AI Agents 101: Unlocking Autonomous Intelligence in Finance

Sivakumar Rajendran

TFG AI & ML

Agenda

AI Agents 101: Core Concepts

Understanding What is Agent

Practical Use Cases

Segmenting use cases through the lens of Alogirthm and Domain.

Practical Considerations & Future

What are the barriers that was broke, still exist and to consider

Questions & Discussion

An open forum for insights, clarifications, and exploring potential applications.

Few points before starting...

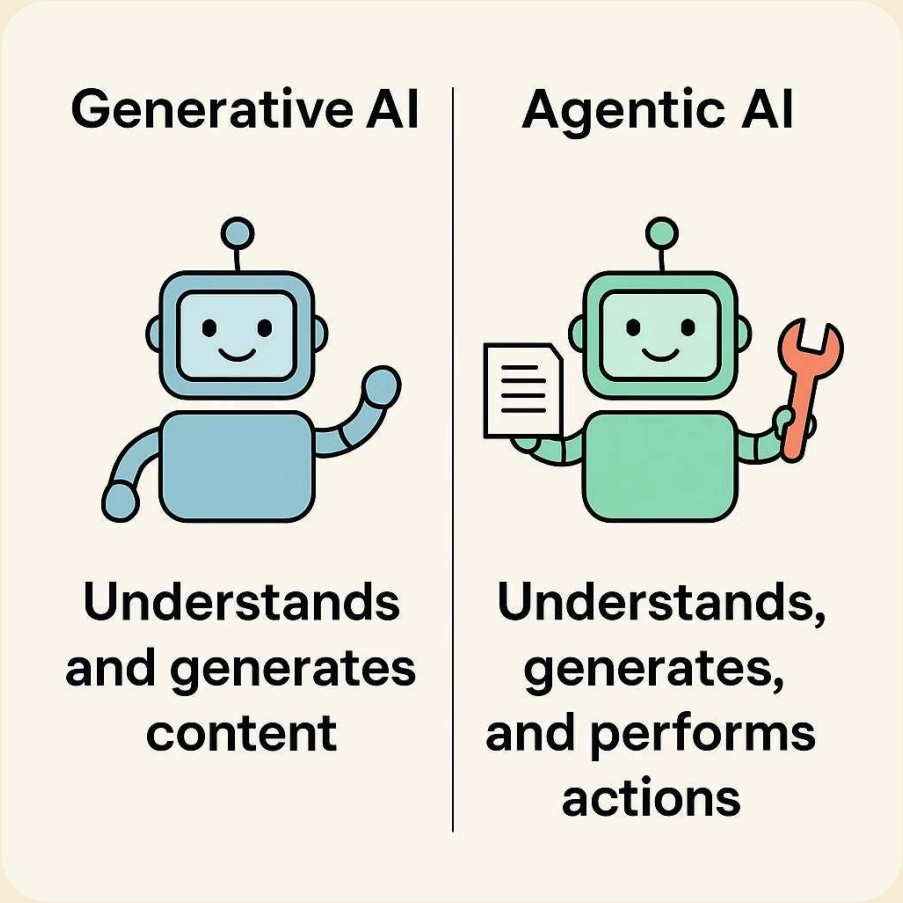
Believe the participants already has good knowledge on LLM and its building blocks

This is 101 level session with a bird-eye view and with reduced altitude in few places. Depends on team requirement, further detailed session can be planned on any of the topics.

AI Agents 101

An artificial intelligence (AI) agent is a system that autonomously performs tasks by designing workflows with available tools.

Reference: **What Are AI Agents? | IBM**



- Traditional programming ↣ Needed code to operate
- Traditional ML ↣ Needed feature engineering
- Deep learning ↣ Needed task-specific training

