Mathematics of Learning:
Mathematical Interpretations of Machine Learning Algorithms.
*Because **JUST TRUST the MODEL** isn't Good Enough.*

Prepared By: Siman Giri

Summer, 2025

1 Basic Course Information.

- **Instructor: Siman Giri {siman.giri@herald}.**
- **Course Code: HCAI5TML01.**
- **Lectures: TBA.**
- **Office Hours: On Demand and By Appointment.**
- **Quick Links and Navigation:**
  - **Course Logistics and Learning Outcomes.**
  - **Final Grading.**
  - **Getting Help.**
  - **Academic Integrity Policies.**
  - **Approximate Schedule.**

2 Course Logistics.

2.1 Course Introduction:

This course is offered as part of the **Theoretical Initiative** at the **Center for AI, Herald College**, and provides a mathematically rigorous introduction to the foundations of machine learning. It is designed for students who wish to engage deeply with the theoretical principles that underpin the process of learning from data.

The course develops a strong conceptual and analytical framework for understanding modern learning algorithms. Topics include **empirical risk minimization**, **PAC learning**, **VC dimension**, **Rademacher complexity**, **information-theoretic measures**, and **optimization techniques**. These foundational tools enable students to reason about the performance, reliability, and inherent limitations of learning systems beyond empirical heuristics.

Although the focus is not on immediate application or implementation, the course cultivates essential intuition and theoretical fluency—what might be called the "arrows in your quiver"—that support advanced study and innovation in machine learning, artificial intelligence, and data science.

Students will be expected to engage with formal derivations, proofs, and critical theoretical discussions. The emphasis is on understanding the **why** behind learning algorithms, rather than merely the **how**. While rooted in advanced theory, the course has been thoughtfully designed to be accessible to undergraduate students with a strong foundation in mathematics, statistics, or computer science. It builds each topic incrementally, making it an ideal stepping stone toward graduate-level coursework or research in machine learning.

2.2 Pre-requisites:

Must have obtained passing grades on following Modules:

- Introduction to Python Programming - Level - 4.
- Computational Mathematics - Level - 4.
- 5CS037 - Concepts and Technologies of AI - Level - 5.

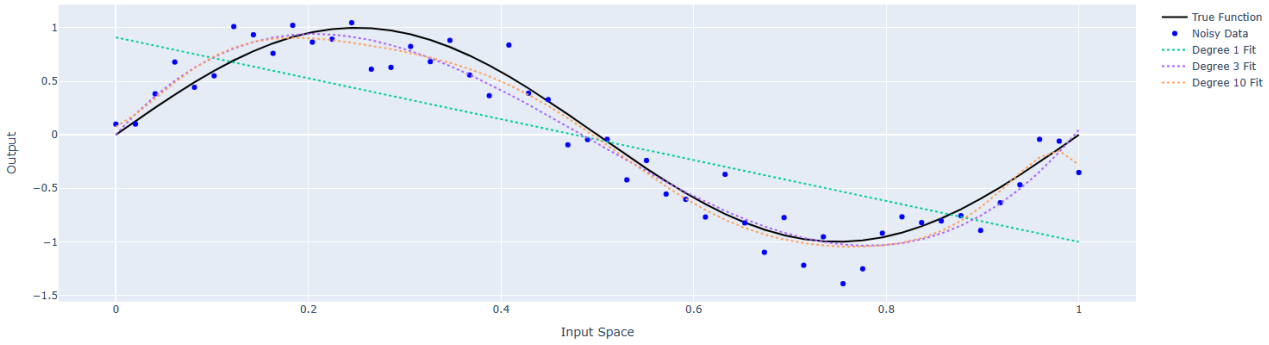

Figure 1: Bias - Variance Tradeoff.

2.3 Recommended Reading:

There are no required textbooks for this course. Lecture notes, annotated readings, and worksheets will provide comprehensive coverage of the material. However, students seeking a deeper or broader understanding may find the following texts helpful:

1. **Understanding Machine Learning: From Theory to Algorithms**
   Shai Shalev-Shwartz and Shai Ben-David
   A rigorous and accessible introduction to the theoretical foundations of machine learning, including formal learning models, VC dimension, and algorithm analysis.
   [**Free PDF**] `https://www.cs.huji.ac.il/~shais/UnderstandingMachineLearning/`

2. **Foundations of Machine Learning**
   Mehryar Mohri, Afshin Rostamizadeh, and Ameet Talwalkar
   Covers core concepts in statistical learning theory, generalization bounds, stability, and regularization, with an emphasis on mathematical rigor.

