risks plus extra short comments (e.g. on generalisation)	