But when the User needs more

💡 Instead of just **summarizing meeting notes**, could it **create Jira task**

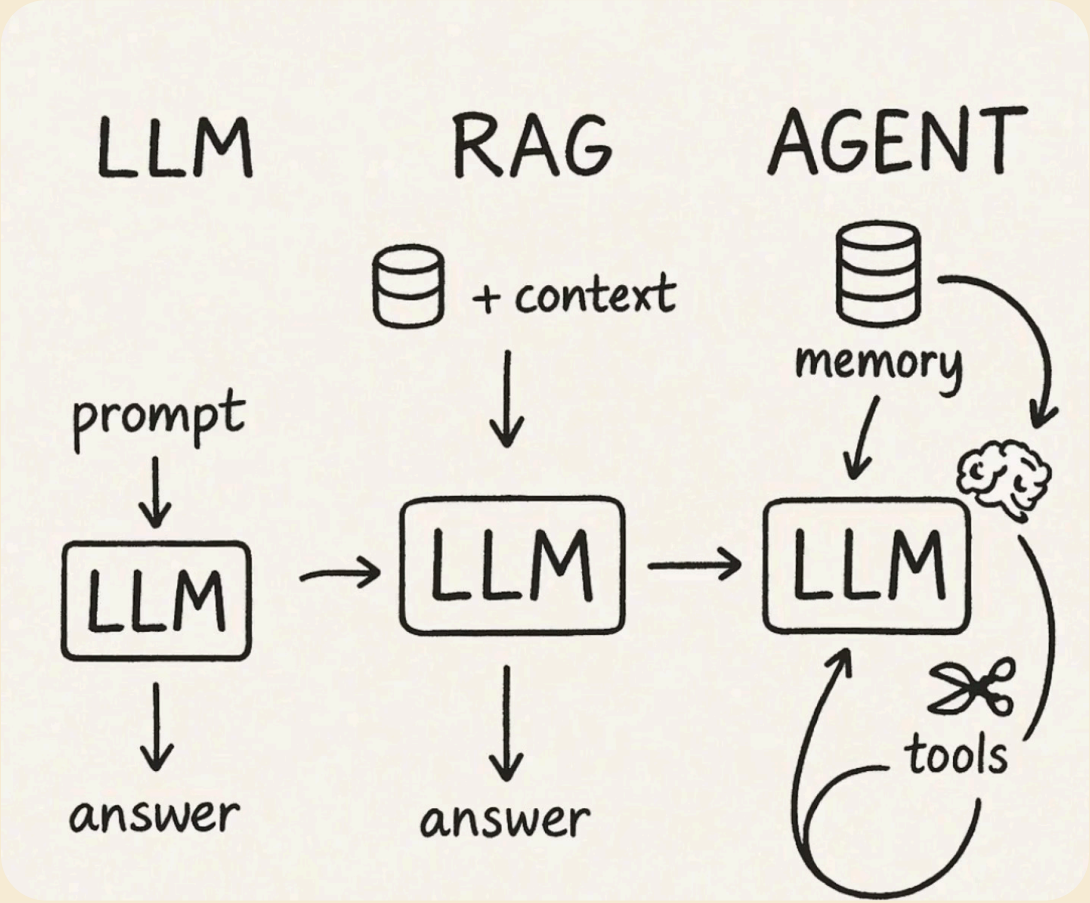
💡 Instead of just **extracting entities from contracts**, could it **auto-update the compliance register**

💡 instead of just **flagging unusual transactions**, could it **freeze the payment, notify the fraud team, and create a case in the risk system**?

THE ANSWER IS

Image: https://github.com/aishwaryanr/awesome-generative-ai-guide/blob/main/free_courses/agentic_ai_crash_course/part1_what_are_ai_agents_anyway.md

LLM vs RAG vs AI Agents



Source: https://www.threads.com/@techno_thinkers/post/DH2XC9vPGMQ/media?utm_source=chatgpt.com

Building blocks of AI Agents

Architecture

Understanding the core components of AI agents is crucial for effective design and implementation. These elements work in concert to enable intelligent, autonomous behavior.

Tools

External functionalities (APIs, databases, models) agents can call upon.

Planning

The ability to strategize and sequence actions to achieve goals.

Memory

Persistent storage of past experiences, observations, and learnings.

State

The agent's current internal understanding of its environment and objectives.

