

Sumário

- Prefácio
- CAPÍTULO 1: Introdução aos agentes
- Definindo agentes de IA
- A revolução do pré-treinamento
- Tipos de agentes
- Seleção de modelo
- De operações síncronas para operações assíncronas
- Aplicações práticas e casos de uso
- Fluxos de trabalho e agentes
- Princípios para a construção de sistemas agênticos eficazes
- Organizando para o sucesso na construção de sistemas agênticos
- Frameworks agênticos
- LangGraph
- AutoGen
- CrewAI
- Kit de Desenvolvimento de Software (SDK) para agentes da OpenAI
- Conclusão
- CAPÍTULO 2: Projetando sistemas de agentes
- Nosso primeiro sistema de agentes
- Componentes essenciais de sistemas de agentes
- Seleção do modelo
- Ferramentas
- Desenvolvendo capacidades para tarefas específicas
- Integração e modularidade de ferramentas
- Memória (histórico de interações passadas)
- Memória de curto prazo (histórico da sessão)
- Memória de longo prazo (base de conhecimento persistente)
- Gestão e recuperação da memória
- Orquestração
- Trade-offs de projeto
- Desempenho: trade-offs entre velocidade e precisão
- Escalabilidade: projetar escalabilidade para sistemas de agentes
- Confiabilidade: garantindo comportamento robusto e consistente do agente
- Custos: equilibrando desempenho e despesas
- Padrões de projeto de arquitetura
- Arquiteturas de agente único
- Arquiteturas multiagentes: colaboração, paralelismo e coordenação
- Melhores práticas
- Projeto iterativo
- Estratégia de avaliação
- Testes no mundo real
- Conclusão
- CAPÍTULO 3: Projeto de UX para sistemas agênticos
- Modalidades de interação
- Baseada em texto
- Interfaces gráficas
- Interfaces de fala e voz
- Interfaces baseadas em vídeo

- Combinando modalidades para experiências perfeitas
- O controle deslizante de autonomia
- Experiências de agentes síncronos versus assíncronos
- Princípios de projeto para experiências síncronas
- Princípios de projeto para experiências assíncronas
- Encontrando o equilíbrio entre o comportamento proativo e intrusivo do agente
- Retenção e continuidade do contexto
- Manter o estado ao longo das interações
- Personalização e adaptabilidade
- Comunicando as capacidades do agente
- Comunicando confiança e incerteza
- Solicitar orientação e contribuições dos usuários
- Falhar de forma controlada
- Confiança no projeto de interação
- Conclusão
- CAPÍTULO 4: Uso de ferramentas
- Fundamentos do LangChain
- Ferramentas locais
- Ferramentas baseadas em API
- Ferramentas plug-in
- Protocolo de Contexto de Modelo (MCP)
- Ferramentas com estado
- Desenvolvimento automatizado de ferramentas
- Modelos de fundação como criadores de ferramentas
- Geração de código em tempo real
- Configuração de uso da ferramenta
- Conclusão
- CAPÍTULO 5: Orquestração
- Tipos de agentes
- Agentes de reflexo
- Agentes ReAct
- Agentes de planejamento e execução
- Agentes de decomposição de consultas
- Agentes de reflexão
- Agentes de pesquisa profunda
- Seleção de ferramentas
- Seleção padrão de ferramentas
- Seleção semântica de ferramentas
- Seleção hierárquica de ferramentas
- Execução de ferramentas
- Topologias de ferramentas
- Execução de ferramenta única
- Execução paralela de ferramentas
- Cadeias (Chains)
- Grafos
- Engenharia de contexto
- Conclusão
- CAPÍTULO 6: Conhecimento e memória
- Abordagens fundamentais da memória
- Gerenciando janelas de contexto

