ICTSS00120 - Artificial Intelligence Skill Set

Session 15: Applying LLMs as Agents in Agentic Workflows

Lecturer: Jordan Hill

GOVERNMENT OF WESTERN AUSTRALIA
TAFE WA North Metropolitan

Learning Objectives

- Understand the concept of LLMs acting as autonomous agents
- Explore how LLMs can perform sequential tasks via agentic workflows
- Review the core ideas from Dominik Jeurissen's presentation on LLMs playing text-based games
- Discuss practical applications of LLM agents in industry
- Learn how to design and implement basic agentic workflows

What is an AI Agent?

- An AI agent is an autonomous system capable of perceiving its environment and acting upon it to achieve specific goals
- In language models, this means LLMs that can think, plan, and execute tasks independently, often through prompting strategies

Agentic Workflow:

- LLMs not only generate text but can be orchestrated to perform multiple steps
- Adaptively solve problems
- Interact with environments or tasks

Core Idea of LLM Agents

- Break down complex tasks into smaller subtasks
- Use the LLM iteratively to plan, reason, and execute
- Achieve persistent goal fulfillment through agent loops

Example:

- An LLM acting as a virtual assistant that:
  - Schedules meetings
  - Writes emails
  - Learns from interactions

LLMs as agents: Text-Based Games

<iframe width="100%" height="600" src="https://www.youtube.com/embed/d3rFLAfT2gw?start=10" title="LLMs playing text games" frameborder="0" allowfullscreen></iframe>

Why This Is Interesting: Zero-Shot Automation

- **Generalist to Specialist Transformation**:
  - Taking a general-purpose LLM and applying it to specific domains without domain-specific training
  - Demonstrates the versatility of foundation models
- **Zero-Shot Capabilities**:
  - LLMs can perform tasks they weren't explicitly trained for
  - Reduces the need for specialized AI systems for every task

This is a big deal!

- **Paradigm Shift in Automation**:
  - Traditional automation: Domain-specific systems built for single purposes
  - LLM agents: One model adapts to multiple domains through prompting
- **Democratizing Complex AI Applications**:
  - Lowers the barrier to implementing sophisticated AI workflows
  - Enables rapid prototyping and deployment of intelligent systems

This represents a fundamental shift from building specialized AI to orchestrating general AI for specific purposes

Why Employ LLMs as Agents?

- Automate complex, multi-step workflows
- Enable dynamic interaction with real or simulated environments
- Improve decision-making with continuous feedback
- Facilitate adaptable, intelligent automation in real-world industries

Example Applications of LLM Agents

- Customer support bots that resolve problems with multi-stage reasoning
- Code-generating assistants that plan, write, and review code
- Virtual research assistants that perform searches, generate summaries, and synthesize information
- Automated text adventure games and simulations for training AI

How Do LLM Agents Work?

1. **Perception**:
   - Input data, environment state, user instructions
2. **Planning**:
   - Use the LLM to generate a plan or sequence of actions
3. **Execution**:
   - Carry out actions, interact with environment or data
4. **Feedback and Replanning**:
   - Adapt based on results, continuously refine goals

Demo / Exploration

- How can we prompt LLMs to act as agents?
- What design strategies improve agent robustness?
- How do we integrate tools – like search, memory, or APIs?

Summary

- LLMs can be designed as agents to perform complex, multi-step workflows
- Dominik Jeurissen's presentation shows how text-based environments provide a model for agentic AI
- Practical applications in automation, reasoning, and decision-making are rapidly expanding

Questions?

- How might you use an LLM agent in your workplace?
- What are the challenges of building robust AI agents?
- How can agentic workflows improve productivity and innovation?

Let's explore the future of AI agents!

Prepare your questions and think of potential applications in your interest areas.