

# Machine Learning and Neural Networks III (MATH3431)

## Epiphany term

Georgios P. Karagiannis

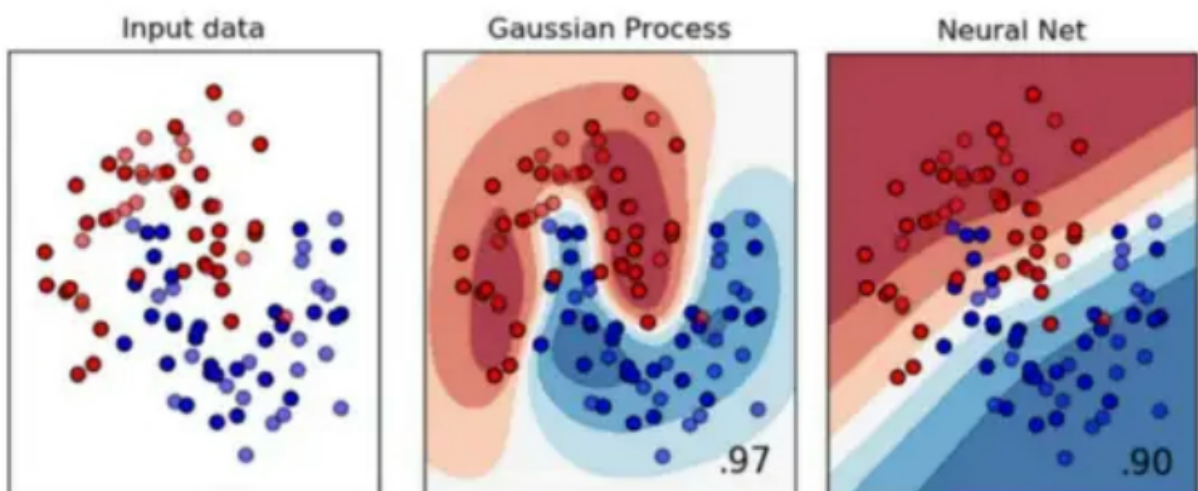
georgios.karagiannis@durham.ac.uk

Department of Mathematical Sciences (Office MCS3088)  
Durham University  
Stockton Road Durham DH1 3LE UK

2025/01/12 at 16:58:39

### Concepts

- Convex learning problems
- Stochastic learning
- Support vector machines
- Artificial neural networks
- Kernel methods, trick
- Gaussian process regression



## READING LIST

These lecture Handouts have been derived based on the reading list below.

### Main texts:

- Bishop, C. M. (2006). Pattern recognition and machine learning. New York: Springer.
  - It is a classical textbook in machine learning (ML) methods. It discusses all the concepts introduced in the course (not necessarily in the same depth). It is one of the main textbooks in the module. The level on difficulty is easy.
  - Students who wish to have a textbook covering traditional concepts in machine learning are suggested to get a copy of this textbook. It is available online from the Microsoft's website <https://www.microsoft.com/en-us/research/publication/pattern-recognition-machine-learning/>
- Shalev-Shwartz, S., & Ben-David, S. (2014). Understanding machine learning: From theory to algorithms. Cambridge university press.
  - It has several elements of theory about machine learning algorithms. It is one of the main textbooks in the module. The level on difficulty is advanced as it requires moderate knowledge of maths.
- Bishop, C. M. (1995). Neural networks for pattern recognition. Oxford university press.
  - It is a classical textbook about 'traditional' artificial neural networks (ANN). It is very comprehensive (compared to others) and it goes deep enough for the module although it may be a bit outdated. It is one of the main textbooks in the module for ANN. The level on difficulty is moderate.

### Supplementary textbooks:

- Vapnik, V. (1999). The nature of statistical learning theory. Springer science & business media.
  - Important textbook in the statistical machine learning theory. To have have an in deep understanding about statistical learning, one has to read it together with the textbook of Shalev-Shwartz, S., & Ben-David, S. (2014)
- Devroye, L., Györfi, L., & Lugosi, G. (2013). A probabilistic theory of pattern recognition (Vol. 31). Springer Science & Business Media.
  - Important textbook in the theoretical aspects about machine learning algorithms. The level on difficulty is advanced as it requires moderate knowledge of probability.
- Theodoridis, S. (2015). Machine learning: a Bayesian and optimization perspective. Academic press.
  - A textbook in general machine learning methods. It includes a large collection of different machine learning methods. It does not go too deep into the theoretical details of the method.
- Murphy, K. P. (2012). Machine learning: a probabilistic perspective. MIT press.
  - A popular textbook in general machine learning methods. It discusses all the concepts introduced in the module. It focuses more on the probabilistic/Bayesian framework but not with great detail. It can be used as a comparison textbook

for brief reading about ML methods just to see another perspective than that in (Bishop, C. M., 2006). The level on difficulty is easy.

- Murphy, K. P. (2022). Probabilistic machine learning: an introduction. MIT press.
  - A textbook in general machine learning methods. It covers a smaller number of ML concepts than (Murphy, K. P., 2012) but it contains more fancy/popular topics such as deep learning ideas. It is suggested to be used in the same manner as (Murphy, K. P., 2012). The level on difficulty is easy.
- Bishop, C. M., & Bishop, H. (2024). Deep learning: foundations and concepts. New York: Springer.
  - A textbook in machine learning methods focusing on Neural Networks philosophy and deep learning. Essentially, this is an update of the earlier book “Bishop, C. M. (1995). Neural networks for pattern recognition. Oxford university press.” where: the concepts about Neural networks, stochastic gradient descent have been extended; new deep learning concepts have been added; and the kernel methods are left out.
- Ripley, B. D. (2007). Pattern recognition and neural networks. Cambridge university press.
  - A classical textbook in artificial neural networks (ANN) that also covers other machine learning concepts. It contains interesting theory about ANN.
  - It is suggested to be used as a supplementary reading for neural networks as it contains a few interesting theoretical results. The level on difficulty is moderate.
- Williams, C. K., & Rasmussen, C. E. (2006). Gaussian processes for machine learning (Vol. 2, No. 3, p. 4). Cambridge, MA: MIT press.
  - A classic book in Gaussian process regression (GPR) that covers the material we will discuss in the course about GPR. It can be used as a companion textbook with that of (Bishop, C. M., 2006). The level on difficulty is easy.

#### Preparatory textbooks:

- Strang, G. (2019). Linear algebra and learning from data. Wellesley-Cambridge Press.
  - Material regarding linear algebra concepts.
- Boyd, S. P., & Vandenberghe, L. (2004). Convex optimization. Cambridge university press.
  - Material regarding Convex optimization, quadratic optimization, Lagrange duality.

## CONTENTS

- (1) Handout 1: Machine learning –A recap on: definitions, notation, and formalism (1 Lecture)
- (2) Handout 2: Elements of convex learning problems (1 Lecture)
- (3) Handout 3: Learnability, and stability
- (4) Handout 4: Gradient descent
- (5) Handout 5: Stochastic gradient descent
- (6) Handout 6: Bayesian Learning via Stochastic gradient and Stochastic gradient Langevin dynamics
- (7) Handout 7: Support Vector Machines
- (8) Handout 8: Kernel methods
- (9) Handout 9: Artificial neural networks
- (10) Handout 10: Multi-class classification
- (11) Handout 11: Gaussian process regression

# Lecture notes 1: Machine learning -A recap on: definitions, notation, and formalism

Lecturer &amp; author: Georgios P. Karagiannis

georgios.karagiannis@durham.ac.uk

**Aim.** To get some definitions and set-up about the learning procedure; essentially to formalize what introduced in term 1.

## Reading list & references:

- Bishop, C. M. (2006). Pattern recognition and machine learning. New York: Springer.
  - Ch. 1 Introduction
- Shalev-Shwartz, S., & Ben-David, S. (2014). Understanding machine learning: From theory to algorithms. Cambridge university press.
  - Ch. 1 Introduction

## 1. GENERAL INTRODUCTIONS AND DEFINITIONS

**Pattern recognition** is the automated discovery of patterns and regularities in data  $z \in \mathcal{Z}$ . **Machine learning (ML)** are statistical procedures for building and understanding probabilistic methods that 'learn'. **ML algorithms**  $\mathfrak{A}$  build a (probabilistic/deterministic) model able to make predictions or decisions with minimum human interference and can be used for pattern recognition. **Learning** (or training, estimation, fitting) is called the procedure where the ML model is tuned. **Training data** (or observations, sample data set, examples) is a set of observables  $\{z_i \in \mathcal{Z}\}$  used to tune the parameters of the ML model. By  $\mathcal{Z}$  we denote the examples (or observables) domain. **Test set** is a set of available examples/observables  $\{z'_i\}$  (different than the training data) used to verify the performance of the ML model for a given a measure of success. **Measure of success** (or performance) is a quantity that indicates how bad the corresponding ML model or Algorithm performs (eg quantifies the failure/error), and can also be used for comparisons among different ML models; eg, **Risk function** or **Empirical Risk Function**. Two main problems in ML are the supervised learning (we will focus on this here) and the unsupervised learning.

**Supervised learning** problems involve applications where the training data  $z \in \mathcal{Z}$  comprise examples of the input vectors  $x \in \mathcal{X}$  along with their corresponding target vectors  $y \in \mathcal{Y}$ ; i.e.  $\mathcal{Z} = \mathcal{X} \times \mathcal{Y}$ . By  $\mathcal{X}$  we denote the inputs (or instances) domain, and by  $\mathcal{Y}$  we denote the target domain. **Classification problems** are those which aim to assign each input vector  $x$  to one of a finite number of discrete categories of  $y$ . **Regression problems** are those where the output  $y$  consists of one or more continuous variables. All in all, the learner wishes to discover an unknown pattern (i.e. functional relationship) between components  $x \in \mathcal{X}$  that serves as inputs and components  $y \in \mathcal{Y}$  that act as outputs; i.e.  $x \mapsto y$ . Hence,  $\mathcal{X}$  is the input domain, and  $\mathcal{Y}$  is the output (or target) domain. The goal of learning is to discover a function which predicts (or help us make decisions about)  $y \in \mathcal{Y}$  from  $x \in \mathcal{X}$ .

**Unsupervised learning** problems involve applications where the training data  $z \in \mathcal{Z}$  consist of a set of input vectors  $x \in \mathcal{X}$  without any corresponding target values ; i.e.  $\mathcal{Z} = \mathcal{X}$ . In clustering the goal is to discover groups of similar examples within the data of it is to discover groups of similar examples within the data.

## 2. NOTATION & DEFINITIONS IN LEARNING

*Note 1.* The aim is to learn the mapping  $x \rightarrow y$  where  $x \in \mathcal{X}$  and  $y \in \mathcal{Y}$  with purpose to predict  $y \in \mathcal{Y}$  from  $x \in \mathcal{X}$ . Denote  $z = (x, y)^\top$  and  $\mathcal{Z} = \mathcal{X} \times \mathcal{Y}$ .

