Jingmin Sun on Robustness of ML models against adversarial perturbations:

1. Decide the topic
2. Read papers on Distributional Robustness Optimization and have some write ups
3. Discuss with members for Virtual adversarial training, understand all the methods in our project
4. Code WRM ,VAT, REG model based on some original implementation and other minor supplement functions .

Notes: For convenience, you can execute the code using the provided run.sh script.
Code also at https://github.com/JingminSun/VATWRM-pytorch.git