3. **Information Theory, Inference, and Learning Algorithms**
   David J.C. MacKay
   Blends information theory, probabilistic modeling, and machine learning in a mathematically rich yet engaging style.
   [**Free PDF**] `https://www.inference.org.uk/mackay/itila/`

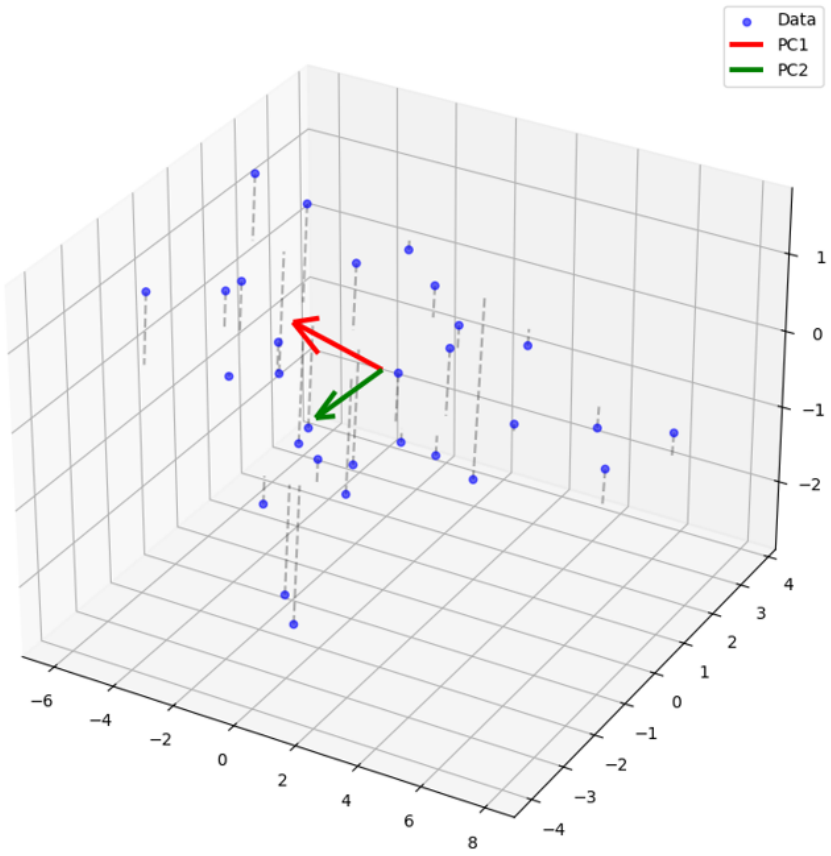

Figure 2: Vector Projections in Principal Component Analysis.

2.4 Learning Outcomes:

Upon successful completion of this course, students will be able to:

1. Understand and Apply Theoretical Foundations of Learning:
   - Explain the principles of Empirical Risk Minimization (ERM), Probably Approximately Correct (PAC) learning, and Statistical Learning Theory.
   - Analyze the learnability of hypothesis classes using concepts like VC dimension and Rademacher complexity.
2. Analyze Generalization and Regularization in Machine Learning:
   - Derive and interpret generalization bounds using concentration inequalities and complexity measures.
   - Understand and apply regularization methods to mitigate overfitting and improve model robustness.
3. Explore the Role of Optimization and Information Theory:
   - Study gradient-based optimization methods and convergence guarantees in the context of learning algorithms.
   - Utilize information-theoretic tools (e.g., entropy, KL divergence) to understand uncertainty and capacity in learning.
4. Engage Critically with Advanced Learning Concepts:
   - Evaluate the theoretical assumptions and limitations underlying commonly used machine learning algorithms.
   - Communicate complex mathematical ideas clearly through formal proofs, structured derivations, and logical reasoning.