**Definition 2.** The learner's output is a function,  $h : \mathcal{X} \rightarrow \mathcal{Y}$  which predicts  $y \in \mathcal{Y}$  from  $x \in \mathcal{X}$ . It is also called hypothesis, prediction rule, predictor, or classifier.

*Notation 3.* We often denote the set of hypothesis as  $\mathcal{H}$  ; i.e.  $h \in \mathcal{H}$ .

**Example 4.** (Linear Regression)<sup>1</sup> Consider the regression problem where the goal is to learn the mapping  $x \rightarrow y$  where  $x \in \mathcal{X} \subseteq \mathbb{R}^d$  and  $y \in \mathcal{Y} \subseteq \mathbb{R}$ . A hypothesis is a linear function  $h : \mathcal{X} \rightarrow \mathcal{Y}$  (that learner wishes to learn) with  $h(x) = \langle w, x \rangle$  approximating the mapping  $x \rightarrow y$ . The hypothesis set is  $\mathcal{H} = \{x \rightarrow \langle w, x \rangle : w \in \mathbb{R}^d\}$ .

**Example 5.** (Binary Classification) Consider the classification problem where the goal is to learn the mapping  $x \rightarrow y$  where  $x \in \mathcal{X} \subseteq \mathbb{R}^d$  and  $y \in \mathcal{Y} = \{-1, +1\}$ . A hypothesis can be a function  $h : \mathcal{X} \rightarrow \mathcal{Y}$  with  $h(x) = \text{sign}(\langle w, x \rangle)$  approximating the mapping  $x \rightarrow y$ . The hypothesis set  $\mathcal{H} = \{x \rightarrow \text{sign}(\langle w, x \rangle) : w \in \mathbb{R}^d\}$ .

**Definition 6.** (Loss function) Given any set of hypothesis  $\mathcal{H}$  and some domain  $\mathcal{Z} = \mathcal{X} \times \mathcal{Y}$ , a loss function  $\ell(\cdot)$  is any function  $\ell : \mathcal{H} \times \mathcal{Z} \rightarrow \mathbb{R}_+$ . Loss function  $\ell(h, z)$  for  $h \in \mathcal{H}$  and  $z \in \mathcal{Z}$  is specified according to the purpose the machine learning algorithm. It reflects how the “error” is quantified for a given hypothesis  $h$  and a given example  $z$ . The rule is “the greater the error the greater the value of the loss”.

**Example 7.** (Cont. Example 4) In regression problems  $\mathcal{Z} = \mathcal{X} \times \mathcal{Y}$  and  $\mathcal{Y} \subset \mathbb{R}$  is uncountable, a potential loss function is

$$\ell_{\text{sq}}(h, (x, y)) = (h(x) - y)^2$$

**Example 8.** (Cont. Example 5) In binary classification problems with hypothesis  $h : \mathcal{X} \rightarrow \mathcal{Y}$  where  $\mathcal{Y} = \{0, 1\}$  is discrete, a loss function can be

$$\ell_{0-1}(h, (x, y)) = 1(h(x) \neq y),$$

**Definition 9.** A learning problem with hypothesis class  $\mathcal{H}$ , examples domain  $\mathcal{Z}$ , and loss function  $\ell$  may be denoted with a triplet  $(\mathcal{H}, \mathcal{Z}, \ell)$ .

**Example 10.** The standard multiple linear regression problem with regressors  $x \in \mathcal{X} \subseteq \mathbb{R}^d$  and response  $y \in \mathcal{Y} \subseteq \mathbb{R}$ , is a learning problem with examples domain  $\mathcal{Z} = \mathcal{X} \times \mathcal{Y} = \mathbb{R}^{d+1}$ , hypothesis class  $\mathcal{H} = \{x \rightarrow \langle w, x \rangle : w \in \mathbb{R}^d\}$ , and loss function  $\ell_{\text{sq}}(h, (x, y)) = (h(x) - y)^2$ .

---

<sup>1</sup> $\langle w, x \rangle = w^\top x$

**Example 11.** The binary classification regression problem with regressors  $x \in \mathcal{X} \subseteq \mathbb{R}^d$  and response  $y \in \mathcal{Y} = \{-1, +1\}$ , is a learning problem with examples domain  $\mathcal{Z} = \mathcal{X} \times \mathcal{Y}$ , hypothesis class  $\mathcal{H} = \{x \rightarrow \text{sign}(\langle w, x \rangle) : w \in \mathbb{R}^d\}$ , and loss function  $\ell_{0-1}(h, (x, y)) = 1(h(x) \neq y) = 1(\langle w, x \rangle y < 0)$ .

**Definition 12.** Data generation model  $g(\cdot)$  is the probability distribution over  $\mathcal{Z} = \mathcal{X} \times \mathcal{Y}$ , unknown to the learner which describes the probabilistic law that realizations  $z = (x, y) \in \mathcal{Z}$  are realized.

## 2.1. Learning...

**Definition 13.** (Risk function) The risk function  $R_g(h)$  of  $h$  is the expected loss of the hypothesis  $h \in \mathcal{H}$ , w.r.t. the data generation model (which is a probability distribution)  $g$  over domain  $\mathcal{Z}$ ; i.e.

$$(2.1) \quad R_g(h) = \mathbb{E}_{z \sim g}(\ell(h, z))$$

**Definition 14.** (Risk minimization learning) The Risk minimization (RM) learning paradigm computes the optimal predictor  $h^*$  as the minimizer of the risk  $R_g(h)$  of  $h$ ; i.e.

$$(2.2) \quad h^* = \arg \min_h (R_g(h))$$

**Example 15.** (Cont. Ex. 7) The risk function is  $R_g(h) = \mathbb{E}_{z \sim g}(h(x) - y)^2 = \mathbb{E}_{z \sim g}(\langle w, x \rangle - y)^2$ , and it measures the quality of the hypothesis function  $h : \mathcal{X} \rightarrow \mathcal{Y}$ , (or equiv. the validity of the class of hypotheses  $\mathcal{H}$ ) against the data generating model  $g$ , as the expected square difference between the predicted values from  $h$  and the true target values  $y$  at every  $x$ .

**Example 16.** (Cont. Ex. ) The risk function is  $R_g(h) = \mathbb{E}_{z \sim g}(1(h(x) \neq y)) = \Pr_{z \sim g}(\langle x, w \rangle y < 0)$ .

*Note 17.* Computing the risk minimizer may be practically challenging due to the integration w.r.t. the unknown data generation model  $g$  involved in the expectation (2.1). Sub-optimally, instead of the Risk function in (2.2), one use the Empirical risk function as a Monte Carlo approximation of it.

**Definition 18.** Training data set  $\mathcal{S}$  of size  $m$  is any finite sequence of pairs  $(z_i = (x_i, y_i); i = 1, \dots, m)$ , called examples, in  $\mathcal{Z} = \mathcal{X} \times \mathcal{Y}$ ; i.e.  $\mathcal{S} = \{(x_i, y_i); i = 1, \dots, m\}$ . This is the information that the learner has assess.

**Definition 19.** (Empirical risk function) The Empirical Risk Function (ERF)  $\hat{R}_S(h)$  of  $h$  is the expectation of loss of  $h$  over a given sample  $S = (z_1, \dots, z_m) \in \mathcal{Z}^m$ ; i.e.

$$\hat{R}_S(h) = \frac{1}{m} \sum_{i=1}^m \ell(h, z_i).$$

**Definition 20.** (Empirical risk minimization learning) The Empirical risk minimization (ERM) learning paradigm computes the optimal predictor  $h^*$  as the minimizer of the ERF  $\hat{R}_S(h)$  of  $h$ ; i.e.

$$(2.3) \quad h^* = \arg \min_h (\hat{R}_S(h))$$

**Example 21.** (Cont. Example 15) Given given sample  $S = \{(x_i, y_i); i = 1, \dots, m\}$  the empirical risk function is  $\hat{R}_S(h) = \frac{1}{m} \sum_{i=1}^m (h(x_i) - y_i)^2 = \frac{1}{m} \sum_{i=1}^m (x_i^\top w - y_i)^2$ .

**Example 22.** (Cont. Example 8) Given given sample  $S = \{(x_i, y_i); i = 1, \dots, m\}$  the empirical risk function is  $\hat{R}_S(h) = \frac{1}{m} \sum_{i=1}^m 1(h(x_i) \neq y_i) = \frac{1}{m} \sum_{i=1}^m 1(\langle x_i, w \rangle y_i < 0)$ .

**Definition 23.** We denote as  $\mathfrak{A}(S)$  the hypothesis (outcome) that a learning algorithm  $\mathfrak{A}$  returns given training sample  $S$ .

## 2.2. Conventions...

*Note 24.* If the Hypothesis set  $\mathcal{H}$  is a known parametric family of functions; i.e.  $\mathcal{H} = \{h_w(\cdot); w \in \mathcal{W}\}$  parameterized by unknown  $w \in \mathcal{W}$ , then we can equivalently consider the convention  $\mathcal{H} = \{w \in \mathcal{W}\} = \mathcal{W}$  keeping in mind that the learner's output is restricted to formula  $h_w(\cdot)$ .

**Example 25.** Because it involves only linear functions as predictors  $h_w(x) = \langle w, x \rangle$ , we could consider a hypothesis class  $\mathcal{H} = \{w \in \mathbb{R}^d\} = \mathbb{R}^d$  and loss function  $\ell(w, (x, y)) = (\langle w, x \rangle - y)^2$  for simplicity.

**Example 26.** Because it involves only linear functions as predictors  $h_w(x) = \text{sign}(\langle w, x \rangle)$ , we could consider a hypothesis class  $\mathcal{H} = \{w \in \mathbb{R}^d\} = \mathbb{R}^d$  and loss function  $\ell(w, (x, y)) = 1(\langle w, x \rangle y < 0)$  for simplicity.

**Example 27.** Consider a learning problem where the true data generation distribution (unknown to the learner) is  $g(z)$ , the statistical model (known to the learner) is given by a sampling distribution  $f_\theta(y) := f(y|\theta)$  labeled by an unknown parameter  $\theta$ . The goal is to learn  $\theta$ . If we assume loss function

$$\ell(\theta, z) = \log \left( \frac{g(z)}{f_\theta(z)} \right)$$

then the risk is

$$(2.4) \quad R_g(\theta) = \mathbb{E}_{z \sim g} \left( \log \left( \frac{g(z)}{f_\theta(z)} \right) \right) = \mathbb{E}_{z \sim g} (\log(g(z))) - \mathbb{E}_{z \sim g} (\log(f_\theta(z)))$$

whose minimizer is

$$\theta^* = \arg \min_{\forall \theta} (R_g(\theta)) = \arg \min_{\forall \theta} (\mathbb{E}_{z \sim g} (-\log(f_\theta(z))))$$

as the first term in (2.4) is constant. Note that in the Maximum Likelihood Estimation technique the MLE  $\theta_{\text{MLE}}$  is the minimizer

$$\theta_{\text{MLE}} = \arg \min_{\theta} \left( \frac{1}{m} \sum_{i=1}^m (-\log(f_\theta(z_i))) \right)$$

where  $S = \{z_1, \dots, z_m\}$  is an IID sample from  $g$ . Hence, MLE  $\theta_{\text{MLE}}$  can be considered as the minimizer of the empirical risk  $R_S(\theta) = \frac{1}{m} \sum_{i=1}^m (-\log(f_\theta(z_i)))$ .

