Planeación de acciones usando un sistema basado en reglas para robots de servicio doméstico

Luis Sergio Cano Olguin

Tutor: Dr. Jesús Savage Carmona

Agradecimientos

Resumen

Índice general

Índice de figuras

Capítulo 1

Introducción

La robótica de servicio doméstico representa un campo de proyección para la inteligencia artificial y la automatización, con aplicaciones que van desde la asistencia a personas mayores hasta la gestión autónoma de entornos residenciales (**?**). En este contexto, la planificación de acciones, es decir, la capacidad de un robot para descomponer objetivos de alto nivel en secuencias ejecutables, es un desafío en entornos dinámicos y no estructurados donde interactúan humanos, objetos móviles y tareas imprevistas (**?**).

Los sistemas basados en reglas, como los implementados en motores de inferencia del tipo CLIPS, han demostrado ser robustos y predecibles en escenarios estructurados, como líneas de producción o laboratorios controlados (**?**). Su fortaleza radica en la transparencia del razonamiento simbólico y la capacidad de priorizar acciones críticas, como la evasión de obstáculos o la gestión de emergencias. Sin embargo, su rigidez los hace poco adaptables ante variaciones no previstas en el entorno o ante comandos expresados en lenguaje natural con alto grado de ambigüedad o complejidad (**?**).

Recientemente, los modelos de lenguaje grande (LLMs), como ChatGPT o Qwen, han emergido como herramientas capaces de interpretar y generar lenguaje natural, e incluso de actuar como agentes de planificación autónomos (**?**). Su flexibilidad contextual permite traducir instrucciones verbales en secuencias de acciones, complementando así la solidez de los sistemas basados en reglas. No obstante, su naturaleza probabilística y la falta de garantías formales de seguridad limitan su uso directo en aplicaciones robóticas donde la integridad física y la predictibilidad son prioritarias (**?**).

Esta tesis propone un **sistema híbrido de planificación de tareas** que integra un motor de reglas CLIPS (**?**) con modelos de lenguaje natural (ChatGPT/Qwen), aprovechando las ventajas de ambos enfoques: la previsibilidad y seguridad de CLIPS,

y la adaptabilidad y capacidad de comprensión lingüística de los LLMs. El sistema se implementa y valida en el robot de servicio doméstico *Justina*, desarrollado en el Laboratorio de Bio-Robótica de la UNAM, utilizando ROS 2 como marco de integración (**?**).

1.1. Contexto y Motivación

El área de la rebotica orientada al servicio doméstico ha evolucionado significativamente en la última década, impulsada por avances en percepción, planificación y interacción humano-robot (**?**). Estos sistemas están diseñados para operar en entornos no estructurados como hogares, hospitales o centros de cuidado, donde deben realizar tareas que van desde la entrega de objetos hasta la asistencia en actividades de la vida diaria. En este contexto, la capacidad de planificar acciones de manera autónoma, segura y adaptativa se convierte en un requisito fundamental.

La planificación de acciones en robótica ha sido tradicionalmente abordada mediante sistemas basados en reglas (RBS), que ofrecen un marco predecible y verificable para la toma de decisiones (**?**). Sin embargo, la creciente complejidad de los entornos domésticos—caracterizados por la presencia de humanos, objetos dinámicos y situaciones imprevistas—ha expuesto las limitaciones de los enfoques puramente simbólicos. Paralelamente, el reciente surgimiento de modelos de lenguaje grande (LLMs) ha abierto nuevas posibilidades para la interpretación de comandos en lenguaje natural y la generación de planes flexibles, aunque a menudo carentes de garantías formales de seguridad (**?**).

Esta tesis se desarrolla en el marco del Laboratorio de Bio-Robótica de la UNAM, utilizando como plataforma el robot de servicio Justina, un sistema modular basado en ROS 2 con capacidades avanzadas de navegación, manipulación y percepción. La motivación central del trabajo radica en la necesidad de desarrollar arquitecturas de planificación que combinen lo mejor de ambos mundos: la robustez y transparencia de los sistemas basados en reglas, y la adaptabilidad y capacidad de diálogo de los modelos de lenguaje modernos.

1.2. Problemática: Sistemas Basados en Reglas en Entornos Dinámicos

Los sistemas basados en reglas, implementados en motores de inferencia como CLIPS, se fundamentan en la lógica simbólica y el ciclo reconocer-actuar"(**?**). Su principal ventaja es la previsibilidad: ante un conjunto de hechos y reglas bien definidos, la respuesta del sistema es determinista y explicable. Esto los hace idóneos para aplicaciones donde la seguridad y la certificación son críticas, como en entornos industriales o médicos.

