Yale University CPSC 683

# Stability in Machine Learning: Generalization, Privacy & Replicability Course Syllabus

**Instructor:** Alkis Kalavasis, alkis.kalavasis@yale.edu

| Lecture | Context | References |
|---|---|---|
| 1 | VC Theory and Uniform Convergence | Vapnik (2013); Shalev-Shwartz and Ben-David (2014) |
| 2 | Generalization Bounds and Algorithmic Stability | Bousquet and Elisseeff (2002) |
| 3 | Stability of SGD and Empirical Observations | Hardt et al. (2016), Zhang et al. (2021) |
| 4 | Failure of Uniform Convergence and Domain Adaptation | Nagarajan and Kolter (2019) |
| 5 | Differentially Private PAC Learning | Kasiviswanathan et al. (2011) |
| 6 | Littlestone dimension is necessary for DP PAC learning | Alon et al. (2019) |
| 7 | Littlestone dimension is sufficient for DP PAC learning | Bun et al. (2020) |
| 8 | TV Stability, Replicability, and their connections to Differential Privacy | Impagliazzo et al. (2022), Bun et al. (2023), Kalavasis et al. (2023) |
| 9 | Memorization and Generalization | Feldman (2020), Brown et al. (2021) |
| 10 | A Theory of Learning Curves | Bousquet et al. (2021) |
| 11 | Language Identification and Generation | Gold (1967), Angluin (1979), Kleinberg and Mullainathan (2024) |
| 12 | Language Generation and Mode Collapse | Kalavasis et al. (2024b) |
| 13–14 | Presentations | |