## 3. REGULARIZED LOSS MINIMIZATION (RLM) LEARNING

*Note 28.* Consider a learning problem  $(\mathcal{H}, \mathcal{Z}, \ell)$  with training data set  $S$ .

**Definition 29.** (Regularized loss minimization learning) Regularized loss minimization learning paradigm computes the optimal rule  $h^* \in \mathcal{H}$  by jointly minimizing the Risk function  $R_g(h)$  (or



Empirical Risk Function  $\hat{R}_{\mathcal{S}}(h)$ ) and a regularization function  $J : \mathcal{H} \rightarrow \mathbb{R}$  where  $J(h)$  increases in value with the complexity of the hypothesis  $h \in \mathcal{H}$ . Formally, the Regularized loss minimization rule  $h^*$  is

$$h^* = \arg \min_{h \in \mathcal{H}} (R_g(h) + J(h)), \text{ given the Risk function}$$

$$h^* = \arg \min_{h \in \mathcal{H}} (\hat{R}_{\mathcal{S}}(h) + J(h)), \text{ given the Empirical risk function}$$

### 3.1. $\ell_0$ , $\ell_1$ , and $\ell_2$ norm regularization problems.

*Note 30.* Consider a parameterized hypothesis  $h_w(\cdot)$  (e.g.  $h_w(x) = \eta(\langle x, w \rangle)$ ) with  $\eta(\cdot)$  a function and  $w \in \mathbb{R}^d$ . Consider the hypothesis class in the simplified form  $\mathcal{H} = \mathcal{W} = \{w \in \mathbb{R}^d\} = \mathbb{R}^d$  of Note 24. Assume we want the vector  $w$  to be sparse, in the sense that “sparser” means more zero elements.

#### 3.1.1. $\ell_0$ norm regularization.

*Note 31.* The problem of minimizing the empirical risk subject to a budget of  $k$  features can be written as

$$\begin{aligned} & \underset{w \in \mathcal{H}}{\text{minimize}} R(w) \\ & \text{subject to } \|w\|_0 \leq k_0 \end{aligned}$$

where  $\|w\|_0 = \#\{j : w_j \neq 0\}$ . By Lagrange multipliers we can re-write it as

$$w^* = \arg \min_{w \in \mathcal{H}} (R(w) + \lambda_0 \|w\|_0)$$

for some  $\lambda_0 \geq 0$  ( $k_0$  dependent). Hence,  $h^*(x) = h_{w^*}(x)$ .

**Example 32.** (Cont. Example 25) The  $\ell_0$ -RLM rule in Example 25 becomes

$$w^* = \arg \min_w \left( \mathbb{E}_{z \sim g} (\langle w, x_i \rangle - y)^2 + \lambda_0 \|w\|_0 \right)$$

using the Risk function, and

$$w^* = \arg \min_w \left( \frac{1}{m} \sum_{i=1}^m (\langle w, x_i \rangle - y_i)^2 + \lambda_0 \|w\|_0 \right)$$

using the Empirical risk function.

#### 3.1.2. $\ell_1$ norm regularization (LASSO).

*Note 33.* Solving  $\ell_0$  norm optimization problem is computationally hard. To simplify computations, we can replace  $J(\cdot) = \|\cdot\|_0$  with  $J(\cdot) = \|\cdot\|_1$  i.e.

$$\begin{aligned} & \underset{w \in \mathcal{H}}{\text{minimize}} R(w) \\ & \text{subject to } \|w\|_1 \leq k_1 \end{aligned}$$

where  $\|w\|_1 = \sum_j |w_j|$ . By Lagrange multiplies we can re-write it as

$$w^* = \arg \min_w (R(w) + \lambda_1 \|w\|_1)$$

for some  $\lambda_1 \geq 0$  ( $k_1$  dependent). Hence,  $h^*(x) = h_{w^*}(x)$ .

**Example 34.** (Cont. Example 25) The  $\ell_1$ -RLM rule in Example 25 becomes

$$w^* = \arg \min_w \left( \mathbb{E}_{z \sim g} (\langle w, x \rangle - y)^2 + \lambda_1 \sum_{j=1}^d |w_j| \right)$$

using the Risk function, and

$$w^* = \arg \min_w \left( \frac{1}{m} \sum_{i=1}^m (\langle w, x_i \rangle - y_i)^2 + \lambda_1 \sum_{j=1}^d |w_j| \right)$$

using the Empirical risk function.

### 3.1.3. $\ell_2$ norm regularization (Ridge).

*Note 35.* To further simplify computations, we can consider  $J(\cdot) = \|\cdot\|_2$  i.e.

$$\begin{aligned} & \underset{w}{\text{minimize}} R(w) \\ & \text{subject to } \|w\|_2^2 \leq k_2 \end{aligned}$$

where  $\|w\|_2^2 = \sum_j w_j^2$ . By Lagrange multiplies we can re-write it as

$$w^* = \arg \min_w \left( R(w) + \lambda_2 \|w\|_2^2 \right)$$

for some  $\lambda_1 \geq 0$  ( $k_1$  dependent). Hence,  $h^*(x) = h_{w^*}(x)$ .

**Example 36.** (Cont. Example 25) The  $\ell_2$ -RLM rule in Example 25 becomes

$$w^* = \arg \min_w \left( \mathbb{E}_{z \sim g} (\langle w, x \rangle - y)^2 + \lambda_2 \sum_{j=1}^d w_j^2 \right)$$

using the Risk function, and

$$w^* = \arg \min_w \left( \frac{1}{m} \sum_{i=1}^m (h(x_i) - y_i)^2 + \lambda_2 \sum_{j=1}^d w_j^2 \right)$$

using the Empirical risk function.

**Example 37.** (Cont. Example 26) The  $\ell_2$ -RLM rule in Example 26 becomes

$$w^* = \arg \min_w \left( \Pr_{z \sim g} (\langle x, w \rangle y < 0) + \lambda_2 \sum_{j=1}^d w_j^2 \right)$$

using the Risk function, and

$$w^* = \arg \min_w \left( \frac{1}{m} \sum_{i=1}^m 1(\langle x_i, w \rangle y_i < 0) + \lambda_2 \sum_{j=1}^d w_j^2 \right)$$

using the Empirical risk function.

## Lecture notes 2: Elements of convex learning problems

Lecturer &amp; author: Georgios P. Karagiannis

georgios.karagiannis@durham.ac.uk

---

**Aim.** To introduce convex learning problems that can be used as a framework for the analysis of stochastic gradient related learning algorithms.

---

### Reading list & references:

- Shalev-Shwartz, S., & Ben-David, S. (2014). Understanding machine learning: From theory to algorithms. Cambridge university press.
  - Ch. 12 Convex Learning Problems

Further reading

- Bishop, C. M. (2006). Pattern recognition and machine learning. New York: Springer.

## 1. MOTIVATIONS

*Note 1.* We introduce learning problems associated with convexity, Lipschitzness and smoothness to be able to analyze and understand the machine learning (ML) tools we will discuss later on (eg stochastic gradient descent, SVM). We discuss ways allowing to address non-convex ML problems (eg, Artificial neural networks, Gaussian process regression) in the convex setting.

## 2. CONVEXITY

*Note 2.* Convexity is a central concept in learning, e.g. least squares, as it often considers a Euclidean distance as a Risk function to be minimized.

**Definition 3.** A set  $C$  is convex if for any  $u, v \in C$  and for any  $\alpha \in [0, 1]$  we have that  $\alpha u + (1 - \alpha)v \in C$ .

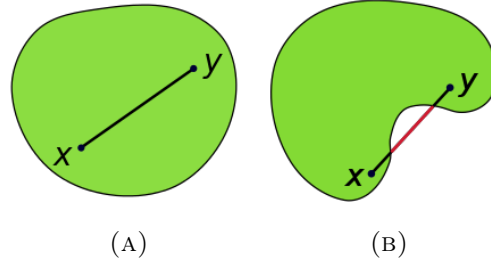


FIGURE 2.1. (2.1a) is a Convex set ; (2.1b) is a non-convex set

**Example 4.** For instance  $\mathbb{R}^d$  for  $d \geq 1$  is a convex set.

**Definition 5.** Let  $C$  be a convex set. A function  $f : C \rightarrow \mathbb{R}$  is convex function if for any  $u, v \in C$  and for any  $\alpha \in [0, 1]$

$$f(\alpha u + (1 - \alpha)v) \leq \alpha f(u) + (1 - \alpha)f(v)$$

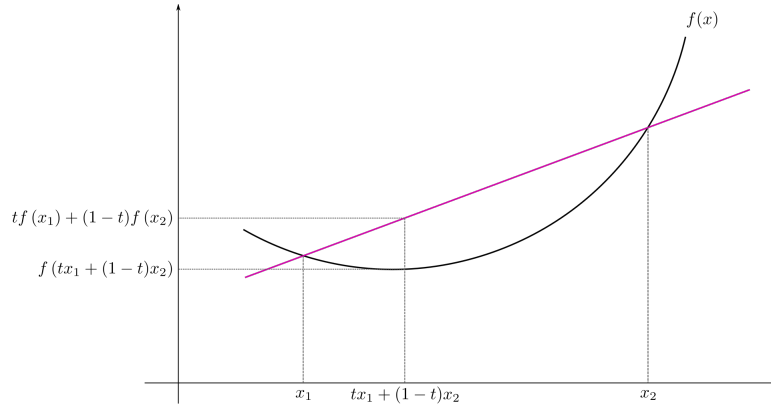


FIGURE 2.2. A convex function

**Example 6.** The function  $f : \mathbb{R}^d \rightarrow \mathbb{R}_+$  with  $f(x) = \|x\|_2^2$  is convex function. For any  $u, v \in C$  and for any  $\alpha \in [0, 1]$  it is

$$\begin{aligned} & \|\alpha u + (1 - \alpha)v\|_2^2 - \alpha \|u\|_2^2 - (1 - \alpha) \|v\|_2^2 \\ &= (\alpha u + (1 - \alpha)v)^\top (\alpha u + (1 - \alpha)v) - \alpha \|u\|_2^2 - (1 - \alpha) \|v\|_2^2 \\ &= \dots = -\alpha(1 - \alpha) \|u - v\|_2^2 \leq 0 \end{aligned}$$

*Note 7.* Every local minimum of a convex function is the global minimum.

*Note 8.* Let  $f : C \rightarrow \mathbb{R}$  be convex function. The tangent of  $f$  at  $w \in C$  is below  $f$ , namely

$$\forall u \in C \quad f(u) \geq f(w) + \langle \nabla f(w), u - w \rangle$$

**Proposition 9.** Let  $f : \mathbb{R}^d \rightarrow \mathbb{R}$  such that  $f(w) = g(\langle w, x \rangle + y)$  for some  $x \in \mathbb{R}^d$ ,  $y \in \mathbb{R}$ . If  $g$  is convex function then  $f$  is convex function.

