Skoltech
Skolkovo Institute of Science and Technology

Jury Member Report – Doctor of Philosophy thesis.

Name of Candidate: Talgat Daulbaev

PhD Program: Computational and Data Science and Engineering

Title of Thesis: Applications of differential equations and reduced-order modeling for deep learning

Supervisor: Professor Ivan Oseledets
Co-supervisor: Professor Andrzej Cichocki

Name of the Reviewer: Evgeny Burnaev, Full Professor

I confirm the absence of any conflict of interest (Alternatively, Reviewer can formulate a possible conflict)	**Signature** **Date: 06-03-2023**

The purpose of this report is to obtain an independent review from the members of PhD defense Jury before the thesis defense. The members of PhD defense Jury are asked to submit signed copy of the report at least 30 days prior the thesis defense. The Reviewers are asked to bring a copy of the completed report to the thesis defense and to discuss the contents of each report with each other before the thesis defense. *If the reviewers have any queries about the thesis which they wish to raise in advance, please contact the Chair of the Jury.*
Reviewer's Report
The thesis is devoted to applications of differential equations and model order reduction techniques to different deep learning problems.

The first part of this thesis addresses various challenges for the so-called neural ordinary differential equations (neural ODEs) models: how to compute gradients w.r.t. parameters of neural ODEs, such that the computations are memory-efficient, fast, and stable? what normalizations can be potentially applied to neural ODEs? how to modify the training procedure of neural ODEs in order to improve the robustness of the models to adversarial attacks?

The second part of this thesis is devoted to model order reduction techniques that are applied to standard neural networks.

The introduction gives the background and the context of the thesis. This chapter contains brief formulations of the considered machine learning problems, some general information about neural ODEs, and the basic intuition about reduced-order modeling techniques.

The second chapter introduces an approximate method for fast and stable "backpropagation" through the neural ODEs model. This method is based on the Barycentric Lagrange Interpolation, which is incorporated into the standard adjoint method instead of the backward-in-time subsystem of ODEs for the activations of neural ODEs.

In the third chapter, the author experimentally evaluates the impact of different normalizations (batch/layer/spectral/weight normalizations) on the quality of the neural ODEs classifier.

The fourth chapter introduces several training procedures that improve the robustness of neural ODEs. Two of these procedures do not require additional computations and are better than the standard training procedure. The improvements in robustness are not so huge but systematic. Moreover, these methods can be easily implemented.

In the fifth chapter, the model order reduction techniques traditionally applied to systems of ODEs are used to accelerate neural networks. The initial neural network is transformed into the feedforward network in a low-dimensional space. Experiments on the CIFAR-10 dataset showed that it is possible to gain more than ×2 acceleration without any quality drop.

The sixth chapter introduces the application of the active subspaces method to neural networks. The contributions are two-fold. First, the active subspaces method is used for neural network compression. Second, there proposed a way to compute universal adversarial attacks that utilizes the computation of the dominant active subspace vector.

The topic of the dissertation is fully relevant to its actual content. The methods are novel and are relevant for this research area.

The text of the thesis is OK, but still there are a lot of things that can be and should be improved, e.g.

- The section Publications on page iii does not include an explicit list with the authors' papers. The section itself requires significant formatting. For each paper the authors should specify its rank, i.e. whether it is Q1, or A*, etc. Moreover, the logic of section is strange, since the authors mentions chapters in some random order.
- In the list of figures (pages ix - xiii) some text is in red, and some text is in black.

- Page 4: “odel reduction to standard artificial…” – the sentence is incomplete.
- “see ??” on page 16.
- The experimental setup in Chapter 3 should be described in more detail. Which datasets? What is the protocol of experiments/comparisons? Etc.
- On pages 24, 25, 42, 43 and 44 the author many times mentioned some magic section “Supplementary materials”. However, the thesis does not contain this section.
- In Section 4.3.5 the author mentioned some results on learned dynamics. However, the results are located in non-existing section with supplementary materials, and at the same time section 4.3.5 itself does not contain any conclusions from the results of this learned dynamics.
- Algorithm 1: it looks like description of step 5 is missing.
- Proof of lemma 6.3.2 is missing.

The presented results are tested on standard benchmarks, and the code of all methods is publicly available. There are comparisons with the state-of-the-art approaches and experimental evaluations. The results are published in international journals, including A* conference and Q1 journal, i.e. the requirements to publications have been fulfilled.

The proposed methods from Chapters 2-4 can be potentially applied for all practical problems, where neural ODEs can be used. Results from Chapters 5-6 can be applied to any classification problems.

Speaking about the drawbacks, in the last two chapters, the experiments are conducted only for small datasets. Moreover, the method from chapter 5 is only applied to feedforward networks without skip-connections. In addition, the content of chapter 3 lacks thoughtful theoretical explanations of the observable effect. It could be interesting to discuss these issues during the defense.

Also, during the defense, I would like to get comments on the following issues:

- The results, presented in Chapter 2, are about an approximate method for fast and stable “backpropagation” through the neural ODEs model. The author demonstrates on some standard classification problems like CIFAR10 that the proposed neural ODE can achieve better performance. However, it is not clear whether there are practically important cases where the proposed approach really allows achieving results better than SOTA methods;

- It is not clear from the results of section 2.4 whether the error term (2.9) for the approach, proposed in chapter 2, is smaller compared to the basic approaches? Can we get any explicit formulas? Is it possible to combine the estimate in a single statement?

- All baselines in table 5.4 for RON were developed before 2019. Are there any other more recent methods in this domain? Is 2-4 FLOP reduction enough for industrial applications?

- In section 6 the author proposed to approximate the network output by a linear combination of the orthogonal polynomial basis functions forming so-called polynomial chaos expansion. However, it is well known that PCE is valid if distributions of input coordinates of this polynomial approximation are independent and are from some limited list of well-known distributions like normal distribution. To what extent do these assumptions on PCE influence efficiency of the proposed method?

Overall conclusion: the candidate obtained important results verified by publications in good venues. However, the text of the thesis should be significantly extended and improved.

Provisional Recommendation
Yes: *I recommend that the candidate should defend the thesis by means of a formal thesis defense*