Tools https://github.com/aishwaryanr/awesome-generative-ai-guide/blob/main/free_courses/agentic_ai_crash_course/part3_what_are_tools_in_ai.md

Planning https://github.com/aishwaryanr/awesome-generative-ai-guide/blob/main/free_courses/agentic_ai_crash_course/part6_planning_in_agents_reasoning_models.md

Memory https://github.com/aishwaryanr/awesome-generative-ai-guide/blob/main/free_courses/agentic_ai_crash_course/part7_memory_in_agents.md

Use cases

Use case by Algorithms

Statistical

Purpose: Explain/forecast with assumptions

Example Techniques: Regression, ARIMA

Sample Banking Use Cases: Credit risk scoring, budget forecasting

ML

Purpose: Predict from data patterns

Example Techniques: Random Forest, XGBoost

Sample Banking Use Cases: Customer churn, fraud detection

NLP

Purpose: Understand unstructured text

Example Techniques: BERT, Text Classification

Sample Banking Use Cases: Chatbots, complaint classification

RL

Purpose: Learn via interaction

Example Techniques: Q-learning, Bandits

Sample Banking Use Cases: ATM refill, personalization

Rule-Based

Purpose: Automate clear logic

Example Techniques: IF-THEN, flowcharts

Sample Banking Use Cases: AML flags, data validation

LLM, Agents

<Intentionally left it blank for discussion>

10

Use case by Functional Area

Operations

Document classification, ticket routing using NLP

Retail Banking

Personal finance advisory, churn prediction, product recommendations

Treasury

Forecasting liquidity, stress testing under macroeconomic variables

Corporate Banking

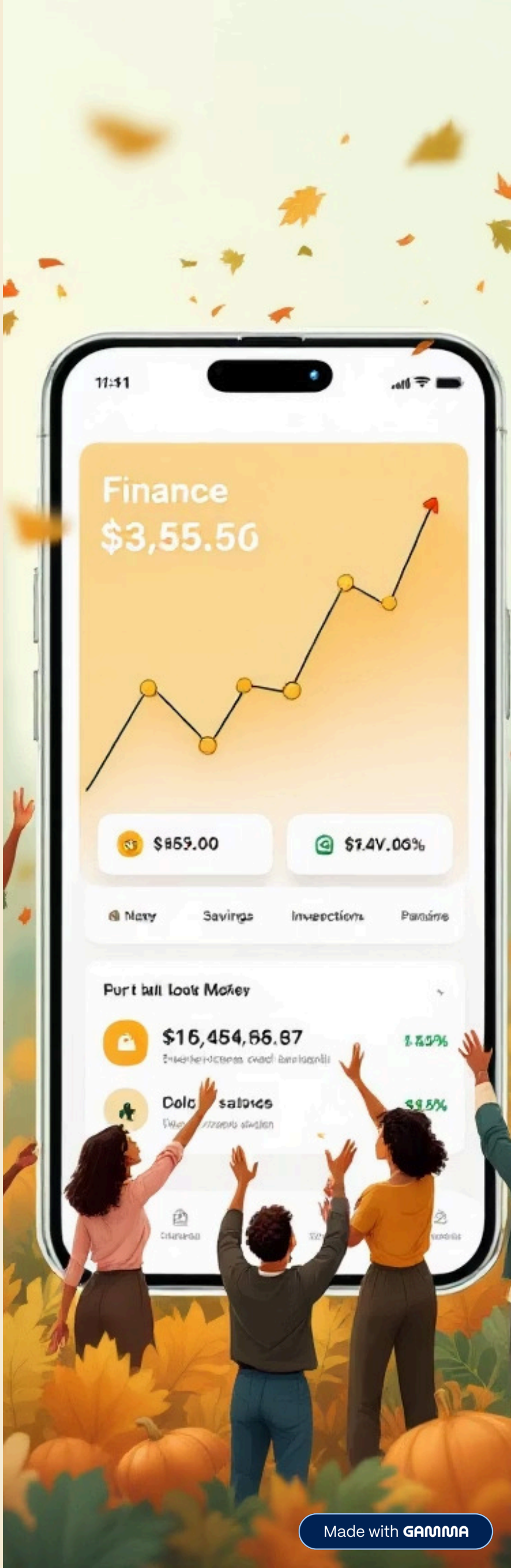
ISupply chain finance risk scoring, credit exposure modeling

Marketing

Customer segmentation, campaign targeting optimization

Risk & Compliance

Fraud detection, Anti-Money Laundering (AML), regulatory monitoring



Fraud Detection & Security

Use Case	Description	Source
Adaptive fraud checkout	AI-powered real-time risk scoring during transactions	TickPick regained $3M
Real-time anomaly detection	ML monitors transactions for fraud patterns	Detect suspicious behavior
AML monitoring	AI flags money-laundering behaviors	AML use cases
Biometric auth	Face/voice match for login/transactions	Fair AI use cases
Transaction fraud AI	Multi-model monitoring reduces false positives	DigitalDefynd case studies