*Proof.* See Exercise 1 in the Exercise sheet. □

**Example 10.** Consider the regression problem with regressor  $x \in \mathbb{R}^d$ , and response  $y \in \mathbb{R}$  and predictor rule  $h(x) = \langle w, x \rangle$ . The loss function  $\ell(w, (x, y)) = (\langle w, x \rangle - y)^2$  is convex because  $g(a) = (a)^2$  is convex and Proposition 9.

*Note 11.* Let  $f_j : \mathbb{R}^d \rightarrow \mathbb{R}$  convex functions for  $j = 1, \dots, r$ . Then:

- (1)  $g(x) = \max_{\forall j} (f_j(x))$  is a convex function
- (2)  $g(x) = \sum_{j=1}^r w_j f_j(x)$  is a convex function where  $w_j > 0$

*Proof.*

- (1) For any  $u, v \in \mathbb{R}^d$  and for any  $\alpha \in [0, 1]$

$$\begin{aligned}
 g(\alpha u + (1 - \alpha)v) &= \max_{\forall j} (f_j(\alpha u + (1 - \alpha)v)) \\
 &\leq \max_{\forall j} (\alpha f_j(u) + (1 - \alpha)f_j(v)) && (f_j \text{ is convex}) \\
 &\leq \alpha \max_{\forall j} (f_j(u)) + (1 - \alpha) \max_{\forall j} (f_j(v)) && (\max(\cdot) \text{ is convex}) \\
 &\leq \alpha g(u) + (1 - \alpha)g(v)
 \end{aligned}$$

- (2) For any  $u, v \in \mathbb{R}^d$  and for any  $\alpha \in [0, 1]$

$$\begin{aligned}
 g(\alpha u + (1 - \alpha)v) &= \sum_{j=1}^r w_j f_j(\alpha u + (1 - \alpha)v) \\
 &\leq \alpha \sum_{j=1}^r w_j f_j(u) + (1 - \alpha) \sum_{j=1}^r w_j f_j(v) && (f_j \text{ is convex}) \\
 &\leq \alpha g(u) + (1 - \alpha)g(v)
 \end{aligned}$$

□

**Example 12.**  $g(x) = \|x\|_1$  is convex according to Note 11, since  $|x_j| = \max(-x_j, x_j)$  and  $\|x\|_1 = \sum_j |x_j|$ .

### 3. STRONG CONVEXITY

*Note 13.* Strong convexity is a central concept in Ridge regularization, as it makes a convex loss function strongly convex by adding a shrinkage term.

**Definition 14.** (Strongly convex functions) A function  $f$  is  $\lambda$ -strongly convex function is for all  $w, u$ , and  $\alpha \in (0, 1)$  we have

$$(3.1) \quad f(\alpha w + (1 - \alpha)u) \leq \alpha f(w) + (1 - \alpha)f(u) - \frac{\lambda}{2}\alpha(1 - \alpha)\|w - u\|^2$$

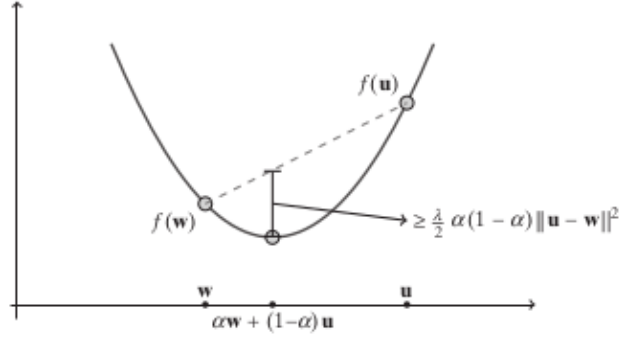


FIGURE 3.1. Strongly convex function

*Note 15.* The following can be checked from the definition by substitution

- (1) The function  $f(w) = \lambda \|w\|^2$  is  $2\lambda$ -strongly convex
- (2) If  $f$  is  $\lambda$ -strongly convex and  $g$  is convex then  $f + g$  is  $\lambda$ -strongly convex

#### 4. LIPSCHITZNESS

**Definition 16.** Let  $C \in \mathbb{R}^d$ . Function  $f : \mathbb{R}^d \rightarrow \mathbb{R}^k$  is  $\rho$ -Lipschitz over  $C$  if for every  $w_1, w_2 \in C$  we have that

$$(4.1) \quad \|f(w_1) - f(w_2)\| \leq \rho \|w_1 - w_2\|. \quad \text{Lipschitz condition}$$

*Note 17.* That means: a Lipschitz function  $f(x)$  cannot change too drastically wrt  $x$ .

**Example 18.** Consider the function  $f : \mathbb{R} \rightarrow \mathbb{R}_+$  with  $f(x) = x^2$ .

- (1)  $f$  is not a  $\rho$ -Lipschitz in  $\mathbb{R}$ .
- (2)  $f$  is a  $\rho$ -Lipschitz in  $C = \{x \in \mathbb{R} : |x| < \rho/2\}$ .

$$|f(x_2) - f(x_1)| = |x_2^2 - x_1^2| = |(x_2 + x_1)(x_2 - x_1)| \leq 2\rho/2(x_2 - x_1) = \rho|x_2 - x_1|$$

**Solution.**

- (1) For  $x_1 = 0$  and  $x_2 = 1 + \rho$ , it is

$$|f(x_2) - f(x_1)| = (1 + \rho)^2 > \rho(1 + \rho) = \rho|x_2 - x_1|$$

- (2) It is

$$|f(x_2) - f(x_1)| = |x_2^2 - x_1^2| = |(x_2 + x_1)(x_2 - x_1)| \leq 2\rho/2(x_2 - x_1) = \rho|x_2 - x_1|$$

*Note 19.* Let functions  $g_1$  be  $\rho_1$ -Lipschitz and  $g_2$  be  $\rho_2$ -Lipschitz. Then  $f$  with  $f(x) = g_1(g_2(x))$  is  $\rho_1\rho_2$ -Lipschitz.

[See Exercise 2 from the exercise sheet]

**Example 20.** Let functions  $g$  be  $\rho$ -Lipschitz. Then  $f$  with  $f(x) = g(\langle v, x \rangle + b)$  is  $(\rho|v|)$ -Lipschitz.

**Solution.** It is

$$\begin{aligned} |f(w_1) - f(w_2)| &= |g(\langle v, w_1 \rangle + b) - g(\langle v, w_2 \rangle + b)| \leq \rho |\langle v, w_1 \rangle + b - \langle v, w_2 \rangle - b| \\ &\leq \rho |v^\top w_1 - v^\top w_2| \leq \rho |v| |w_1 - w_2| \end{aligned}$$

*Note 21.* So, given Examples 18 and 20, in the linear regression setting using loss  $\ell(w, z = (x, y)) = (w^\top x - y)^2$ , the loss function is  $\rho$ -Lipschitz for a given  $z = (x, y)$  and bounded  $\|w\| < \rho$ .

## 5. SMOOTHNESS

**Definition 22.** A differentiable function  $f : \mathbb{R}^d \rightarrow \mathbb{R}$  is  $\beta$ -smooth if its gradient is  $\beta$ -Lipschitz; namely for all  $v, w \in \mathbb{R}^d$

$$(5.1) \quad \|\nabla f(w_1) - \nabla f(w_2)\| \leq \beta \|w_1 - w_2\|.$$

*Note 23.* Function  $f : \mathbb{R}^d \rightarrow \mathbb{R}$  is  $\beta$ -smooth iff

$$(5.2) \quad f(v) \leq f(w) + \langle \nabla f(w), v - w \rangle + \frac{\beta}{2} \|v - w\|^2$$

*Note 24.* Let  $f : \mathbb{R}^d \rightarrow \mathbb{R}$  with  $f(w) = g(\langle w, x \rangle + y)$   $x \in \mathbb{R}^d$  and  $y \in \mathbb{R}$ . Let  $g : \mathbb{R} \rightarrow \mathbb{R}$  be a  $\beta$ -smooth function. Then  $f$  is a  $(\beta \|x\|^2)$ -smooth.

[See Exercise 3 from the Exercise sheet]

**Example 25.** Let  $f(w) = (\langle w, x \rangle + y)^2$  for  $x \in \mathbb{R}^d$  and  $y \in \mathbb{R}$ . Then  $f$  is  $(2\|x\|^2)$ -smooth.

**Solution.** It is  $f(w) = g(\langle w, x \rangle + y)$  for  $g(a) = a^2$ .  $g$  is 2-smooth since

$$\|g'(w_1) - g'(w_2)\| = \|2w_1 - 2w_2\| \leq 2 \|w_1 - w_2\|.$$

Hence from Theorem 24,  $f$  is  $(2\|x\|^2)$ -smooth.

**Example 26.** Consider the regression problem with predictor rule  $h(x) = \langle w, x \rangle$ , loss function  $\ell(w, (x, y)) = (\langle w, x \rangle - y)^2$ , feature  $x \in \mathbb{R}^d$ , and target  $y \in \mathbb{R}$ . Then  $\ell(w, \cdot)$  is  $(2\|x\|^2)$ -smooth.

[Follows from Example 25.]



## 6. CONVEX LEARNING PROBLEMS

**Definition 27.** Convex learning problem is a learning problem  $(\mathcal{H}, \mathcal{Z}, \ell)$  that the hypothesis class  $\mathcal{H}$  is a convex set, and the loss function  $\ell$  is a convex function for each example  $z \in \mathcal{Z}$ .

**Example 28.** Consider the regression problem with predictor rule  $h(x) = \langle w, x \rangle$ , loss function  $\ell(w, (x, y)) = (\langle w, x \rangle - y)^2$ , feature  $x \in \mathbb{R}^d$ , and target  $y \in \mathbb{R}$ . This imposes a convex learning problem due to Examples 4 and 11.

**Definition 29.** Convex-Lipschitz-Bounded Learning Problem  $(\mathcal{H}, \mathcal{Z}, \ell)$  with parameters  $\rho$ , and  $B$ , is called the learning problem whose the hypothesis class  $\mathcal{H}$  is a convex set, for all  $w \in \mathcal{H}$  it is  $\|w\| \leq B$ , and the loss function  $\ell(\cdot, z)$  is convex and  $\rho$ -Lipschitz function for all  $z \in \mathcal{Z}$ .

**Example 30.** Consider the regression problem with predictor rule  $h(x) = \langle w, x \rangle$ , loss function  $\ell(w, (x, y)) = (\langle w, x \rangle - y)^2$ , feature  $x \in \mathbb{R}^d$ , and target  $y \in \mathbb{R}$ . This imposes a Convex-Lipschitz-Bounded Learning Problem if  $\mathcal{H} = \{w \in \mathbb{R}^d : \|w\| \leq B\}$  due to Examples 11, and 18(2).

