JARAMOGI OGINGA ODINGA UNIVERSITY OF SCIENCE AND TECHNOLOGY

SCHOOL OF INFORMATICS AND INNOVATIVE SYSTEMS DEPARTMENT OF COMPUTER SCIENCE AND SOFTWARE ENGINEERING

UNIVERSITY EXAMINATION FOR THE DEGREE OF BACHELOR SCIENCE IN

COMPUTER SECURITY AND FORENSICS 3RD YEAR 2ND SEMESTER 2024/2025 ACADEMIC YEAR

MAIN CAMPUS

COURSE CODE: ICB 1312

COURSE TITLE: ARTIFICIAL INTELLIGENCE

EXAM VENUE: LAB 9 **STREAM: BSC COMP. SECURITY**

DATE: 25/4/2025 **EXAM SESSION: 15.00-17.00**

TIME: 2.00 HOURS

INSTRUCTIONS:

1. **Answer Question 1 (Compulsory) and ANY other two questions**
2. **Candidates are advised not to write on the question paper**
3. **Candidates must hand in their answer booklets to the invigilator while in the examination room**

QUESTION ONE **[30 MARKS]**

a) Explain why achieving *general intelligence* in AI is significantly more complex than building *narrow AI*. Provide an example of a challenge that general AI must overcome. [4 Marks]

b) Consider a *state space search problem* where an AI agent must navigate a maze. Explain why *iterative deepening depth-first search (IDDFS)* would be preferred over *breadth-first search (BFS)* in a memory-constrained environment. [4 Marks]

c) A self-driving car uses *First-Order Logic (FOL)* to make real-time driving decisions. Identify two limitations of FOL in dynamic environments and suggest one possible solution. [4 Marks]

d) An AI medical chatbot built in Prolog incorrectly diagnoses patients due to *incorrect rule formulation*. Suggest two debugging strategies to identify and fix faulty rules. [4 Marks]

e) A household robot uses STRIPS (Stanford Research Institute Problem Solver) for task planning. Explain how STRIPS ensures the robot executes tasks in the correct sequence. [4 Marks]

f) A chatbot trained for semantic analysis fails to understand sarcasm. Explain why this happens and suggest one potential solution using NLP techniques. [4 Marks]

g) A deep learning model trained for medical diagnosis fails when applied to a different hospital's dataset. Explain the likely cause, and how transfer learning can help. [4 Marks]

h) A cybersecurity firm uses an *Artificial Immune System (AIS)* for intrusion detection. Explain how the *negative selection algorithm* helps in detecting cyber threats. [2 Marks]

QUESTION TWO **[20 MARKS]**

(i) A team of developers is working on an AI-powered chatbot for a financial institution. The chatbot is expected to handle complex customer inquiries, detect fraudulent activities, and make recommendations based on user behavior. However, after initial deployment, users complain that the chatbot frequently makes incorrect recommendations and struggles with understanding user intent.

(ii) Identify and explain three key AI techniques that could improve the chatbot's performance. [6 Marks]

(b) Give real-world examples where the mentioned techniques have been successfully implemented. [3 Marks]

(c) A logistics company wants to optimize its delivery routes using Artificial Intelligence. The current system relies on a simple GPS routing algorithm but fails to account for real-time traffic, weather conditions, and road closures, leading to frequent delays.

(i) Describe how heuristic search algorithms, such as A* search, could improve the efficiency of the company's delivery system. [6 Marks]

(ii) Compare it to blind search methods and justify why heuristic search is a better approach. [5 Marks]

QUESTION THREE **[20 MARKS]**

a) A medical research institute is using Prolog to develop an expert system that diagnoses rare diseases based on patient symptoms. However, the system sometimes returns contradictory conclusions, making it unreliable.

(i) Examine how *facts*, *rules*, and *goals* in Prolog influence the system's decision-making process. [6 Marks]
(ii) Suggest debugging techniques to resolve contradictions and improve accuracy. [4 Marks]

b) An AI-controlled robotic assistant in a warehouse must autonomously plan and execute tasks such as organizing inventory, handling fragile items, and assisting human workers. The robot occasionally gets stuck in infinite loops while planning tasks.

(i) Discuss how *Goal Stack Planning* can help the robotic assistant avoid infinite loops and improve its efficiency. [7 Marks]
(ii) Discuss the potential limitations of this approach. [3 Marks]

QUESTION FOUR **[20 MARKS]**

a) A social media platform implements an AI-based content moderation system to detect hate speech and misinformation. However, the AI frequently flags harmless posts while allowing inappropriate content to remain online.

(i) Discuss the challenges of *syntactic*, *semantic*, and *pragmatic processing* in Natural Language Processing (NLP) when moderating social media content. [6 Marks]
(ii) Suggest improvements that could reduce false positives and false negatives. [4 Marks]

b) A financial institution deploys an AI-driven credit scoring system based on neural networks. The system denies loans to applicants with high financial stability but approves risky individuals, raising concerns about bias in AI decision-making.

(i) Discuss how *explanation-based learning (EBL)* and *formal learning theory* could be used to enhance the model's fairness and interpretability. [6 Marks]
(ii) Give examples of real-world AI bias mitigation strategies. [4 Marks]

QUESTION FIVE **[20 MARKS]**

a) An agricultural AI system is designed to recommend optimal irrigation schedules based on weather patterns, soil conditions, and crop type. Farmers report that the AI's recommendations are inconsistent, sometimes suggesting excessive watering during dry periods.

(i) Discuss how *Fuzzy Logic Systems* can help the AI model make more reliable irrigation recommendations. [5 Marks]
(ii) Explain a practical example of how fuzzy logic differs from traditional Boolean logic in AI applications. [4 Marks]

b) A cybersecurity firm is developing an AI system to detect new malware threats. Traditional antivirus methods struggle to identify zero-day attacks due to the ever-changing nature of malware.

(i) Discuss how *Genetic Algorithms (GAs)* and *Artificial Immune Systems (AIS)* can be used to improve the detection of zero-day malware threats. [6 Marks]

(ii) Compare the efficiency of these techniques in evolving threat landscapes. [4 Marks]

- **END -**