Chair of Applied Computer Science X

Prof. Dr. Ruben Mayer

UNIVERSITÄT BAYREUTH

Title

MCP-Based Tool-Using Agent with Proactive Toolchain Construction – Project (B.Sc./M.Sc.)

Background

This topic centers on LLM agents built on the Model Context Protocol (MCP) that can autonomously discover, select, and compose tools into *toolchains* instead of relying on a fixed, hand-curated tool list. The focus is on proactive toolchain construction mechanisms—such as dynamic tool request, vector-based routing over large tool registries, and iterative invocation strategies—that enable agents to scale to thousands of tools with lower context overhead and improved success rates. By studying architectures like MCP-Zero-style proactive tool usage, this project explores how protocol-level design (MCP), retrieval and routing algorithms, and interaction policies jointly determine the efficiency, robustness, and generality of modern tool-using LLM agents.

Task definition

Implement an MCP-based agent that does *proactive* toolchain construction at runtime, aiming to reduce context overhead while preserving accuracy.

Literature review:

MCP-Zero: Proactive Toolchain Construction for LLM Agents from Scratch (https://arxiv.org/html/2506.01056v1)

Supervisor

Nikita Agrawal
Feel free to ask any questions anytime via Teams or e-mail (Nikita.Agrawal@uni-bayreuth.de)