**Definition 31.** Convex-Smooth-Bounded Learning Problem  $(\mathcal{H}, \mathcal{Z}, \ell)$  with parameters  $\beta$ , and  $B$ , is called the learning problem whose the hypothesis class  $\mathcal{H}$  is a convex set, for all  $w \in \mathcal{H}$  it is  $\|w\| \leq B$ , and the loss function  $\ell(\cdot, z)$  is convex, nonnegative, and  $\beta$ -smooth function for all  $z \in \mathcal{Z}$ .

**Example 32.** Consider the regression problem with predictor rule  $h(x) = \langle w, x \rangle$ , loss function  $\ell(w, (x, y)) = (\langle w, x \rangle - y)^2$ , feature  $x \in \mathbb{R}^d$ , and target  $y \in \mathbb{R}$ . This imposes a Convex-Smooth-Bounded Learning Problem if  $\mathcal{H} = \{w \in \mathbb{R}^d : \|w\| \leq B\}$  due to Examples 11, and 26.

*Note 33.* If  $\ell$  is a convex loss function and the class  $\mathcal{H}$  is convex, then the  $\text{ERM}_{\mathcal{H}}$  problem, of minimizing the empirical risk  $\hat{R}_{\mathcal{S}}(w)$  over  $\mathcal{H}$ , is a convex optimization problem

*Proof.* The  $\text{ERM}_{\mathcal{H}}$  problem is

$$w^* = \arg \min_{w \in \mathcal{H}} \left\{ \hat{R}_{\mathcal{S}}(w) \right\}$$

given a sample  $\mathcal{S} = \{z_1, \dots, z_m\}$  for  $\hat{R}_{\mathcal{S}}(w) = \frac{1}{m} \sum_{i=1}^m \ell(w, z_i)$ .  $\hat{R}_{\mathcal{S}}(w)$  is a convex function from Note (11). Hence ERM rule is a problem of minimizing a convex function subject to the constraint that the solution should be in a convex set.  $\square$

**Example 34.** Multiple linear regression with predictor rule  $h(x) = \langle w, x \rangle$ , loss function  $\ell(w, (x, y)) = (\langle w, x \rangle - y)^2$ , feature  $x \in \mathbb{R}^d$ , and target  $y \in \mathbb{R}$  where

$$w^* = \arg \min_w \mathbb{E}((\langle w, x \rangle - y)^2)$$

or

$$w^{**} = \arg \min_w \frac{1}{m} \sum_{i=1}^m (\langle w, x_i \rangle - y_i)^2$$

is a convex learning problem –from Proposition 33.

*Note 35.* (Ridge /  $\ell_2$ -RLM problem) If  $\ell$  is a convex loss function w.r.t.  $w$ , the class  $\mathcal{H}$  is convex, and  $J(\cdot; \lambda) = \lambda \|\cdot\|_2^2$  with  $\lambda > 0$  then  $\hat{R}_S(w) + \lambda \|w\|_2^2$  is a  $2\lambda$ -strongly convex function, and hence the  $\ell_2$ -RLM problem

$$w^* = \arg \min_{w \in \mathcal{H}} \left\{ \hat{R}_S(w) + \lambda \|w\|_2^2 \right\}$$

is a strongly convex optimization problem (i.e. the learning rule is the minimizer of a strongly convex function over a convex set).

*Proof.*  $\hat{R}_S(\cdot)$  is a convex function from Proposition 33,  $\lambda \|\cdot\|_2^2$  is  $2\lambda$ -strongly convex, hence  $\hat{R}_S(w) + \lambda \|w\|_2^2$  is a  $2\lambda$ -strongly convex function. Hence the above  $\text{ERM}_{\mathcal{H}}$  problem is a strongly convex optimization problem.  $\square$

## 7. NON-CONVEX LEARNING PROBLEMS (SURROGATE TREATMENT)

*Note 36.* A learning problem may involve non-convex loss function  $\ell(w, z)$  which implies a non-convex risk function  $R_g(w)$ . A suitable treatment to analyze the associated learning tools within the convex setting would be to upper bound the non-convex loss function  $\ell(w, z)$  by a convex surrogate loss function  $\tilde{\ell}(w, z)$  for all  $w$ , and use  $\tilde{\ell}(w, z)$  instead of  $\ell(w, z)$ .

**Example 37.** Consider the binary classification problem with inputs  $x \in \mathcal{X}$ , outputs  $y \in \{-1, +1\}$ ; we need to learn  $w \in \mathcal{H}$  from hypothesis class  $\mathcal{H} \subset \mathbb{R}^d$  with respect to the loss

$$\ell(w, (x, y)) = 1_{(y\langle w, x \rangle \leq 0)}$$

with  $y \in \mathbb{R}$ , and  $x \in \mathbb{R}^d$ . Here  $\ell(\cdot)$  is non-convex. A convex surrogate loss function can be

$$\tilde{\ell}(w, (x, y)) = \max(0, 1 - y\langle w, x \rangle)$$

which is convex (Example 11) wrt  $w$ . Note that:

- $\tilde{\ell}(w, (x, y))$  is convex wrt  $w$ ; because  $\max(\cdot)$  is convex
- $\ell(w, (x, y)) \leq \tilde{\ell}(w, (x, y))$  for all  $w \in \mathcal{H}$

Then we can compute

$$\tilde{w}_* = \arg \min_{\forall x} \left( \tilde{R}_g(w) \right) = \arg \min_{\forall x} \left( \mathbb{E}_{(x, y) \sim g} (\max(0, 1 - y\langle w, x \rangle)) \right)$$

instead of

$$w_* = \arg \min_{\forall x} (R_g(w)) = \arg \min_{\forall x} \left( \mathbb{E}_{(x, y) \sim g} (1_{(y\langle w, x \rangle \leq 0)}) \right)$$

Of course by using the surrogate loss instead of the actual one, we introduce some approximation error in the produced output  $\tilde{w}_* \neq w_*$ .

*Note 38.* (Intuitions...) Using a convex surrogate loss function instead the convex one, facilitates computations but introduces extra error to the solution. If  $R_g(\cdot)$  is the risk under the non-convex loss,  $\tilde{R}_g(\cdot)$  is the risk under the convex surrogate loss, and  $\tilde{w}_{\text{alg}}$  is the output of the learning algorithm under  $\tilde{R}_g(\cdot)$  then we have the upper bound

$$R_g(\tilde{w}_{\text{alg}}) \leq \underbrace{\min_{w \in \mathcal{H}} (R_g(w))}_{\text{I}} + \underbrace{\left( \min_{w \in \mathcal{H}} (\tilde{R}_g(w)) - \min_{w \in \mathcal{H}} (R_g(w)) \right)}_{\text{II}} + \underbrace{\epsilon}_{\text{III}}$$

where term I is the approximation error measuring how well the hypothesis class performs on the generating model, term II is the optimization error due to the use of surrogate loss instead of the actual non-convex one, and term III is the estimation error due to the use of a training set and not the whole generation model.

## Lecture notes 3: Learnability and stability in learning problems

Lecturer &amp; author: Georgios P. Karagiannis

georgios.karagiannis@durham.ac.uk

---

**Aim.** To introduce concepts PAC, fitting vs stability trade off, stability, and their implementation in regularization problems and convex problems.

---

### Reading list & references:

- Shalev-Shwartz, S., & Ben-David, S. (2014). Understanding machine learning: From theory to algorithms. Cambridge university press.  
– Ch. 2, 3, 13
- Vapnik, V. (2000). The nature of statistical learning theory. Springer science & business media.

### 1. LEARNABLE PROBABLY APPROXIMATELY CORRECT (PAC) LEARNING

*Note 1.* We formally define the broad learning problem we will work on.

*Note 2.* Learning algorithms  $\mathcal{A}$  use training data sets  $\mathcal{S}$  which may miss characteristics of the unknown data-generating process  $g$ . Essentially, approximations (aka errors) are inevitable; some characteristics of data generating process  $g$  will be missed even if we use a very representative training set  $\mathcal{S}$ . We cannot hope that the learning algorithm will find a hypothesis whose error is smaller than the minimal possible error.

*Note 3.* The PAC learning problem requires no prior assumptions about the data-generating process  $g$ . It requires that the learning algorithm  $\mathcal{A}$  will find a predictor  $\mathcal{A}(\mathcal{S})$  whose error is not much larger than the best possible error of a predictor in some given benchmark hypothesis class. So essentially, in practice, the researcher's effort falls on the hypothesis class  $\mathcal{H}$ .

**Definition 4.** (Agnostic PAC Learnability for General Loss Functions) A hypothesis class  $\mathcal{H}$  is agnostic PAC learnable with respect to a domain  $\mathcal{Z}$  and a loss function  $\ell : \mathcal{H} \times \mathcal{Z} \rightarrow \mathbb{R}_+$ , if there exist a function  $m_{\mathcal{H}} : (0, 1)^2 \rightarrow \mathbb{N}$  and a learning algorithm  $\mathcal{A}$  with the following property:

- for every  $\epsilon \in (0, 1)$ ,  $\delta \in (0, 1)$ , and distribution  $g$  over  $\mathcal{Z}$ , when running algorithm  $\mathcal{A}$  given training set  $\mathcal{S}_m = \{z_1, \dots, z_m\}$  with  $z_i \stackrel{\text{iid}}{\sim} g$  for  $m \geq m_{\mathcal{H}}(\epsilon, \delta)$  then  $\mathcal{A}$  returns

$\mathfrak{A}(\mathcal{S}) \in \mathcal{H}$  such as

$$(1.1) \quad \Pr_{\mathcal{S} \sim g} \left( R_g(\mathfrak{A}(\mathcal{S}_m)) - \min_{h' \in \mathcal{H}} (R_g(h')) \leq \epsilon \right) \geq 1 - \delta$$

*Note 5.* About 1.1: The accuracy parameter  $\epsilon$  determines how far the output rule  $\mathfrak{A}(\mathcal{S}_m)$  of  $\mathfrak{A}$  can be from the optimal one (this corresponds to the ‘approximately correct’). The confidence parameter  $\delta$  indicates how likely the classifier is to meet that accuracy requirement (corresponds to the “probably” part of “PAC”).

*Note 6.* It may be easier to work with expectations: by using Markov inequality (1.1) becomes

$$(1.2) \quad \Pr_{\mathcal{S} \sim g} \left( R_g(\mathfrak{A}(\mathcal{S}_m)) - \min_{h' \in \mathcal{H}} (R_g(h')) \leq \epsilon \right) \geq 1 - \frac{1}{\epsilon} \mathbb{E}_{\mathcal{S} \sim g} \left( R_g(\mathfrak{A}(\mathcal{S}_m)) - \min_{h' \in \mathcal{H}} (R_g(h')) \right)$$

and hence can just compute expectations and bound them from above.