3 Final Grading:

The assessment for this course is structured to reinforce consistent engagement with theoretical concepts, rigorous problem solving, and the development of deep analytical insights. Evaluation is based on weekly assignments, participation, and a culminating final paper or project. The grading breakdown is as follows:

- 50% **Weekly Worksheets and Problem Sets:** Students will complete weekly assignments that include derivations, theoretical exercises, and conceptual questions designed to reinforce the mathematical foundations covered in lectures.
- 10% **Participation:** Active involvement in class discussions, whiteboard problem solving, and critical questioning during sessions. This also includes in-class peer reviews and brief oral check-ins on learning progress. Please note that participation cannot be retroactively made up.
- 40% **Final Project or Paper:** Students will either (a) write a critical paper exploring an advanced topic in learning theory or (b) undertake a theoretical project analyzing a learning algorithm from a mathematical standpoint. Emphasis will be placed on clarity of exposition, correctness of arguments, and depth of theoretical insight.

This grading scheme is intended to encourage sustained theoretical engagement, support mastery of foundational principles, and foster the ability to articulate and critique core ideas in machine learning theory.

Caution: These plans are tentative and subject to change. Final confirmation will be provided.

4 Getting Help:

The preferred method of communication for course-related inquiries is via email, ensuring a timely response. For urgent matters or recommendations, students are encouraged to meet with the teaching staff or the designated teaching assistant (TA) during their office hours.

4.1 About Office Hours:

The teaching staff holds weekly office hours to assist students with course-related matters. Students can obtain details of office hours time by contacting their **designated instructor**, the **Student Support Desk (SSD)**, or the **Personal Academic Tutor (PAT) office**. Meetings outside of scheduled office hours are strictly by prior **appointment only**.

5 Academic Integrity Policies:

The Academic Integrity Policy of this course must be strictly adhered to when completing assignments and participating in discussions.**Please - Read this carefully.**

5.1 Collaboration among Students:

Collaboration among students is intended to **facilitate deeper learning and comprehension, rather than to circumvent the learning process**. Engaging in group discussions and collaborative study of course materials is strongly encouraged. Students may seek clarification and conceptual guidance from their peers to enhance their understanding of the subject matter required for completing assignments. However, such collaboration must support independent learning rather than substitute for individual effort. **The direct reproduction of any material from other students or external sources is strictly prohibited**. All submitted work must be the sole effort of each student.
All of the following activities will be considered cheating:

1. **Sharing or Copying code, files or answers:** whether through direct copying, retyping or using online sources e.g. Stack-overflow Git-hub without proper attribution.

2. **Submitting work that is not original:** including using external code or code generated by LLMs, with intention of passing off such work as the student's own.

3. **Copying answers** to quizzes, assignments, or projects from another individual or from any published or unpublished written or electronic sources.

4. **Collaborating with others** on individual assignments, quizzes or project without explicit permission from the instructor.

5.2 Duty to Protect One's Work:

Students are responsible for safeguarding their work against unauthorized access, copying, or misuse by others.If a student's work is copied by another student, both parties will be held accountable for violating course policies. This applies regardless of whether the original author explicitly permitted the copying or failed to take adequate precautions to prevent it. If identical or highly similar work is submitted by multiple students, all involved will face academic penalties.
To uphold academic integrity and protect future students, solutions to assignments must not be shared publicly, either during the course or after its completion.

5.3 Duty to Give Viva:

It is **student's responsibility to attend viva** examinations at the scheduled time determined by the instructor. Failure to comply with this requirement may result in academic penalties.

5.4 Plagiarism and AI - Generated Content:

Plagiarism, including the use of AI-generated content without proper attribution, constitutes a violation of academic integrity. Students must ensure that all work submitted for evaluation is their own and properly cites any external sources, including AI-generated material, used in their assignments.
Using AI tools to generate content without disclosing their use, or presenting AI-generated work as one's own, is considered plagiarism. Any attempt to submit plagiarized work, whether through manual copying or the use of AI tools, will be subject to academic penalties. It is essential that students recognize the importance of maintaining transparency regarding the sources and tools utilized in their work to uphold academic standards.

