HSLU Hochschule Luzern

SAS LLMs and AI Agents (Bootcamp)

Program Directors

Prof. Dr. Aygul Zagidullina
aygul.zagidullina@hslu.ch

Dr. Elena Nazarenko
elena.nazarenko@hslu.ch

Website

hslu.ch/sas-llm

Overview
This practical bootcamp offers you an opportunity to immerse yourself in the world of natural language processing (NLP), Large Language Models (LLMs) and AI Agents. Over eight days, you will have access to expert guidance and support and learn everything from the basic concepts to the latest developments and innovation in the field.

Natural Language Processing
This training introduces the foundational concepts of NLP. Participants will explore core modeling techniques such as vector representations and probabilistic models. The program provides an overview of modern transformer-based models, setting the stage for advanced applications.

LLM Techniques and AI Agents
Participants will also develop LLMs skills. The course covers the fundamentals of prompt engineering and explores retrieval-augmented generation (RAG) to enhance LLM contexts. In the framework of hands-on projects, attendees will build LLM-powered Agents capable of executing tasks, solving problems, and integrating with various tools.
Key topics such as model evaluation, bias mitigation, security considerations, and MLOps practices are also addressed to ensure responsible and effective deployment of LLMs and AI Agents.

Aims
Participants finish the Bootcamp with an in-depth understanding of NLP and LLM concepts, methods and tools, reinforced by practical, hands-on experience. The modules build on each other and offer both foundational knowledge and advanced technical skills to apply across a variety of domains.

Module 1: Foundational Principles of NLP
- Introduction to NLP and preprocessing techniques
- Advanced NLP techniques
- Representation and embeddings
- Probabilistic and sequence models

Module 2: Transformer Models and Fundamentals of LLMs
- Introduction to transformer models
- Transfer learning
- Applying transformers for NLP tasks (chatbots, classification, summarization)
- Introduction to LLMs and prompt engineering

Methodology

This certificate program is delivered in the shape of an intense bootcamp, with focus on day-to-day practical projects. Participants should be ready to get actively involved in hands-on exercises and projects and deepen their understanding and consolidate their skills in the process.

We offer a dynamic learning environment that transcends the traditional classroom setting. This to ensure that our participants develop a profound understanding of Natural Language Processing and the skills to apply it in practice.

Module 3: RAG and Language Agents
- Introduction to vector databases
- RAG (LlamaIndex/LangChain)
- RAG variations (GraphRAG, CAG)
- Semantic search and document retrieval
- Language agents

Module 4: Parameter-Efficient Fine-Tuning and Model Evaluation in LLMs
- Introduction to PEFT (LoRA, QLoRA)
- Full fine-tuning vs. PEFT
- Fine-tuning (full and PEFT) vs. RAG (what to use when)
- Evaluation metrics for LLMs and RAG
- Bias in LLMs
- Responsible AI

Module 5: MLOps for NLP and Deploying Models to Production
- Introduction to MLOps for NLP and LLMs
- Deploying models for production
- Cloud vs. on-premise deployment strategies
- Testing strategies for AI applications

Module 6: Real-World Applications for NLP and LLMs
- Real-World Applications for NLP and LLMs
- Industry case studies
- Hands-on applied NLP tasks
- Emerging trends and challenges associated with LLMs

Module 7: Agent Orchestration and Multi-Agent Systems
- Foundations of Multi-Agent Systems and Agentic AI
- Architectures and Orchestration patterns for Agent workflows
- Use cases: collaborative Multi-Agent Systems
- Challenges and Evaluation Strategies for Agents performance
- Coordination strategies: communication protocols and tool calling

Module 8: Red Teaming, Guardrails, and Evaluation Strategies
- Introduction to Red Teaming techniques for LLMs
- Identifying vulnerabilities: jailbreaks, prompt leakage, misuse scenarios
- Overview and application of the Guardrails Framework
- Evaluating LLMs for robustness, reliability, and safety
- Hands-on: Red Teaming and Guardrails application in enterprise use cases
- Exploring Model Context Protocol (MCP) by Anthropic

Last updated 8 July 2025