No obstante, en contextos domésticos dinámicos, estos sistemas enfrentan desafíos significativos (**?**):

1. **Rigidez interpretativa:** No pueden procesar comandos en lenguaje natural complejo o ambiguo, como "trae el libro rojo que está cerca de la ventana".
2. **Falta de adaptabilidad:** Las reglas deben ser definidas a priori; cualquier situación no prevista en la base de conocimiento puede llevar al fracaso o a un comportamiento no deseado.
3. **Dificultad para gestionar la incertidumbre:** No manejan bien la información incompleta o cambiante del entorno en tiempo real.
4. **Escalabilidad limitada:** Mantener y extender un conjunto grande de reglas para cubrir todos los escenarios posibles resulta complejo y laborioso.

Por otro lado, los enfoques puramente basados en aprendizaje automático — especialmente los LLMs—ofrecen flexibilidad y capacidad de generalización, pero introducen riesgos como (**?**)

- Comportamientos impredecibles o no verificables.
- Falta de garantías de seguridad en la ejecución física.
- Dependencia de grandes volúmenes de datos y recursos computacionales.

La problemática central, por tanto, es cómo diseñar un sistema de planificación que mantenga la seguridad y explicabilidad de los RBS, pero que sea lo suficientemente flexible para operar en entornos domésticos dinámicos e interactuar de manera natural con humanos.

1.3. Hipótesis

La hipótesis central de esta investigación postula que la integración sinérgica de un sistema basado en reglas (CLIPS) con un modelo de lenguaje grande (ChatGPT o

Qwen) puede superar las limitaciones de cada enfoque por separado, resultando en un sistema híbrido de planificación que es a la vez seguro, explicable, adaptable y capaz de entender lenguaje natural.

Esta complementariedad se articula en tres niveles:

1. **Nivel de interpretación:** Los LLMs actúan como traductores de lenguaje natural a hechos estructurados, permitiendo que comandos complejos y ambiguos sean convertidos en representaciones simbólicas que CLIPS puede procesar (**?**).
2. **Nivel de planificación:** Se implementa una arquitectura de planificación dual, donde CLIPS genera planes predecibles y seguros para tareas conocidas, mientras que los LLMs proponen soluciones flexibles para situaciones novedosas o complejas (**?**).
3. **Nivel de validación y selección:** Un mecanismo de supervisión evalúa los planes generados por ambos motores con base en criterios de seguridad, eficiencia y contexto, seleccionando la mejor opción o combinándolas de manera segura.

Se espera que este sistema híbrido:

- Mejore la tasa de éxito en la ejecución de tareas en entornos domésticos.
- Reduzca el tiempo de respuesta ante comandos complejos.
- Mantenga un comportamiento seguro y predecible en situaciones críticas.
- Permita una interacción más natural e intuitiva con usuarios no expertos.

La validación de esta hipótesis se realizará mediante experimentos en simulación y con el robot físico Justina, comparando el desempeño del sistema híbrido frente a enfoques puramente basados en reglas o puramente basados en LLMs (**?**).

1.4. Objetivos

- **Diseño del Sistema Híbrido:**
  - Definir un conjunto jerárquico de reglas en CLIPS para priorizar acciones críticas.
  - Especificar la arquitectura de integración entre CLIPS y modelos de lenguaje natural.
  - Diseñar un marco de planificación dual que permita tanto a CLIPS como a ChatGPT generar y ejecutar planes.
  - Establecer protocolos de comunicación y validación entre los módulos.
- **Implementación Técnica:**

  - Integrar el motor de reglas CLIPS con ROS (Robot Operating System).
  - Desarrollar el módulo de interfaz con APIs de ChatGPT o implementación local de Qwen2.5-0.5B.
  - Implementar capacidades de planificación autónoma en ChatGPT mediante prompting estructurado.
  - Desarrollar un mecanismo de selección y validación entre planes generados por diferentes motores.
- **Capacidades de Interacción Natural:**
  - Implementar traducción de comandos en lenguaje natural a hechos estructurados de CLIPS.
  - Desarrollar mecanismos de diálogo para resolución de ambigüedades.
  - Crear protocolos de retroalimentación para aprendizaje incremental.
- **Validación Experimental:**
  - Validar el sistema en escenarios realistas con el robot físico y simulaciones.
  - Evaluar el rendimiento mediante métricas comparativas:
    - Tiempo de ejecución de tareas y tasa de éxito.
    - Precisión en interpretación de comandos complejos.
    - Robustez ante instrucciones ambiguas o novedosas.
  - Comparar el sistema híbrido vs. abordajes puramente basados en reglas.
  - Evaluar la calidad de planes generados por CLIPS vs. ChatGPT en diferentes escenarios.

