EEL6812 Final Project - Guidelines

Instructor: Dr. Shahana Ibrahim
January 26, 2026

1 Project Overview

The final project of our course EEL-6812 provides a unique opportunity to delve into a specific research topic within deep learning. The primary aim is to understand deep learning models and their training strategies, and apply these algorithms to solve some of the interesting applications. You may choose a topic that falls in any of the following two tracks. Along with the track details, you are also given a list of representative publications in each directions. This is not a comprehensive list and you are free to choose any topics/ideas/methods under each sub-track.

- **Track I: Robust Deep Learning**: This track focuses on failure scenarios of deep learning. Here, you will investigate why models break and how to make them resilient to unexpected, uncertain or malicious inputs.
  - **Sub-track I: Adversarial Defense**: Adversarial defense is the set of techniques designed to restore the robustness of a deep neural network against inputs that have been maliciously perturbed to exploit the model's underlying vulnerabilities.
    - S. Amini and S. Ghaemmaghami, "Towards Improving Robustness of Deep Neural Networks to Adversarial Perturbations," in IEEE Transactions on Multimedia, vol. 22, no. 7, pp. 1889-1903, July 2020, doi: 10.1109/TMM.2020.2969784
    - A. Fawzi, S. -M. Moosavi-Dezfooli and P. Frossard, "The Robustness of Deep Networks: A Geometrical Perspective," in IEEE Signal Processing Magazine, vol. 34, no. 6, pp. 50-62, Nov. 2017, doi: 10.1109/MSP.2017.2740965.
    - Ahmadreza Jeddi, Mohammad Javad Shafiee, Michelle Karg, Christian Scharfenberger, Alexander Wong; Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR), 2020, pp. 1241-1250
  - **Sub-track II: Domain Adaptation for Distributional Robustness**: This focuses on developing models that can maintain high performance when the data distribution at test time differs from the training distribution. The goal is to adapt knowledge learned from a source domain to a target domain with minimal performance drop, ensuring reliability under real-world shifts such as environmental changes or sampling biases.
    - Tzeng, Eric, et al. "Adversarial discriminative domain adaptation." Proceedings of the IEEE conference on computer vision and pattern recognition. 2017.
    - Ding, Ning, et al. "Source-free domain adaptation via distribution estimation." Proceedings of the IEEE/CVF conference on computer vision and pattern recognition. 2022.
    - Zhang, Jing, et al. "Importance weighted adversarial nets for partial domain adaptation." Proceedings of the IEEE conference on computer vision and pattern recognition. 2018.
  - **Sub-track III: Out-of-distribution/Anomaly Detection**: Out-of-distribution (OOD) or anomaly detection aims to identify inputs that differ significantly from the data seen during training. The goal is to ensure that models can recognize when they encounter unfamiliar or abnormal samples instead of making overconfident predictions.
    - Miyai, Atsuyuki, et al. "Locoop: Few-shot out-of-distribution detection via prompt learning." Advances in Neural Information Processing Systems 36 (2023): 76298-76310.
    - Mueller, Maximilian, and Matthias Hein. "Mahalanobis++: Improving OOD Detection via Feature Normalization." arXiv preprint arXiv:2505.18032 (2025).

    - Sultani, Waqas, Chen Chen, and Mubarak Shah. ”Real-world anomaly detection in surveillance videos.” Proceedings of the IEEE conference on computer vision and pattern recognition. 2018.

  - **Sub-track IV: Hallucination Mitigation in VLMs/LLMs**: Hallucinations in vision-language models (VLMs) or large language models (LLMs) occur when the model generates confident but incorrect or irrelevant information. This sub-track focuses on analyzing the causes of such hallucinations and developing methods to mitigate them, aiming to enhance the reliability and factual accuracy of AI systems.
    - Yang, Le, et al. ”Nullu: Mitigating object hallucinations in large vision-language models via halluspace projection.” Proceedings of the Computer Vision and Pattern Recognition Conference. 2025.
    - Park, Seongheon, et al. ”Steer LLM Latents for Hallucination Detection.” arXiv preprint arXiv:2503.01917 (2025).
    - Yang, Zhihe, et al. ”Mitigating hallucinations in large vision-language models via dpo: On-policy data hold the key.” Proceedings of the Computer Vision and Pattern Recognition Conference. 2025.