Credit & Lending

Use Case	Description	Source
AI loan underwriting	Uses transaction data to assess borrower risk	**Abound's AI loans**
Credit scoring ML	Improves fairness and accuracy with XAI	**Explainable credit scoring**
Instant credit decisions	GenAI-driven loan approvals	**GenAI use cases**
Debt-collection bots	Personalized repayment recommendations	**GenAI examples**
Underwriting for thin files	ML assesses borrowers with limited credit history	**Upstart/ZestFinance on wiki**

Customer Experience & Chatbots

Use Case	Description	Source
AI-powered chatbots	24/7 support across channels	Commonwealth Bank AI chat
Virtual financial advisor	GenAI provides budgeting/spending advice	GenAI in banking
Complaint/ticket routing	NLP classifies customer issues	DigitalDefynd AI case studies
Document search via app	Conversational query across transactions	Bunq’s Finn
Research chatbots for advisors	Internal LLM tool for market insights	Morgan Stanley “AskResearchGPT”

Analytics & Risk Management

Use Case	Description	Source
Credit risk forecasting	ML predicts default and NPA trends	GenAI banking use cases
Market risk analysis	AI simulates scenarios for VaR/P&L	DigitalDefynd analytics
Liquidity forecasting	AI projects cash requirements dynamically	Citizens Bank trends
Portfolio optimization	RL-based asset allocation models	Applications of AI wiki
Continuous auditing	Auto-detect anomalies in financial logs	AI in fraud detection wiki

Operations & Automation

Use Case	Description	Source
Digital employees	AI “agents” automate payments and ops	BNY Mellon digital workers
Document classification	NLP categorizes KYC/loan files	DigitalDefynd case studies
Back-office automation	AI handles compliance and data tasks	HSBC AI bots pilot
Code-review bots	AI assists in coding, docs, memos	JPMorgan code AI
Regulatory summarization	Generative AI digests compliance documents	Citi regulation bot

Advantages

AI agents integrate seamlessly into existing financial ecosystems, driving automation and intelligence across operations.

Seamless Integration

Connects via APIs and event triggers, minimizing disruption.

Reduced Latency

Autonomous decisions cut operational costs and response times.

Multi-Agent Collaboration

Enables complex task decomposition and orchestration for efficiency.

Continuous Learning

Adapts to market shifts and evolving regulations for ongoing relevance.

4

Enhanced Scalability

Boosts responsiveness in high-stakes, data-intensive environments.

Tools for Development

Leading AI Agent Frameworks

Several robust frameworks are available to facilitate the development and deployment of AI agents, each offering unique strengths.

LangChain

A versatile framework for developing applications powered by language models, enabling chaining of LLMs with other components.

Google ADK

Agent Development Kit (ADK) is a flexible and modular framework for **developing and deploying AI agents**. While optimized for Gemini and the Google ecosystem,

Microsoft Autogen

AutoGen is an open-source programming framework for building AI agents and facilitating cooperation among multiple agents to solve tasks.

Alibaba

Alibaba offers several agent frameworks, including Qwen-Agent, a Python framework for building applications with Qwen LLMs, Spring AI Alibaba, a Java framework for creating enterprise-level agents within the Spring ecosystem, and the more comprehensive WebAgent framework, which integrates multiple projects for advanced AI research in web contexts.

Safeguards

Key challenges in AI Agents Implementation

Strategic Approach

Design Considerations for AI Agents

Building effective AI agents requires careful planning and adherence to best practices to ensure reliability, transparency, and adaptability.

01

Define Clear Goals & Boundaries

Crucial for preventing unintended behaviors and maintaining focus.

02

Modular Architecture

Supports extensibility and facilitates multi-agent collaboration for complex tasks.

03

Robust Error Handling

Implement comprehensive fallback strategies to ensure reliability and resilience.

04

Transparent Decision-Making

Prioritize explainability to build trust and meet compliance requirements.

05

Continuous Monitoring & Iteration

Establish observability and improvement cycles for ongoing optimization.