1.5. Estructura del documento

Este documento está organizado en los siguientes capítulos que describen el sistema propuesto para el desarrollo de esta tesis, abarcando el planteamiento, desarrollo, implementación y validación del sistema híbrido de planificación. La estructura es la siguiente:

1. **Capítulo 1: Introducción.** Presenta el contexto, motivación, problemática, hipótesis y objetivos de la investigación, así como la justificación del enfoque híbrido en robótica de servicio doméstico.
2. **Capítulo 2: Antecedentes y estado del arte.** Revisa la evolución de los sistemas basados en reglas en robótica, las características de CLIPS, los enfoques modernos de aprendizaje automático y los sistemas híbridos existentes.

3. **Capítulo 3: Marco teórico y conceptual.** Describe los fundamentos de la planificación jerárquica, los sistemas de producción, los modelos de lenguaje grande (LLMs) y la arquitectura de integración propuesta.
4. **Capítulo 4: Metodología.** Detalla el diseño del sistema híbrido, incluyendo la definición de reglas en CLIPS, la integración con ChatGPT/Qwen, y los mecanismos de planificación dual y validación.
5. **Capítulo 5: Implementación.** Explica los entornos de desarrollo, la configuración técnica, la interfaz con APIs y las pruebas utilizados para validar la integración de los módulos.
6. **Capítulo 6: Escenarios de validación y experimentación.** Presenta el diseño experimental, los escenarios de prueba y las métricas cuantitativas y cualitativas utilizadas para evaluar el sistema.
7. **Capítulo 7: Análisis de resultados.** Compara el rendimiento del sistema híbrido frente al sistema basado solo en reglas, evalúa la efectividad de los LLMs y discute limitaciones y costos computacionales.
8. **Capítulo 8: Discusión.** Interpreta los resultados en relación con los objetivos, analiza ventajas y desventajas del enfoque híbrido, y explora implicaciones éticas y de seguridad.
9. **Capítulo 9: Contribuciones y relevancia.** Destaca la aportación técnica del marco híbrido, su aplicabilidad práctica en distintos sectores y su relevancia académica como benchmark.
10. **Capítulo 10: Conclusiones y trabajo futuro.** Resume los hallazgos principales y propone líneas de investigación futura, como el fine-tuning de LLMs y la mejora de mecanismos de seguridad.

Capítulo 2

Antecedentes y Estado del Arte

Se realiza una revisión comprensiva de la evolución histórica de los sistemas basados en reglas en robótica, analizando aplicaciones tradicionales y limitaciones actuales. Se examinan las características técnicas de CLIPS y se contrastan con enfoques modernos de aprendizaje automático, culminando con el estudio de sistemas híbridos que combinan la predictibilidad de las reglas con la flexibilidad del ML para entornos dinámicos.

2.1. Sistemas Basados en Reglas en Robótica: Historia y Aplicaciones

Los sistemas basados en reglas (Rule-Based Systems, RBS), constituyen uno de los paradigmas más antiguos y consolidados en inteligencia artificial y robótica (**?**). Su origen se remonta a los sistemas expertos de la década de 1970, donde se utilizaban para representar el conocimiento de especialistas humanos en dominios bien delimitados, como el diagnóstico médico o la configuración de sistemas complejos (**?**). En robótica, la adopción de estos sistemas se popularizó en los años 80 y 90, particularmente en entornos industriales estructurados, donde la previsibilidad y seguridad eran prioritarias.

Históricamente, los RBS han sido fundamentales en arquitecturas de control robótico jerárquico, como la propuesta por Brooks (**?**), donde capas de comportamientos reactivos podían ser coordinadas mediante reglas de supresión. Más adelante, motores de inferencia como CLIPS (C Language Integrated Production System), desarrollado por la NASA en 1985, se convirtieron en herramientas estándar para la implementación de sistemas de planificación y toma de decisiones en robots autónomos (**?**). CLIPS

permitió la representación simbólica del conocimiento a través de hechos y reglas, y su ciclo de inferencia reconocer-actuar.ºfreció un marco eficiente para el razonamiento en tiempo real.