**Hint:** Markov inequality  $\Pr(X \geq a) \leq \frac{1}{a} \mathbb{E}(X)$  for  $X > 0$ .

## 2. ANALYSIS OF THE RISK BASED ON THE TRADE-OFF FITTING VS STABILITY

*Note 7.* Let  $R^* = \min_{h \in \mathcal{H}} (R(h))$  be an ideal/optimal (hence minimum) Risk, and  $\mathfrak{A}(\mathcal{S})$  the learning rule from a learning algorithm  $\mathfrak{A}$  trained against dataset  $\mathcal{S}$ . The Risk of a learning algorithm  $\mathfrak{A}$  can be decomposed as

$$(2.1) \quad R_g(\mathfrak{A}(\mathcal{S})) - R^* = \hat{R}_{\mathcal{S}}(\mathfrak{A}(\mathcal{S})) - R^* + \underbrace{R_g(\mathfrak{A}(\mathcal{S})) - \hat{R}_{\mathcal{S}}(\mathfrak{A}(\mathcal{S}))}_{\text{over-fitting}}$$

*Note 8.* Over-fitting can be represented by  $R_g(\mathfrak{A}(\mathcal{S})) - \hat{R}_{\mathcal{S}}(\mathfrak{A}(\mathcal{S}))$ . However,  $\hat{R}_{\mathcal{S}}(\cdot)$  is a random variable and, here, for our computational convenience, we focus on its expectation w.r.t.  $\mathcal{S} \sim g$ . Hence, we provide the following (arguable) definition for over-fitting on which we base our analysis.

**Definition 9.** For a learning algorithm  $\mathfrak{A}$ , as a measure of over-fitting we consider the expected difference between true Risk and empirical Risk

$$(2.2) \quad \mathbb{E}_{\mathcal{S} \sim g} \left( R_g(\mathfrak{A}(\mathcal{S})) - \hat{R}_{\mathcal{S}}(\mathfrak{A}(\mathcal{S})) \right)$$

**Definition 10.** We say that learning algorithm  $\mathfrak{A}$  suffers from over-fitting when (2.2) is ‘too’ large.

*Note 11.* The expected Risk of a learning algorithm  $\mathfrak{A}(\mathcal{S})$  can be decomposed as

$$(2.3) \quad \mathbb{E}_{\mathcal{S} \sim g} (R_g(\mathfrak{A}(\mathcal{S}))) = \underbrace{\mathbb{E}_{\mathcal{S} \sim g} \left( \hat{R}_{\mathcal{S}}(\mathfrak{A}(\mathcal{S})) \right)}_{\text{(I)}} + \underbrace{\mathbb{E}_{\mathcal{S} \sim g} \left( R_g(\mathfrak{A}(\mathcal{S})) - \hat{R}_{\mathcal{S}}(\mathfrak{A}(\mathcal{S})) \right)}_{\text{(II)}}$$

by applying expectations in (2.1) and ignoring  $R^*$ . (I) indicates how well  $\mathfrak{A}(\mathcal{S})$  fits the training set  $\mathcal{S}$ , and (II) indicates the discrepancy between the true and empirical risks of  $\mathfrak{A}(\mathcal{S})$ . In Section 3, we argue that the over-fitting term (II) is directly related to a certain type of stability of  $\mathfrak{A}(\mathcal{S})$ .

*Note 12.* The following result connects the need for upper bounding (and minimizing this bound) the Expected Risk in (2.3) and PAC learning (Definition 4).

**Proposition 13.** *Let  $\mathfrak{A}$  be a learning algorithm that guarantees the following:*

- *If  $m \geq m_{\mathcal{H}}(\epsilon)$  then for every distribution  $g$ , it is*

$$E_{\mathcal{S} \sim g}(R_g(\mathfrak{A}(\mathcal{S}_m))) \leq \min_{h' \in \mathcal{H}}(R_g(h')) + \epsilon$$

*Then  $\mathfrak{A}$  satisfies the PAC guarantee in Definition 4:*

- *for every  $\delta \in (0, 1)$ , if  $m \geq m_{\mathcal{H}}(\epsilon\delta)$  then*

$$\Pr_{\mathcal{S} \sim g} \left( R_g(\mathfrak{A}(\mathcal{S}_m)) - \min_{h' \in \mathcal{H}}(R_g(h')) \leq \epsilon \right) \geq 1 - \delta$$

*Proof.* Let  $\xi = R_g(\mathfrak{A}(\mathcal{S}_m)) - \min_{h' \in \mathcal{H}}(R_g(h'))$ . From Markov's inequality  $\Pr(\xi \geq E(\xi)/\delta) \leq \frac{1}{E(\xi)/\delta} E(\xi) = \delta$ . Namely,  $\Pr(\xi \leq E(\xi)/\delta) = 1 - \delta$ . But it is given that if  $m \geq m_{\mathcal{H}}(\epsilon\delta)$  for every distribution  $g$  it is  $E(\xi) \leq (\epsilon\delta)$ . So by substitution  $\Pr(\xi \leq (\epsilon\delta)/\delta) = 1 - \delta$  implies  $\Pr(\xi \leq \epsilon) = 1 - \delta$ . Now substitute back  $\xi$  and we conclude the proof.  $\square$

*Note 14.* Hence, we aim to design a learning algorithm  $\mathfrak{A}(\mathcal{S})$  that both fits the training set and is stable; i.e, keep both (I) and (II) in (2.3) small. As seen later, in certain learning problems, there may be a trade-off between empirical risk term (I) and (II) in (2.3). Consequently, we aim to upper bound (2.3) by upper bounding (I) and (II) individually and decide which term we should benefit against the other to achieve a certain total bound.

### 3. STABILITY AND ITS ASSOCIATION WITH OVER-FITTING

*Notation 15.* Consider a learning problem  $(\mathcal{H}, \mathcal{Z}, \ell)$ . Let  $\mathcal{S} = \{z_1, \dots, z_m\}$  be a training sample, and  $\mathfrak{A}$  be a learning algorithm with output  $\mathfrak{A}(\mathcal{S})$ .

*Note 16.* It is reasonable to consider that a learning algorithm  $\mathfrak{A}$  can be stable if a small change of the algorithm input does not change the algorithm output much. Mathematically formalizing this, we can say that if  $\mathcal{S}^{(i)} = \{z_1, \dots, z_{i-1}, z', z_{i+1}, \dots, z_m\}$  is another training dataset equal to  $\mathcal{S}$  but the  $i$ th element being replaced by another independent example  $z' \sim g$ , then a good learning algorithm  $\mathfrak{A}$  would produce a small value of

$$\ell(\mathfrak{A}(\mathcal{S}^{(i)}), z_i) - \ell(\mathfrak{A}(\mathcal{S}), z_i) \geq 0$$

**Definition 17.** A learning algorithm  $\mathfrak{A}$  is **on-average-replace-one-stable** with rate a decreasing function  $\epsilon : \mathbb{N} \rightarrow \mathbb{R}$  if for every distribution  $g$

$$(3.1) \quad \mathbb{E}_{\substack{\mathcal{S} \sim g \\ z' \sim g, i \sim U\{1, \dots, m\}}} (\ell(\mathfrak{A}(\mathcal{S}^{(i)}), z_i) - \ell(\mathfrak{A}(\mathcal{S}), z_i)) \leq \epsilon(m)$$

*Note 18.* The following result demonstrates the direct association of stability and over-fitting as defined in Definitions 10 & 17.

**Theorem 19.** For any learning algorithm  $\mathfrak{A}$  it is

$$(3.2) \quad \mathbb{E}_{\mathcal{S} \sim g} (R_g(\mathfrak{A}(\mathcal{S})) - \hat{R}_{\mathcal{S}}(\mathfrak{A}(\mathcal{S}))) = \mathbb{E}_{\substack{\mathcal{S} \sim g, z' \sim g \\ i \sim U\{1, \dots, m\}}} (\ell(\mathfrak{A}(\mathcal{S}^{(i)}), z_i) - \ell(\mathfrak{A}(\mathcal{S}), z_i))$$

where  $g$  is a distribution,  $\mathcal{S} = \{z_1, \dots, z_m\}$  and  $\mathcal{S}^{(i)} = \{z_1, \dots, z_{i-1}, z', z_{i+1}, \dots, z_m\}$  are training datasets with  $z', z_1, \dots, z_m \stackrel{\text{iid}}{\sim} g$ .

*Proof.* As  $z', z_1, \dots, z_m \stackrel{\text{iid}}{\sim} g$ , then for every  $i$

$$\mathbb{E}_{\mathcal{S} \sim g} (R_g(\mathfrak{A}(\mathcal{S}))) = \mathbb{E}_{\substack{\mathcal{S} \sim g \\ z' \sim g}} (\ell(\mathfrak{A}(\mathcal{S}), z')) = \mathbb{E}_{\substack{\mathcal{S} \sim g \\ z' \sim g}} (\ell(\mathfrak{A}(\mathcal{S}^{(i)}), z_i))$$

and

$$\mathbb{E}_{\mathcal{S} \sim g} (\hat{R}_{\mathcal{S}}(\mathfrak{A}(\mathcal{S}))) = \mathbb{E}_{\substack{\mathcal{S} \sim g \\ i \sim U\{1, \dots, m\}}} (\ell(\mathfrak{A}(\mathcal{S}^{(i)}), z_i))$$

□

*Note 20.* Hence, we desire to design learning algorithms corresponding to as small as possible (3.2).

#### 4. IMPLEMENTATION IN REGULARIZED LOSS LEARNING PROBLEMS

**Definition 21.** A Regularized Loss Minimization (RLM) learning problem  $(\mathcal{H}, \mathcal{Z}, \ell)$  with a regularization function  $J : \mathcal{H} \rightarrow \mathbb{R}$  aims at a RLM learning rule that is the minimizer

$$(4.1) \quad h^* = \arg \min_{h \in \mathcal{H}} (\hat{R}_{\mathcal{S}}(h) + J(h))$$

where  $\hat{R}_{\mathcal{S}}(\cdot) = \frac{1}{m} \sum_{i=1}^m \ell(\cdot, z_i)$ , and  $\mathcal{S} = \{z_1, \dots, z_m\} \subset$  an IID training sample.

*Remark 22.* The motivation for considering the regularization function  $J$  in (4.1) is to: (1.) control complexity and (2.) improve stability; as we will see later.

*Note 23.* Here, we make our example more specific and narrow it to the Ridge RLM learning problem (could have been LASSO etc.).

**Definition 24.** The Ridge RLM learning problem  $(\mathcal{H}, \mathcal{Z}, \ell)$ , with  $\mathcal{H} = \mathcal{W} \subset \mathbb{R}^d$ , uses regularization function  $J(w; \lambda) = \lambda \|w\|_2^2$  with  $\lambda > 0$ ,  $w \in \mathcal{W}$  and produces learning rule

$$(4.2) \quad \mathfrak{A}(\mathcal{S}) = \arg \min_{w \in \mathcal{W}} \left( \hat{R}_{\mathcal{S}}(w) + \lambda \|w\|_2^2 \right)$$

*Note 25.* Recall (Term 1) how the regularization function in Ridge RLM learning problem  $(\mathcal{H}, \mathcal{Z}, \ell)$  penalizes complexity. Essentially, it implies a sequence of hypothesis  $\mathcal{H}_1 \subset \mathcal{H}_2 \subset \dots$  with  $\mathcal{H}_i = \{w \in \mathbb{R}^d : \|w\|_2 < i\}$  due to duality of the corresponding minimization problem.