5.5 Other General Policy:

Students are expected to **attend all lectures, tutorials, and workshops** regularly. **Active participation** in class discussions is encouraged, and students must ensure the timely submission of all coursework as assigned by the instructor. While late submissions may be accepted under certain circumstances, they will incur penalties as per the course policy.
In addition to the aforementioned policies, students are expected to adhere to all rules and regulations established by the College . **Failure to comply with these policies may result in severe academic penalties, including potential exclusion from the module.**

6 Approximate Schedule

Here you will find a detailed breakdown of the weekly topics and instructional themes for the course. Please note that this proposed schedule is tentative and may be adjusted to accommodate pedagogical priorities and the pacing of instruction.

Week 1: Linear Algebra for Learning

Theme:

Geometric and Algebraic Foundations of Learning Algorithms.

Learning Objectives:

- Build geometric intuition of data and transformations in vector spaces.
- Apply matrix algebra in modeling learning problems.
- Understand projections and orthogonality in hypothesis spaces.
- Prepare for interpreting optimization and kernel methods.

Key Concepts:

- Vectors and Norms: Vector operations, L2 and L1 norms, distance measures
- Linear Independence: Span, basis, rank, implications for hypothesis space
- Projections: Orthogonal projection, least squares interpretation
- Matrix Operations: Multiplication, transpose, inverse, pseudoinverse
- Linear Transformations: Geometry of transformations and implications in ML
- Eigenvalues and SVD: Dimensionality reduction and structure in data
- Geometry of Linear Models: Separability, margins, decision boundaries

Week 2: Probability and Generalization in Learning

Theme:

Uncertainty, Generalization, and Statistical Thinking in Learning

Learning Objectives:

- Understand how uncertainty and randomness affect learning.
- Use key probability tools (expectation, variance, concentration) to analyze learning behavior.
- Bridge empirical and theoretical analysis in learning.
- Prepare for deeper theoretical frameworks like PAC and VC.

Key Concepts:

- Random Variables: Definition, indicator functions, discrete vs continuous
- Expectation & Variance: Linearity of expectation, properties of variance
- Law of Large Numbers: Empirical averages and ERM foundations
- Empirical vs Expected Risk: Definitions and interpretations
- Overfitting and Generalization: Geometric and probabilistic perspectives
- Concentration Inequalities: Markov, Chebyshev, Hoeffding
- Conditional Probability & Bayes' Rule: Uncertainty modeling
- Distributions: Bernoulli, Gaussian, Exponential family
- Probabilistic Framing of Learning: ERM and generalization with finite data

Week 3: Statistical Learning Theory (ERM, PAC)

Theme:

Foundations of Learning from Data

Learning Objectives:

- Understand the principle of Empirical Risk Minimization (ERM).
- Grasp the Probably Approximately Correct (PAC) learning framework.
- Analyze sample complexity and consistency of learners.
- Distinguish between realizable and agnostic settings.

Key Concepts:

- ERM Principle: Loss functions, empirical vs true error
- PAC Framework: Definitions of PAC learnability and generalization
- Sample Complexity: Bounds on samples for guaranteed performance
- Agnostic Learning: Noisy and imperfect hypothesis spaces
- Union Bound & Confidence: Bounding error across hypotheses
- Consistency of ERM: Behavior with increasing data
- Hypothesis Classes: Finite vs infinite, learnability implications

Week 4: VC Dimension & Rademacher Complexity

Theme:

Capacity Control and Learnability

Learning Objectives:

- Define and calculate VC Dimension for simple hypothesis classes.
- Understand growth function and Sauer's Lemma.
- Apply Rademacher complexity to bound generalization error.
- Compare combinatorial and probabilistic complexity measures.

Key Concepts:

- VC Dimension: Shattering, capacity, examples
- Growth Function: Number of labelings, combinatorial bounds
- Sauer's Lemma: Bounding growth of hypothesis classes
- Rademacher Complexity: Empirical and expected versions
- Generalization Bounds: Complexity-performance tradeoff
- Structural Risk Minimization: Fit vs complexity

Week 5: Regularization and Generalization

Theme:

Stability and Bias-Variance Tradeoff

Learning Objectives:

- Understand regularization as a form of complexity control.
- Analyze generalization through bias-variance tradeoffs.
- Use regularized loss minimization to improve stability.
- Relate algorithmic stability to overfitting.