- **Track II: Deep Learning for Science**: This track emphasizes using deep learning to advance scientific discovery and understanding across disciplines such as physics, biology, chemistry, and engineering. Students will explore how neural networks can model complex phenomena, accelerate simulations, or extract patterns from high-dimensional experimental data.
  - **Sub-track I: Physics-Informed Neural Networks** — Here, you will develop models that integrate physical laws and constraints into deep neural networks to solve differential equations or model complex physical systems efficiently.
    - Raissi, Maziar, Paris Perdikaris, and George E. Karniadakis. ”Physics-informed neural networks: A deep learning framework for solving forward and inverse problems involving nonlinear partial differential equations.” Journal of Computational physics 378 (2019): 686-707.
    - Cai, Shengze, et al. ”Physics-informed neural networks for heat transfer problems.” Journal of Heat Transfer 143.6 (2021): 060801.
  - **Sub-track I: AI for Molecular and Protein Modeling** —You will apply deep learning to understand biomolecular structures, predict protein dynamics, or simulate interactions relevant to drug discovery and bioengineering.
    - Shabeeb, Zain, et al. ”Learning the diffusion of nanoparticles in liquid phase TEM via physics-informed generative AI.” Nature Communications 16.1 (2025): 6298.
    - Liu, Bojun, et al. ”Exploring transition states of protein conformational changes via out-of-distribution detection in the hyperspherical latent space.” Nature Communications 16.1 (2025): 349.
  - **Sub-track III: Scientific Data Generation and Simulation** — In this subtrack, you will use generative models such as diffusion or GAN-based frameworks to create synthetic scientific data for experiments that are costly or time-consuming to perform.
    - C. Xu, D. Tang, A. Seretis and C. Sarris, ”A Diffusion-Based Propagation Model for Path Loss Prediction in Indoor Environments,” 2025 19th European Conference on Antennas and Propagation (EuCAP), Stockholm, Sweden, 2025, pp. 1-5, doi: 10.23919/EuCAP63536.2025.10999434.
    - Chen, Liang-Yu, et al. ”A Diffusion-Model-Based Methodology for Virtual Silicon Data Generation.” IEEE Transactions on Semiconductor Manufacturing (2025).
  - **Sub-track IV: Climate and Environmental Modeling** — Leverage deep learning to analyze and predict environmental trends, such as climate change impacts, air quality patterns, or natural disaster forecasting.
    - Oyama, Norihiro, et al. ”Deep generative model super-resolves spatially correlated multiregional climate data.” Scientific Reports 13.1 (2023): 5992.
    - Rühling Cachay, Salva, et al. ”Dyffusion: A dynamics-informed diffusion model for spatiotemporal forecasting.” Advances in neural information processing systems 36 (2023): 45259-45287.

For in-depth learning on each track and also for recent progress in these direction, you can take a look at the recent publications in top AI conferences such as NeurIPS, ICML, ICLR, CVPR etc.

Key dates for the final project are as follows:

1. **Initial Project Idea and Group** (Points 5): Due by 11.59 PM on March 4, 2026
2. **Project Presentation and Demo** (Points 25): April 20 and 22, 2026 (in-class) and via zoom for students who registered for the remote session
3. **Final Report Submission** (Points 30): Due by 11.59 PM on May 1, 2026

2 Initial Project Idea and Group

Student should form a group of three and submit an initial idea of the project for review. Only one member per group needs to submit. Considering the volume of the work and the weightage on project, I strongly advise you to form groups of three, collaborate, and produce quality project submissions.