*Note 26.* Below, we will try to analyze the behavior of Ridge RLM learning rule (4.2) w.r.t. the Risk decomposition (2.3). In particular, to upper bounded w.r.t. the shrinkage term  $\lambda$ , training sample size  $m$ , and other characteristics.

#### 4.1. Bounding the empirical risk (I) in (2.3).

*Note 27.* From (4.2), we have

$$\begin{aligned} \hat{R}_{\mathcal{S}}(\mathfrak{A}(\mathcal{S})) &\leq \hat{R}_{\mathcal{S}}(\mathfrak{A}(\mathcal{S})) + \lambda \|\mathfrak{A}(\mathcal{S})\|_2^2 \\ &\leq \hat{R}_{\mathcal{S}}(w) + \lambda \|w\|_2^2; \quad \forall w \in \mathcal{W} \end{aligned}$$

and by taking expectations w.r.t.  $\mathcal{S}$ , it is

$$(4.3) \quad \mathbb{E}_{\mathcal{S} \sim g} \left( \hat{R}_{\mathcal{S}}(\mathfrak{A}(\mathcal{S})) \right) \leq R_g(w) + \lambda \|w\|_2^2; \quad \forall w \in \mathcal{W}$$

because  $\mathbb{E}_{\mathcal{S} \sim g} \left( \hat{R}_{\mathcal{S}}(\cdot) \right) = \frac{1}{m} \sum_{i=1}^m \mathbb{E}_{\mathcal{S} \sim g} (\ell(\cdot, z_i)) = R_g(\cdot)$ .

*Note 28.* From (4.3), we observe that part (I) in the expected risk decomposition (2.3), (aka the upper bound of the expected empirical risk) increases with the regularization term  $\lambda > 0$ . (!!!) –Although anticipated, it did not start well.

#### 4.2. Bounding the empirical risk (II) in (2.3).

*Note 29.* As we will see to bound (II) in (2.3) we will have to impose an additional condition on the behavior of loss function apart from convexity; e.g. Lipschitzness.

**Assumption 30.** The loss function  $\ell(\cdot, z)$  in (4.2) is convex for any  $z \in \mathcal{Z}$ .

*Note 31.* Let  $\tilde{R}_{\mathcal{S}}(w) = \hat{R}_{\mathcal{S}}(w) + \lambda \|w\|_2^2$ .  $\tilde{R}_{\mathcal{S}}(\cdot)$  is  $2\lambda$ -strongly convex as the sum of a convex function  $\hat{R}_{\mathcal{S}}(\cdot)$  (Assumption 30) and a  $2\lambda$ -strongly convex function  $J(\cdot; \lambda) = \lambda \|\cdot\|_2^2$  (results directly from Definition 14 in Lecture notes 2).



**Fact 32.** (To be used in Note 33) If  $f$  is  $\lambda$ -strongly convex and  $u$  is a minimizer of  $f$  then for any  $w$

$$f(w) - f(u) \geq \frac{\lambda}{2} \|w - u\|^2$$

*Note 33.* Let  $\mathfrak{A}(\mathcal{S})$  be the Ridge learning algorithm output minimizing (4.2). Because  $\tilde{R}_{\mathcal{S}}(\cdot)$  is  $2\lambda$ -strongly convex and  $\mathfrak{A}(\mathcal{S})$  is its minimizer, according to Fact 32, for  $\mathfrak{A}(\mathcal{S})$  and any  $w \in \mathcal{W}$ , it is

$$(4.4) \quad \tilde{R}_{\mathcal{S}}(w) - \tilde{R}_{\mathcal{S}}(\mathfrak{A}(\mathcal{S})) \geq \lambda \|w - \mathfrak{A}(\mathcal{S})\|^2, \quad \forall w \in \mathcal{W}$$

*Note 34.* Also, for any  $w, u \in \mathcal{W}$ , it is

$$\begin{aligned} \tilde{R}_{\mathcal{S}}(w) - \tilde{R}_{\mathcal{S}}(u) &= \left( \hat{R}_{\mathcal{S}}(w) + \lambda \|w\|_2^2 \right) - \left( \hat{R}_{\mathcal{S}}(u) + \lambda \|u\|_2^2 \right) \\ &= \left( \hat{R}_{\mathcal{S}^{(i)}}(w) + \lambda \|w\|_2^2 \right) - \left( \hat{R}_{\mathcal{S}^{(i)}}(u) + \lambda \|u\|_2^2 \right) \\ &\quad + \frac{\ell(w, z_i) - \ell(u, z_i)}{m} + \frac{\ell(u, z') - \ell(w, z')}{m} \\ &= \tilde{R}_{\mathcal{S}^{(i)}}(w) - \tilde{R}_{\mathcal{S}^{(i)}}(u) + \frac{\ell(w, z_i) - \ell(u, z_i)}{m} + \frac{\ell(\textcolor{red}{u}, z') - \ell(\textcolor{red}{w}, z')}{m} \end{aligned}$$

Choosing  $w = \mathfrak{A}(\mathcal{S}^{(i)})$  and  $u = \mathfrak{A}(\mathcal{S})$ , and the fact that  $\tilde{R}_{\mathcal{S}^{(i)}}(\mathfrak{A}(\mathcal{S}^{(i)})) \leq \tilde{R}_{\mathcal{S}^{(i)}}(\mathfrak{A}(\mathcal{S}))$ , it is

$$(4.5) \quad \tilde{R}_{\mathcal{S}}(\mathfrak{A}(\mathcal{S}^{(i)})) - \tilde{R}_{\mathcal{S}}(\mathfrak{A}(\mathcal{S})) \leq \frac{\ell(\mathfrak{A}(\mathcal{S}^{(i)}), z_i) - \ell(\mathfrak{A}(\mathcal{S}), z_i)}{m} + \frac{\ell(\mathfrak{A}(\textcolor{red}{\mathcal{S}}), z') - \ell(\mathfrak{A}(\textcolor{red}{\mathcal{S}^{(i)}}), z')}{m}$$

*Note 35.* Then (4.4) and (4.5) imply

$$(4.6) \quad \lambda \|\mathfrak{A}(\mathcal{S}^{(i)}) - \mathfrak{A}(\mathcal{S})\| \leq \frac{\ell(\mathfrak{A}(\mathcal{S}^{(i)}), z_i) - \ell(\mathfrak{A}(\mathcal{S}), z_i)}{m} + \frac{\ell(\mathfrak{A}(\textcolor{red}{\mathcal{S}}), z') - \ell(\mathfrak{A}(\textcolor{red}{\mathcal{S}^{(i)}}), z')}{m}$$

*Note 36.* Now that we brought it in form (4.6), we can impose/use an additional assumption on the loss to bound it. In this example we use Lipschitzness.

**Assumption 37.** The loss function  $\ell(\cdot, z)$  in (4.2) is convex and  $\rho$ -Lipschitz for any  $z \in \mathcal{Z}$ .

*Note 38.* Given  $\rho$ -Lipschitzness in Assumption 37, it is

$$(4.7) \quad \ell(\mathfrak{A}(\mathcal{S}^{(i)}), z_i) - \ell(\mathfrak{A}(\mathcal{S}), z_i) \leq \rho \|\mathfrak{A}(\mathcal{S}^{(i)}) - \mathfrak{A}(\mathcal{S})\|$$

$$(4.8) \quad \ell(\mathfrak{A}(\mathcal{S}), z') - \ell(\mathfrak{A}(\mathcal{S}^{(i)}), z') \leq \rho \|\mathfrak{A}(\mathcal{S}^{(i)}) - \mathfrak{A}(\mathcal{S})\|$$

and hence plugging 4.7 and (4.8) in (4.6) yields

$$(4.9) \quad \|\mathfrak{A}(\mathcal{S}^{(i)}) - \mathfrak{A}(\mathcal{S})\| \leq 2 \frac{\rho}{\lambda m}$$

Note 39. Plugging (4.9) in (4.7) yields

$$\ell(\mathfrak{A}(\mathcal{S}^{(i)}), z_i) - \ell(\mathfrak{A}(\mathcal{S}), z_i) \leq 2 \frac{\rho^2}{\lambda m}$$

Note 40. Using Theorem 19, we get an upper bound for the stability / over-fitting

$$\mathbb{E}_{\mathcal{S} \sim g} \left( R_g(\mathfrak{A}(\mathcal{S})) - \hat{R}_{\mathcal{D}}(\mathfrak{A}(\mathcal{S})) \right) = \mathbb{E}_{\substack{\mathcal{S} \sim g, z' \sim g \\ i \sim \mathcal{U}\{1, \dots, m\}}} \left( \ell(\mathfrak{A}(\mathcal{S}^{(i)}), z_i) - \ell(\mathfrak{A}(\mathcal{S}), z_i) \right) \leq 2 \frac{\rho^2}{\lambda m}$$

Note 41. After this saga, the researcher could come to the conclusion that: A Ridge RLM learning problem  $(\mathcal{H}, \mathcal{Z}, \ell)$  with the loss function which is convex and  $\rho$ -Lipschitz, regularizer  $J(\cdot; \lambda) = \lambda \|\cdot\|^2$ ,  $\lambda > 0$ , and learning rule trained against an iid sample  $\mathcal{S} = \{z_i\}_{i=1}^m$  from  $g$  is on-average-replace-one-stable with rate  $\epsilon(m) = 2 \frac{\rho^2}{\lambda m}$ ; i.e.

$$(4.10) \quad \mathbb{E}_{\mathcal{S} \sim g} \left( R_g(\mathfrak{A}(\mathcal{S})) - \hat{R}_{\mathcal{S}}(\mathfrak{A}(\mathcal{S})) \right) \leq 2 \frac{\rho^2}{\lambda m}$$

Note 42. From (4.10), we see that stability improves (and over-fitting decreases) as the shrinkage parameter  $\lambda$  increases.

### 4.3. Bounding the Risk (2.3).

Note 43. Given the bounds (4.3) and (4.10), the decomposition of the expected Risk in (2.3) yields that: A Ridge RLM learning problem  $(\mathcal{H}, \mathcal{Z}, \ell)$  with the loss function which is convex and  $\rho$ -Lipschitz, regularizer  $J(\cdot; \lambda) = \lambda \|\cdot\|^2$ ,  $\lambda > 0$ , and learning rule trained against an iid sample  $\mathcal{S} = \{z_i\}_{i=1}^m$  from  $g$  has Expected Risk bound

$$(4.11) \quad \mathbb{E}_{\mathcal{S} \sim g} (R_g(\mathfrak{A}(\mathcal{S}))) \leq \underbrace{R_g(w) + \lambda \|w\|_2^2}_{(I)} + \underbrace{2 \frac{\rho^2}{\lambda m}}_{(II)}; \quad \forall w \in \mathcal{W}$$

Note 44. From (4.11), we see that there is a trade-off between Empirical Risk (I) and stability/overfitting (II) with regards the regularization parameter  $\lambda$ . It is desirable to use the optimal  $\lambda > 0$  corresponding to the smallest bound in (4.11); it has to both fit the training data well (but perhaps not too well) and be very stable to different training data from the same  $g$  (but perhaps not too stable)!

