# Russell Ro

rro@berkeley.edu russro.com LinkedIn Github

## Education

**University of California, Berkeley** **2022 – Exp. 2027**
*Ph.D. | Computer Science*
- Fully funded by **NSF Graduate Research Fellowship Program (GRFP)**.

**University of California, San Diego** **2018 – 2022**
*B.S. | Electrical Engineering (emphasis)*
- Full-ride scholarship from **Jacobs School Scholarship**. Approximately 10 recipients every year.

## Experience

**University of California, San Francisco** **May 2023 – Present**
*Researcher* *San Francisco, CA*
- Thesis spans two arms: **applied** (agentic systems and LLMs for clinical trial eligibility analysis and literature–trial matching) and **basic research** (representation learning on model zoos for model selection and LLM profiling; distillation detection next).
- Building clintriaLM: LLM + retrieval over **500K+ trials** for eligibility analysis, literature–trial matching, and criteria evolution.
- Developed RECITE, an evidence-guided eligibility criteria revision benchmark; **presented at KDD 2026 AI4Sciences**.
- Built BULLPEN, model-zoo embeddings for sample-efficient LLM profiling and model selection; **ICLR 2027 (submitted)**.
- Contributed to research on LLM vulnerabilities in clinical settings; pushed adversarial entity detection from 10% to **17%** via novel **embedding sampling**.

**FenixCommerce** **Aug 2025 – Present**
*ML Engineer (Consultant)* *San Jose, CA*
- Built the company's agentic platform on **AWS** (**Bedrock**, **Lambda**, **EC2**); all employees use it for internal ops and client-facing data analysis via **Slack** as the chat interface.
- Developed an ML system for delivery time prediction to improve shipping accuracy and transparency for ecommerce clients.
- Built automated retraining and redeployment pipelines on **AWS**, triggered by business KPIs to keep models current.
- Applied AutoML practices and causal inference methods to scale ML prediction capabilities across ecommerce logistics products.

**Novartis** **Oct 2020 – Jun 2022**
*Electrical Engineer (Intern)* *San Diego, CA*
- Led a 96-channel automated drug screening system (prev: 8-channel) integrated with Novartis' HTS pipeline; **12x throughput**.
- Collaborated with Cardiovascular Research and Data Science teams to enhance a computer vision-based drug discovery platform [article], [tech details].
- Built low-cost signal switching hardware ($2000 → $100) and automated data acquisition/analysis in **Python** and LabVIEW, achieving a $\mathbf{10^6}\times$ speedup (seconds → microseconds).

## Publications, Patents & Talks

From the Zoo to the BULLPEN: Sample-Efficient LLM Profiling via Multi-Channel Model Embeddings 2026
*Under review, International Conference on Learning Representations (ICLR 2027)*

RECITE: Revising Eligibility Criteria Incorporating Textual Evidence Aug 2026
*Knowledge Discovery and Data Mining (KDD 2026), AI4Sciences Track*

Assessing biomedical knowledge robustness in large language models by query-efficient sampling attacks Dec 2024
*Transactions on Machine Learning Research (TMLR)*

Agentic System for Analyzing Clinical Trial Eligibility 2026
*U.S. Provisional Patent Application (UCSF-943PRV)*

eval ∝ d: Evaluating Evals Before They Dictate Deployment Decisions Oct 2026
*Invited Talk, AI Decisioning Working Group*

## Projects

**Multi-Agent Ops Platform** | *Claude Code, Python, Qdrant, Ollama, Telegram*
- Built and run **6 always-on LLM agents** (bridge, manager, and watchdog processes each) with a shared knowledge base, vector memory (Qdrant + local embeddings), cross-machine coordination, and self-healing restarts.

**Custom Game Controllers** | *Arduino, C++, Python, Embedded*
- Turned toy wheels, toasters, and webcam pose estimation (e.g., the viral '67' hand motion) into virtual Xbox gamepads via Arduino (C++), Python, and MediaPipe; up to 4-player local multiplayer. Demoed at **Open Sauce 2026** [repo].

## Skills & Service

**Languages**: Python, SQL, Bash (Linux)
**LLMs/Agents**: LLM Agents, RAG, MCP, Claude/OpenAI APIs, AWS Bedrock, Ollama, Question Answering, Embeddings
**Machine Learning**: PyTorch, Hugging Face, Scikit-learn; Representation Learning, Model Zoos, Meta-Learning, Computer Vision
**Data/Cloud**: Pandas/Polars, PostgreSQL (pgvector), Qdrant, AWS, Docker, Modal, Oracle Cloud (OCI)
**Service**: Reviewer, International Conference on Learning Representations (ICLR 2027)