Key Concepts:

- Regularized ERM: L1 and L2 penalties, ridge, lasso
- Bias-Variance Tradeoff: Implications for model selection
- Norm-Based Control: Norms constraining hypothesis space
- Stability and Overfitting: Sensitivity to training data
- Leave-One-Out Error: Estimation of generalization
- Tikhonov Regularization: Smoothness constraints

Week 6: Information Theory in Learning

Theme:

Learning as Compression and Information Processing

Learning Objectives:

- Connect information-theoretic quantities to generalization.
- Explore entropy, KL divergence, and mutual information.
- Interpret learning as compression.
- Analyze PAC-Bayes generalization bounds.

Key Concepts:

- Entropy and Mutual Info: Measures of uncertainty
- KL Divergence: Distance between distributions
- Information Bottleneck: Relevant information retention
- PAC-Bayes Bound: Data-dependent generalization guarantees
- Rate-Distortion Theory: Efficiency of learners
- Minimum Description Length: Simplicity in modeling

Week 7: Basic Optimization for Learning

Theme:

Learning through Minimization

Learning Objectives:

- Understand the optimization landscape in ML.
- Analyze gradient-based methods and their convergence.
- Identify challenges in non-convex optimization.
- Explore optimization stability in learning.

Key Concepts:

- Optimization Setup: Objectives and constraints
- Gradient Descent: Batch, stochastic, momentum
- Convexity and Smoothness: Role in convergence
- Lipschitz & Strong Convexity: Guarantees in optimization
- Learning Rate Schedules: Tuning for performance
- Saddle Points and Local Minima: Deep learning challenges

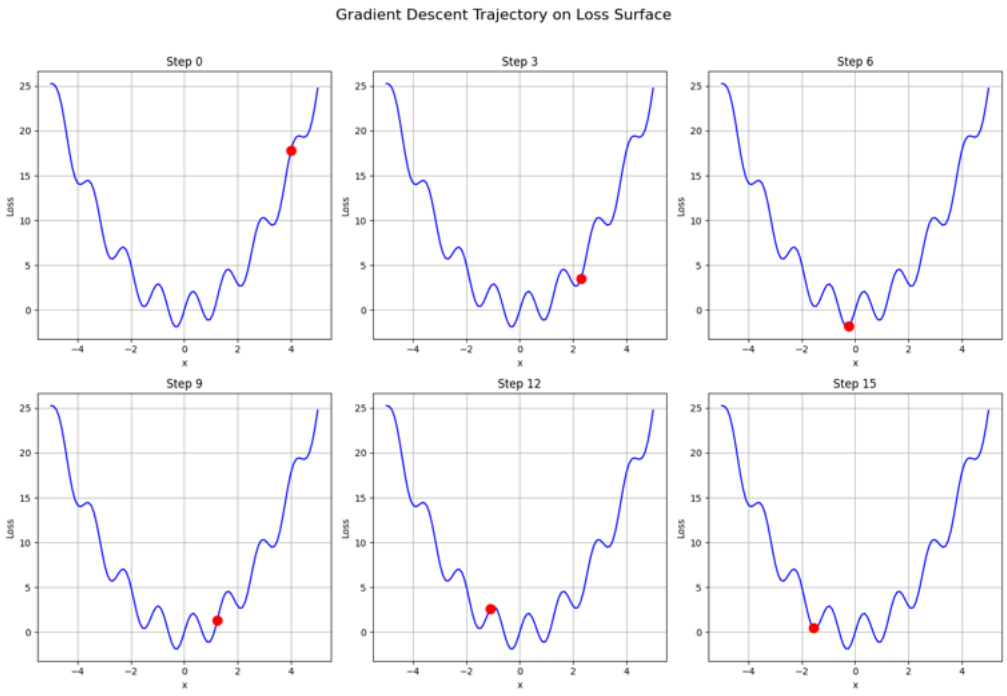

Figure 3: Local Minima is what we aim for.

The - End