En cuanto a aplicaciones, los sistemas basados en reglas han demostrado su utilidad en diversos dominios robóticos:

1. **Robótica industrial:** En cadenas de montaje automatizadas, donde las tareas son repetitivas y el entorno está controlado. Los RBS se utilizan para secuenciar operaciones, gestionar excepciones y garantizar la seguridad de los operarios humanos (**?**).
2. **Robótica de servicio y doméstica:** En tareas como la entrega de objetos, navegación en interiores y asistencia a personas con movilidad reducida.
3. **Robótica espacial y de exploración:** Sistemas como Remote Agent de la NASA emplearon arquitecturas basadas en reglas para la planificación y ejecución autónoma de experimentos en misiones no tripuladas (**?**).
4. **Sistemas híbridos contemporáneos:** Recientemente, los RBS se han integrado con técnicas de aprendizaje automático para compensar sus limitaciones en entornos dinámicos. Por ejemplo, en (**?**) se combina un RBS con un modelo de lenguaje natural para interpretar comandos verbales en tareas de manipulación.

A pesar de la relevancia de enfoques basados en aprendizaje profundo, los sistemas basados en reglas mantienen su relevancia en aplicaciones donde la explicabilidad, verificabilidad y seguridad son críticas (**?**). Su capacidad para representar conocimiento simbólico de forma transparente los hace ideales para entornos regulados o donde se requiere auditoría de las decisiones del robot.

2.2. El Lenguaje CLIPS: Características, Ventajas y Limitaciones

2.3. Enfoques Modernos: Aprendizaje Automático (ML) y Redes Neuronales en Robótica

2.4. Sistemas Híbridos: Combinando la Predictibilidad de las Reglas con la Flexibilidad del ML

Capítulo 3

Marco Teórico y Conceptual

Se presenta el fundamento teórico del sistema propuesto, describiendo arquitecturas de planeación jerárquica y los principios de los sistemas de producción. Se introduce el funcionamiento de los modelos de lenguaje grande y se detalla la integración de traductores de lenguaje natural con sistemas basados en reglas, estableciendo las bases tecnológicas para la implementación del sistema híbrido CLIPS-ChatGPT/Qwen y su uso en la arquitectura ViRoot descrita a continuación (ver Figura **??**).

Arquitectura del Sistema

La arquitectura VIRBOT de Justina se organiza en cuatro capas principales:

- **Capa de Entradas**
  - Procesamiento de datos de sensores internos y externos.
  - Aplicación de técnicas de reconocimiento de patrones.
  - Generación del estado del entorno.
- **Capa de Planificación**
  - Validación mediante gestión del conocimiento.
  - Reconocimiento de situaciones y activación de objetivos.
  - Planificación de secuencias de operaciones físicas.
- **Capa de Gestión del Conocimiento**
  - Mapas del entorno creados con técnicas SLAM.
  - Sistema de localización basado en filtro de Kalman.
  - Sistema basado en reglas CLIPS para representación del conocimiento.
- **Capa de Ejecución**
  - Ejecución y verificación de planes de movimiento.