Implementing AI agents effectively is a multi-faceted endeavour, fraught with technical, operational, and ethical complexities. Our analysis of recent industry reports and academic papers reveals that these challenges typically fall into four primary categories: Technical Hurdles, Operational Complexities, Ethical & Governance Concerns, and Human-Agent Collaboration Dynamics. Understanding these distinctions is crucial for developing targeted strategies and allocating resources judiciously.

Technical Hurdles

Challenges related to the core AI capabilities, infrastructure, and integration.

Operational Complexities

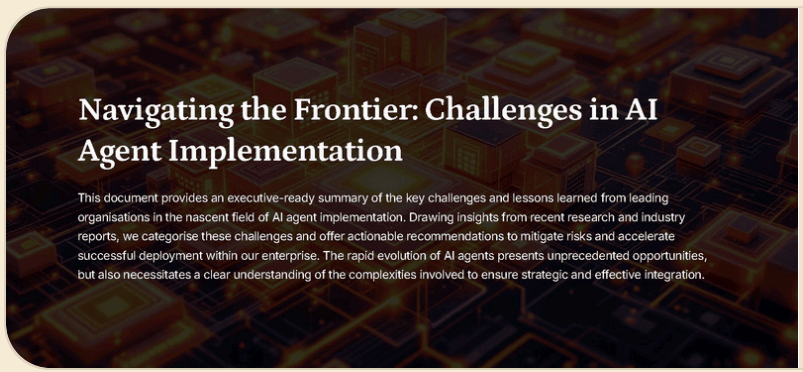
Issues arising from the practical deployment, maintenance, and scaling of agents.

Ethical & Governance Concerns

Risks associated with responsible AI use, bias, transparency, and regulation.

Human-Agent Collaboration Dynamics

Difficulties in designing effective interactions between humans and AI agents.



PDF 文件

Navigating-the-Frontier-Challenges-in-AI-Agent-Implementation.pdf

1.9 MB

Application

Building an AI Agent

A good collection of capstone AI Agent projects that details design, approach, eval and more

areganti on Notion

Enterprise AI Projects Showcase ...

Here's a list of projects that were built by our students as part of the...

prise AI Projects Sho

Notion

Learning Roadmap

Step 1: Building Blocks of AI Agents

Agent Role & Goal	Define clear, measurable objectives	Goal specification, policy functions	ProjectPro 2025 AI Agent Roadmap
Perception	Input modalities: text, vision, audio, tabular	NLP, CV, multimodal learning	Stanford "Generative Agents" paper
Reasoning & Planning	Multi-turn reasoning, decision-making	Reinforcement learning, planning algos	KDNuggets Agentic AI Roadmap
Action & Execution	Output generation: API calls, natural language	LangChain, AutoGen, tool integration	GitHub jitender-insights 2025

Mastering these fundamental components is crucial for any data scientist looking to transition into AI Agent development. Each block represents a distinct area of expertise that, when combined, forms a cohesive and intelligent system.

Step 2: AI Agent Design & Architecture

Modular Design	Decouple perception, reasoning, action modules	LangChain, LangGraph, AutoGen	jitender-insights GitHub 2025
Multi-Agent Systems	Coordination & communication between agents	CrewAI, OpenAI Assistants API	Microsoft Research "Multi-Agent Collaboration"
Memory & Context	Long-term state, context management	Vector DBs (Pinecone, Weaviate), RAG	Medium 2025 AI Agent Roadmap
Scalability & APIs	Backend APIs for deployment & interaction	FastAPI, Docker, Cloud Functions	Hasanul Mukit Dev.to 2025

Designing robust and scalable AI agents requires thoughtful architectural decisions, particularly when dealing with complex tasks, multiple agents, and persistent memory.

Step 3: Monitoring & Observability for AI Agents

Performance Metrics	Latency, throughput, resource usage	Prometheus, Grafana, custom logs	Dev.to AI Engineering Stack 2025
Behavioral Monitoring	Track agent decisions, error rates, anomalies	Logging frameworks, audit trails	jitender-insights GitHub 2025
Health Checks	Automated alerts on failures or degraded ops	CI/CD pipelines, automated tests	Hasanul Mukit Dev.to 2025
User Feedback Loop	Collect user satisfaction, fairness metrics	Custom evals, A/B testing	ProjectPro AI Agent Roadmap

Once deployed, AI agents require continuous monitoring and robust observability to ensure their reliability, ethical operation, and consistent performance in dynamic environments.

Q&A