Initial project idea must include the following details:

- Who is on the team?
- A tentative title for the project and clearly indicate the track/subtrack
- Brief description of project goals and proposed methods
- Reference to at least 3 related works

Submit this in pdf format in webcourse page (preferably latex generated pdf; word file converted to pdf is also accepted). Only one team member need to submit this pdf. The due date for the submission is 11.59 PM on March 4, 2026. No late submissions are accepted.

3 Project Presentation and Demo

The students are expected to make a presentation and demo (no longer than 12 minutes) to convey the key idea of their project. The presentations should include content to address the following questions:

- **What is your project about?** Describe your goals without using many technical terms. Imagine explaining your project to someone unfamiliar with machine learning.
- **How is this done currently, and what are its limitations?** Describe at least three related works and understand their limitations with technical details.
- **What is your approach, what is innovative about your approach, and why do you believe it will succeed?** Explain what is unique about your work. How does it differ from existing methods, and why do you think it will be more effective?
- **How do you evaluate your approach and can you show a successfully implemented demo?** Which dataset or experiment you use? What metrics you employ? Can you present one clear scenario of the results generated from your approach via a live demo?
- **What are the remaining challenges, pending experiments for detailed analysis, and how long will it take to address them?** Provide a timeline for your project and identify the most challenging parts of the proposed approach.

The presentations will be evaluated based on

- Overall quality of the presentation materials including well-represented figures or tables
- Clarity of presentation delivery with convincing details about the proposed method and technical correctness

The project proposal presentation will be held on April 20 and 22, 2026 (in-class). Students who registered in the remote session can join via zoom. The proposal slides should be uploaded in webcourse page after the presentation.

4 Final Report

Each team should submit a final report (latex generated pdf; no other format is allowed) of the project through webcourse page. Only one team member need to submit the report and make sure all the team members' names are shown in author list of paper.
Report Format: The format/template for the report can be downloaded by clicking here or copy and paste the following link to your browser: `https://media.icml.cc/Conferences/ICML2026/Styles/icml2026.zip`. The students must use the template provided. Any report which do not use the posted template will not be evaluated. The report should look similar to a publishable paper, having a title, an introduction about the topic you worked on and the background of your work, discussing related works, technical approach including the mathematical formulations/optimization problem, an experiment section consisting of experiment design and experiment results, and finally a section on conclusion and future work. You should also cite the list of references you used.

The grading of the final report will be based on clarity (5 points) and intellectual merit (25 points)
Clarity. For clarity, clear descriptions of the problems, mathematical formulations, methods, experimental settings, and results are expected. To accomplish this clarity, the final report must be at least 5 pages long (4 full page write up and in the fifthe page, you can present the references) and cannot be more than 8 pages (including appendices, figures, references, and everything else you choose to submit).
Intellectual Merit An ideal report should be a nearly publishable piece of work. I strongly encourage you to continue developing your final project beyond EEL6812 and consider submitting it to a suitable conference or journal. The final report will be evaluated based on several criteria:

- **Effort**: Did the team approach the project seriously, obtain results, and make improvements to their technical approach if initial attempts failed? Were the teams actively engaged and able to convey novel insights about their projects? Do the strategies attempted make sense?
- **Significance**: Did the authors select an interesting or real problem to address, rather than just a small, trivial problem? Is the work likely to be useful and impactful?
- **Novelty**: While groundbreaking novelty is not necessary, the best final projects should offer a slightly different perspective from anything previously published. Just executing the code of an existing work without changing anything will result in considerable score reduction. The evaluation criteria is roughy detailed as follows:
  - Points 25-23: Projects that make significant, novel, nearly publishable deep learning approach
  - Points 22-20: Projects that are well-executed for complex problems but do not lead to significant contribution with limited novelty.
  - Points 19-17: Not so well-executed with a straight-forward application of an exiting deep learning method
  - Points 17-0: Poorly executed with lack of technical understanding of deep learning or just copied an existing approach and their implementation

The final report submission is due by 11.59 PM on May 1, 2026. No late submissions are accepted.