Generalization Bounds

Theoretical Foundations of Deep Learning

Matteo Mazzarelli

December 17, 2024

Motivation

- **Core Challenge**: How can a model learned from *limited training data* perform well on *unseen data*?
- Generalization lies at the heart of the machine learning process.
- A poorly generalized model risks:
  - **Overfitting**: Performing well on training data but poorly on unseen data.
  - **Underfitting**: Failing to capture the underlying patterns of the data.

The Learning Problem

- **Supervised Learning**:
  - Goal: Learn a function (f: X $\rightarrow$Y) mapping inputs (X) to outputs (Y) based on labeled training data.
- **Key Question**: Can the learned function perform well on unseen data?
- **Generalization**:
  - Ability of a model to extend its learning beyond the training data.
  - **Central Problem** in machine learning: balancing *empirical performance* with *future predictions*.

Why Theory Matters

- **Significance of Theory**:
  - Guides **algorithm design** by providing a foundation for developing new methods.
  - Allows **performance analysis** to identify the strengths and weaknesses of algorithms.
  - Reveals **limitations** of learning systems, helping us understand their boundaries.
- **Theoretical Understanding**:
  - Bridges the gap between empirical performance and guarantees on future behavior.

Introducing Generalization Bounds

- **What Are Generalization Bounds?**
  - Theoretical tools offering guarantees about a model's performance on unseen data.
  - Relate:
    - **Generalization Error**: How well the model generalizes.
    - **Empirical Risk**: Performance observed on training data.
    - **Model Complexity**: How expressive the model is.
- **Purpose**:
  - Provide insights into the trade-offs between model accuracy, complexity, and training data size.