- Busca tradicional de texto completo
- Memória semântica e armazenamentos vetoriais
- Introdução à busca semântica
- Implementando memória semântica com armazenamentos vetoriais
- Geração Aumentada por Recuperação (RAG)
- Memória de experiência semântica
- GraphRAG
- Utilizando grafos de conhecimento
- Construindo grafos de conhecimento
- Potencial e riscos dos grafos de conhecimento dinâmicos
- Tomar notas
- Conclusão
- CAPÍTULO 7: Aprendizado em sistemas agênticos
- Aprendizado não paramétrico
- Aprendizado não paramétrico por exemplos
- Reflexion
- Aprendizado experiencial
- Aprendizado paramétrico: ajuste fino
- Ajuste fino de grandes modelos de fundação
- O potencial dos modelos pequenos
- Ajuste fino supervisionado
- Otimização direta de preferências
- Aprendizado por reforço com recompensas verificáveis
- Conclusão
- CAPÍTULO 8: De agente único a múltiplos agentes
- De quantos agentes eu preciso?
- Cenários de agente único
- Cenários multiagentes
- Enxames
- Princípios para adicionar agentes
- Coordenação multiagente
- Coordenação democrática
- Coordenação gerencial
- Coordenação hierárquica
- Abordagens ator-crítico
- Projeto automatizado de sistemas de agentes
- Técnicas de comunicação
- Comunicação local versus distribuída
- Protocolo agente-para-agente
- Brokers de mensagens e barramento de eventos
- Frameworks de atores: Ray, Orleans e Akka
- Mecanismos de orquestração e fluxo de trabalho
- Gerenciando o estado e a persistência
- Conclusão
- CAPÍTULO 9: Validação e medição
- Medindo sistemas agênticos
- A medição é a pedra angular
- Integrando a avaliação ao ciclo de vida do desenvolvimento
- Criar e escalar conjuntos de avaliação
- Avaliação de componentes

- Ferramentas de avaliação
- Planejamento da avaliação
- Avaliando a memória
- Avaliando o aprendizado
- Avaliação holística
- Desempenho em cenários de ponta a ponta
- Consistência
- Coerência
- Alucinação
- Lidando com entradas inesperadas
- Preparando para a implantação
- Conclusão
- CAPÍTULO 10: Monitoramento em produção
- Monitorar é uma forma de aprender
- Pilhas de monitoramento
- Grafana com OpenTelemetry, Loki e Tempo
- Pilha ELK (Elasticsearch, Logstash/Fluentd, Kibana)
- Arize Phoenix
- SigNoz
- Langfuse
- Escolhendo a pilha certa
- Instrumentação OTel
- Visualização e alertas
- Padrões de monitoramento
- Modo sombra (shadow mode)
- Implantações canário
- Coleta de rastreamento de regressão
- Agentes com autocorreção
- Feedback do usuário como sinal de observabilidade
- Mudanças na distribuição
- Responsabilidade pelas métricas e governança interfuncional
- Conclusão
- CAPÍTULO 11: Ciclos de melhoria
- Pipelines de feedback
- Detecção automatizada de problemas e análise da causa raiz
- Revisão com intervenção humana
- Refinamento de ferramentas e prompts
- Agregando e priorizando melhorias
- Experimentação
- Implantações em sombra
- Testes A/B
- Bandits Bayesianos
- Aprendizado contínuo
- Aprendizado contextual
- Retreinamento offline
- Conclusão
- CAPÍTULO 12: Protegendo sistemas agênticos
- Riscos exclusivos dos sistemas agênticos
- Vetores de ameaça emergentes
- Protegendo modelos de fundação

- Técnicas defensivas
- Red Teaming
- Modelagem de ameaças com MAESTRO
- Proteção de dados em sistemas agênticos
- Privacidade e criptografia de dados
- Proveniência e integridade dos dados
- Tratamento de dados sensíveis
- Garantindo a segurança dos agentes
- Medidas de segurança
- Proteções contra ameaças externas
- Proteções contra falhas internas
- Conclusão
- CAPÍTULO 13: Colaboração Humano-Agente
- Papéis e autonomia
- A mudança do papel dos humanos em sistemas de agentes
- Alinhando os stakeholders e impulsionando a adoção
- Escalando a colaboração
- Escopo do agente e papéis organizacionais
- Memória compartilhada e limites de contexto
- Confiança, governança e conformidade
- Ciclo de vida da confiança
- Frameworks de responsabilização
- Projeto de escalonamento e supervisão
- Privacidade e conformidade regulatória
- Conclusão: o futuro das equipes humano-agente
- Glossário
- Índice remissivo