CCST 9080 Semester 2, 2024-25
Tutorial 5 (17/18 March, 2025)

1. TA Introduction and grouping (10 min)

TA will give a short introduction and divide students into smaller groups (about 3 per group)

2. Discussion on aspects related to AI systems (e.g. security, privacy, ChatGPT, applications) (20 min)

Each sub-group can select **two or three** questions related to issues about AI systems provided by the TA. Group members try to discuss among themselves and prepare a five-minute presentation.

- 1. AI + X (where X can be any interesting subjects such as social science, art, law, building and construction, any types of design, medical, cartoon….) how AI can be applied to this X area?
- 2. Security issues behind AI systems and how to provide further protection?
- 3. Is privacy an issue in AI systems?
- 4. Issues related to ChatGPT (bias, wrong answers, jobs, applications of ChatGPT, use of ChatGPT in assignments….).
- 5. Some selected models in AI, e.g. decision tree, random forest etc.
- 6. Will AI systems be biased in the aspects of gender, age, and other factors?
- 7. Try to use a Venn diagram to briefly show the relationship and tasks between different AI concepts including AI, GenAI, LLM, AIGC, NLP, ML, DL, RL, and CNN.
- 8. Discuss "AI for Security" and "Security of AI".
- 9. Different AI models can have varying performance in different domains. For instance, some AI systems excel in programming, while others in translation. Why?
- 10. How do AI systems help FinTech?
- 11. Why do users need to check the generated content before using it? Or, why can the content generated by AI systems contain potential errors?
- 12. Is it possible to embed the GenAI into financial desktop applications to buy or sell stocks directly?
- 13. Normally, GenAI will follow the principles to avoid illegal outputting. Is it possible to bypass these principles to make the GenAI output illegal content (Jailbreak)?
- 14. Talk about some unexpected phenomena such as endless reasoning and 1.11 > 1.9 when using the GenAI.
- 15. What do you think are the jobs that AI cannot replace in the future? Why?
- 16. What are black-box and white-box AI models?
- 17. We usually classify AI techniques into strong AI and weak AI. Do the current state-of-the-art AI models belong to strong AI? Why?
- 18. Talk about multi-media in GenAI.
- 19. Can AI solve moral issues in finance?
- 20. How to prevent spam using AI techniques like fake videos?

3. Presentation by each group (20 min)
Each group will present their answers to the chosen questions.

4. TA comments on the findings (5 min)
Note that TA will observe how your group conducts the discussion and give individual mark to each student.

[Confidential to TAs, do NOT release this to the students before the tutorial]

TAs can also freely pick any related topics.