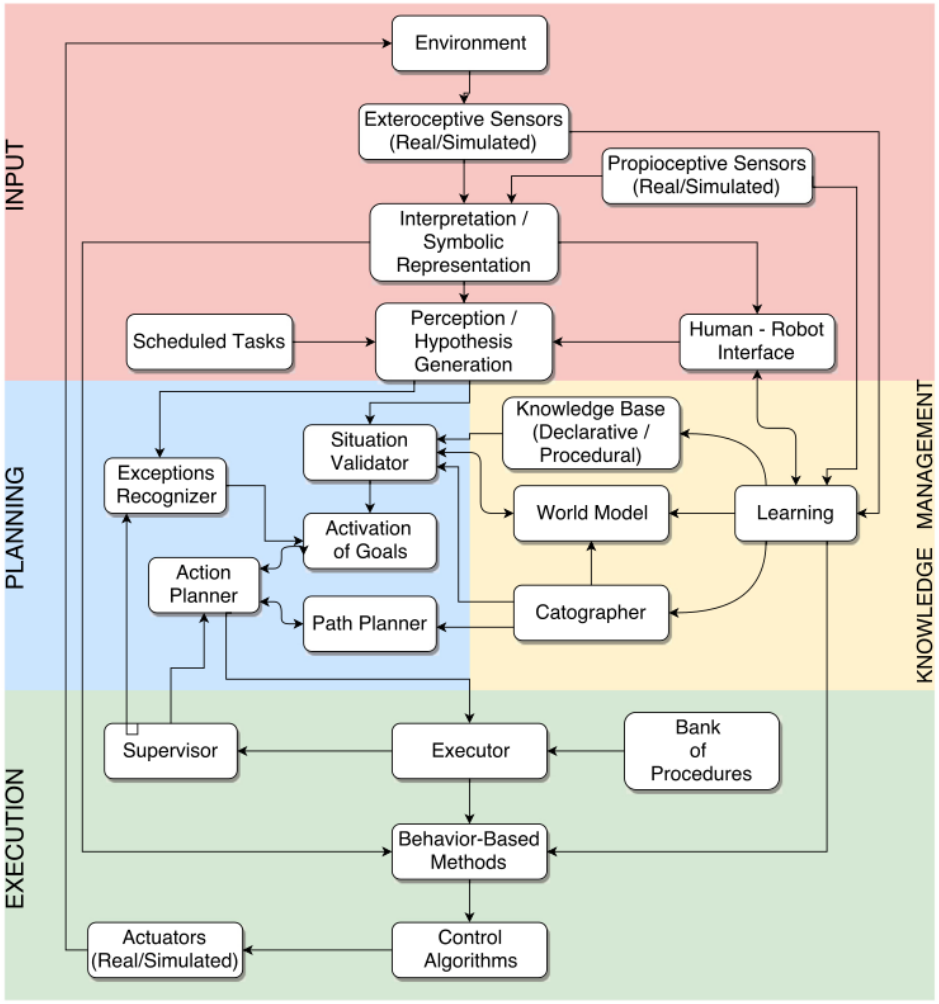

Figura 3.1: Arquitectura ViRoot.

- Procedimientos predefinidos representados como máquinas de estado.
- Integración de procedimientos para generar planes complejos.

3.1. Arquitectura de un Sistema de Planeación de Acciones Jerárquico

Descripción del diseño escalonado del sistema de planificación, donde las decisiones de alto nivel (estrategias) se descomponen en acciones ejecutables de bajo nivel, por ejemplo (”servir la cena”) se descomponen en tareas intermedias (ïr a la cocina”, ”tomar platos”, çolocar en mesa”) y finalmente en acciones primitivas ejecutables por el robot.

3.2. Fundamentos de los Sistemas de Producción (Rule-Based Systems)

Análisis teórico de los sistemas basados en reglas, centrándose en el ciclo de inferencia reconocer-actuarz el algoritmo RETE para emparejamiento eficiente de patrones. Se detalla cómo CLIPS implementa estos conceptos mediante su motor de inferencia y memoria de trabajo.

3.3. Introducción a los Modelos de Lenguaje Grande (LLMs) y ChatGPT/Qwen

Exposición de los principios arquitectónicos de los transformadores y el mecanismo de atención que fundamenta los LLMs. Se contrastan las capacidades de ChatGPT (modelo propietario) frente a Qwen2.5-0.5B (modelo open-source), destacando ventajas computacionales y de personalización para entornos robóticos.

3.4. Integración de Traductores de Lenguaje Natural con Sistemas Basados en Reglas

3.4.1. Utilidad y Función de la Integración

3.4.2. Funcionamiento de la Integración CLIPS-Lenguaje Natural

3.4.3. Descripción de Tecnologías: CLIPS, ChatGPT y Qwen2.5-0.5B

3.5. ChatGPT como Agente de Planificación Autónomo

3.5.1. Capacidades de Planificación de LLMs vs. Sistemas Basados en Reglas

Análisis comparativo de los enfoques de planificación, destacando la rigidez predecible de CLIPS frente a la adaptabilidad contextual de los LLMs.

3.5.2. Arquitectura de Planificación Dual: CLIPS y ChatGPT como Motores Complementarios

3.5.3. Mecanismos de Selección y Validación de Planes

3.5.4. Ventajas y Riesgos de la Planificación con LLMs en Robótica

Capítulo 4

Metodología: Diseño del Sistema Híbrido CLIPS-ChatGPT/Qwen

4.1. Diseño del Sistema Basado en Reglas con CLIPS

4.1.1. Definición del Conjunto de Reglas Jerárquicas

Especificación de las reglas organizadas por niveles de prioridad, donde las reglas de seguridad (evitación de colisiones, gestión de emergencias) tienen máxima prioridad sobre las operativas.

4.1.2. Priorización de Acciones Críticas y Gestión de Emergencias

Diseño de reglas específicas para escenarios de fallo y situaciones críticas, asegurando respuestas predecibles y seguras.

4.1.3. Representación del Conocimiento y Hechos en la Base de Datos de CLIPS

Estructuración del conocimiento del entorno doméstico en hechos CLIPS iniciales que sirven como base para el razonamiento.

Descripción de la base de conocimiento inicial incluye:

- *Topología del entorno:* habitaciones, conexiones, zonas navegables.
- *Taxonomía de objetos:* categorías, subcategorías, propiedades heredables.
- *Relaciones espaciales:* contención, adyacencia, orientación.
- *Capacidades del robot:* acciones posibles, restricciones físicas.

4.2. Integración de ChatGPT/Qwen como Sistema Complementario

4.2.1. Funciones Asignadas al Módulo de Lenguaje Natural

4.2.2. Protocolo de Comunicación entre CLIPS y los Modelos de Lenguaje

4.2.3. Mecanismos de Seguridad y Validación para las Respuestas del LLM

Implementación de verificaciones para asegurar que los planes generados por LLMs cumplen con constraints de seguridad y factibilidad robótica.

4.3. Implementación de Planificación Dual

4.3.1. Diseño del Módulo de Planificación con ChatGPT

4.3.2. Protocolos de Prompting para Generación de Planes Robóticos

4.3.3. Mecanismo de Selección entre Planes CLIPS vs. ChatGPT

4.3.4. Validación y Simulación de Planes Antes de Ejecución

Integración con el Robot Justina

- *Procesamiento de Entrada de Voz.*
- *Ejecución de Planes en el Entorno Físico:*

    - Mecanismos para transformar los planes publicados en los tópicos de resultados en comandos ejecutables por los actuadores del robot (navegación, manipulación de objetos, etc.)
- *Retroalimentación y Aprendizaje Incremental.*

Capítulo 5

Implementación

5.1. Entornos de Desarrollo: Simulación y Plataforma Física

5.2. Implementación del Motor de Reglas en CLIPS

5.3. Desarrollo del Módulo de Integración

5.4. Configuración de la Interfaz con API de OpenAI para ChatGPT o Modelo Qwen Local

5.5. Casos de Prueba para Validar la Interacción entre los Módulos

Capítulo 6

Escenarios de Validación y Experimentación

6.1. Diseño de Experimentos en Entornos Controlados

6.1.1. Escenario 1: Ejecución de Tareas Predefinidas (solo CLIPS)

6.1.2. Escenario 2: Gestión de Órdenes Imprecisas o Novedosas (CLIPS + ChatGPT/Qwen)

6.1.3. Escenario 3: Respuesta a Eventos Inesperados o Fallos

6.1.4. Escenario 4: Planificación Dual para Tareas Complejas (CLIPS vs. ChatGPT)

- Comparativa de eficiencia en generación de planes
- Evaluación de robustez ante escenarios novedosos
- Análisis de seguridad en planes generados por LLMs

6.2. Métricas de Evaluación

6.2.1. Métricas Cuantitativas: Tiempo de Ejecución, Tasa de Éxito, Uso de Recursos Computacionales

6.2.2. Métricas Cualitativas: Robustez, Interpretabilidad y Fluidez en la Interacción Humano-Robot

Capítulo 7

Análisis de Resultados

7.1. Comparativa del Rendimiento del Sistema Solo-CLIPS vs. el Sistema Híbrido

7.2. Evaluación de la Efectividad de ChatGPT/Qwen en las Diferentes Funciones Asignadas

7.3. Discusión de Limitaciones y Errores

7.4. Análisis de la Escalabilidad y el Coste Computacional de la Integración

Capítulo 8

Discusión

8.1. Interpretación de los Resultados en el Contexto de los Objetivos

8.2. Ventajas y Desventajas del Enfoque Híbrido Propuesto

8.3. Implicaciones para la Seguridad y Certificación en Entornos Regulados

8.4. Límites Éticos y Prácticos del Uso de ChatGPT/Qwen en Robótica

Capítulo 9

Contribuciones y Relevancia

9.1. Contribución Técnica: Marco Híbrido Escalable y Documentado

9.2. Relevancia Práctica: Aplicaciones en Salud, Industria y Logística

9.3. Relevancia Académica: Benchmark para Sistemas Rule-Based vs. Híbridos

Capítulo 10

Conclusiones y Trabajo Futuro

10.1. Conclusiones Principales

10.2. Propuestas de Trabajo Futuro

- Fine-tuning de un LLM de código abierto para dominio específico
- Mejora de los mecanismos de seguridad y verificación
- Exploración de arquitecturas de integración más profundas