**Assumption 45.** Assume that the learning problem is additionally  $B$ -bounded by  $B > 0$ ; i.e.  $\mathcal{H} = \{w \in \mathbb{R}^d : \|w\|_2 \leq B\}$ .

Note 46. If additionally the learning problem is  $B$ -bounded then the upper bound in (4.11) becomes

$$(4.12) \quad \mathbb{E}_{\mathcal{S} \sim g} (R_g(\mathfrak{A}(\mathcal{S}))) \leq \underbrace{\min_{w \in \mathcal{H}} R_g(w) + \lambda B^2}_{(I)} + \underbrace{2 \frac{\rho^2}{\lambda m}}_{(II)}$$

*Note 47.* Furthermore, if we choose a shrinkage parameter  $\lambda_m = \sqrt{\frac{2}{m}} \frac{\rho}{B}$  in (4.2) the upper bound in (4.11) becomes

$$(4.13) \quad \mathbb{E}_{\mathcal{S} \sim g} (R_g (\mathfrak{A} (\mathcal{S}))) \leq \min_{w \in \mathcal{H}} R_g (w) + \lambda_m B \sqrt{\frac{8}{m}}$$

#### 4.4. Deriving PAC guarantees.

*Note 48.* In particular, if the size  $m$  of the training sample  $\mathcal{S}$  is

$$m \geq \frac{\lambda_m^2 B^2 8}{\epsilon^2} = \frac{8\rho^2 B^2}{\epsilon^2}$$

for some  $\epsilon > 0$  then for every distribution  $g$ , the upper bound in (4.11) becomes

$$(4.14) \quad \mathbb{E}_{\mathcal{S} \sim g} (R_g (\mathfrak{A} (\mathcal{S}))) \leq \min_{w \in \mathcal{H}} R_g (w) + \epsilon$$

and hence we can have a PAC guarantee that is summarized in the following.

*Summary 49.* Let  $(\mathcal{H}, \mathcal{Z}, \ell)$  be a learning problem convex-Lipschitz-bounded with parameters  $\rho$  and  $B$ , and let  $m$  be the training data size. The associated Ridge Regularized Loss Minimization rule with regularization function  $\lambda_m = \sqrt{\frac{2}{m}} \frac{\rho}{B}$  satisfies

$$\mathbb{E}_{\mathcal{S} \sim g} (R_g (\mathfrak{A} (\mathcal{S}))) \leq \min_{w \in \mathcal{H}} R_g (w) + \lambda_m B \sqrt{\frac{8}{m}}$$

Moreover, if  $m \geq \frac{8\rho^2 B^2}{\epsilon^2}$ ,  $\epsilon > 0$  then for every distribution  $g$  we can get a PAC -guarantee

$$\mathbb{E}_{\mathcal{S} \sim g} (R_g (\mathfrak{A} (\mathcal{S}))) \leq \min_{w \in \mathcal{H}} R_g (w) + \epsilon$$

## Lecture notes 4: Gradient descent

Lecturer &amp; author: Georgios P. Karagiannis

georgios.karagiannis@durham.ac.uk

**Aim.** To introduce gradient descent, its motivation, description, practical tricks, analysis in the convex scenario, and implementation.

### Reading list & references:

- (1) Shalev-Shwartz, S., & Ben-David, S. (2014). Understanding machine learning: From theory to algorithms. Cambridge university press.
  - Ch. 14.1 Gradient Descent

## 1. MOTIVATIONS

**Problem 1.** Consider a learning problem  $(\mathcal{H}, \mathcal{Z}, \ell)$ . Learning may involve the computation of the minimizer  $h^* \in \mathcal{H}$ , where  $\mathcal{H}$  is a class of hypotheses, of the empirical risk function (ERF)  $\hat{R}(h) = \frac{1}{n} \sum_{i=1}^n \ell(h, z_i)$  given a finite sample  $\{z_i; i = 1, \dots, n\}$  generated from the data generating model  $g(\cdot)$  and using loss  $\ell(\cdot)$ ; that is

$$(1.1) \quad h^* = \arg \min_{h \in \mathcal{H}} \left( \hat{R}(h) \right) = \arg \min_{h \in \mathcal{H}} \left( \frac{1}{n} \sum_{i=1}^n \ell(h, z_i) \right)$$

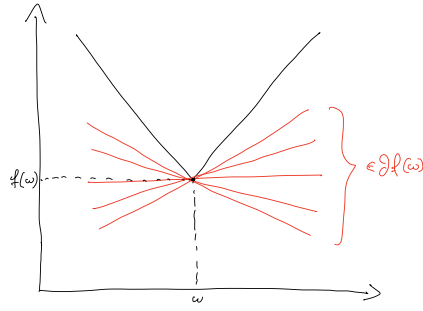
or its corresponding regularized version. If analytical minimization of (1.1) is impossible or impractical, numerical procedures can be applied; eg Gradient Descent (GD) algorithms. Such approaches introduce numerical errors in the solution.

## 2. SUBGRADIENT

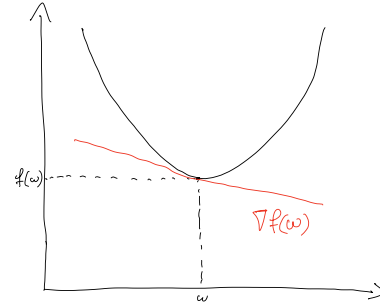
**Definition 2.** Vector  $v$  is called subgradient of a function  $f : S \rightarrow \mathbb{R}$  at  $w \in S$  if

$$(2.1) \quad \forall u \in S, \quad f(u) \geq f(w) + \langle u - w, v \rangle$$

*Note 3.* There may be more than one subgradients of a function at a specific point. As seen by (2.1), subgradients are the slopes of all the lines passing through the point  $(w, f(w))$  and been under the function  $f(\cdot)$ .



(A) subgradients satisfying (2.1) in the non-differentiable case



(B) gradient satisfying the equality in (2.1) in the differentiable case

**Definition 4.** The set of subgradients of function  $f : S \rightarrow \mathbb{R}$  at  $w \in S$  is denoted by  $\partial f(w)$ .

**Fact 5.** Properties of subgradient sets useful for the subgradient construction

- (1) If function  $f : S \rightarrow \mathbb{R}$  is differentiable at  $w$  then the only subgradient of  $f$  at  $w$  is the gradient  $\nabla f(w)$ , and (2.1) is equality; i.e.  $\partial f(w) = \{\nabla f(w)\}$ .
- (2) for constants  $\alpha, \beta$  and convex function  $f(\cdot)$ , it is

$$\partial(\alpha f(w) + \beta) = \alpha(\partial f(w)) = \{\alpha v : v \in \partial f(w), \}$$

- (3) for convex functions  $f(\cdot)$  and  $g(\cdot)$ , it is

$$\partial(f(w) + g(w)) = \partial f(w) + \partial g(w) = \{v + u : v \in \partial f(w), \text{ and } u \in \partial g(w)\}$$

**Example 6.** Consider the function  $f : \mathbb{R} \rightarrow \mathbb{R}_+$  with  $f(w) = |w| = \begin{cases} w & w \geq 0 \\ -w & w < 0 \end{cases}$ . Find the set of subgradients  $\partial f(w)$  for each  $w \in \mathbb{R}$ .

**Solution.** Using Fact 5, it is  $\partial f(w) = 1$  for  $w > 0$  and  $\partial f(w) = -1$  for  $w < 0$  as  $f$  is differentiable for  $x \neq 0$ . At  $x = 0$ ,  $f$  is not differentiable; hence from condition (2.1) it is

$$\forall u \in \mathbb{R}, |u| \geq |0| + (u - 0)v$$

which is satisfied for  $v \in [-1, 1]$ . Hence,

$$\partial f(w) = \begin{cases} \{-1\} & , w < 0 \\ [-1, 1] & , w = 0 \\ \{1\} & , w > 0 \end{cases}$$

### 3. DESCRIPTION OF GRADIENT DESCENT

**Problem 7.** For the sake of notation simplicity and generalization, we will present Gradient Descent (GD) in the following minimization problem

$$(3.1) \quad w^* = \arg \min_{w \in \mathcal{H}} (f(w))$$

where here  $f : \mathbb{R}^d \rightarrow \mathbb{R}$ , and  $w \in \mathcal{H} \subseteq \mathbb{R}^d$ ;  $f(\cdot)$  is the function to be minimized, e.g.,  $f(\cdot)$  can be an empirical risk function  $\hat{R}(\cdot)$ .

**Algorithm 8.** *Gradient Descent (GD) algorithm with learning rate  $\eta_t > 0$  for the solution of the minimization problem (3.1)*

For  $t = 1, 2, 3, \dots$  iterate:

(1) compute

$$(3.2) \quad w^{(t+1)} = w^{(t)} - \eta_t v_t; \text{ where } v_t \in \partial f(w^{(t)})$$

(2) terminate if a termination criterion is satisfied, e.g.

If  $t \geq T_{\max}$  then STOP

*Note 9.* (Intuition) Assume  $f$  is differentiable. GD produces a chain  $\{w^{(t)}\}$  that drifts towards a minimum  $w^*$ . The chain is directed towards the opposite direction of that of the subgradient  $\nabla f(\cdot)$  and at a rate controlled by the learning rate  $\eta_t$ .

*Note 10.* (More intuition) Assume  $f$  is differentiable. Consider the (1st order) Taylor polynomial for the approximation of  $f(w)$  in a small area around  $u$  (i.e.  $\|v - u\| = \text{small}$ )

$$f(u) \approx P(u) = f(w) + \langle u - w, \nabla f(w) \rangle$$

Assuming convexity for  $f$ , it is

$$(3.3) \quad f(u) \geq \underbrace{f(w) + \langle u - w, \nabla f(w) \rangle}_{=P(u;w)}$$

meaning that  $P$  lower bounds  $f$ . Hence we could design an updating mechanism producing  $w^{(t+1)}$  which is nearby  $w^{(t)}$  (small steps) and which minimize the linear approximation  $P(w)$  of  $f(w)$  at  $w^{(t)}$

$$(3.4) \quad P(w; w^{(t)}) = f(w^{(t)}) + \langle w - w^{(t)}, \nabla f(w^{(t)}) \rangle.$$

while hoping that this mechanism would push the produced chain  $\{w^{(t)}\}$  towards the minimum because of (3.3). Hence we could recursively minimize the linear approximation (3.4) and the

distance between the current state  $w^{(t)}$  and the next  $w$  value to produce  $w^{(t+1)}$ ; namely

$$\begin{aligned}
 (3.5) \quad w^{(t+1)} &= \arg \min_{\forall w} \left( \frac{1}{2} \|w - w^{(t)}\|^2 + \eta P(w; w^{(t)}) \right) \\
 &= \arg \min_{\forall w} \left( \frac{1}{2} \|w - w^{(t)}\|^2 + \eta \left( f(w^{(t)}) + \langle w - w^{(t)}, \nabla f(w^{(t+1)}) \rangle \right) \right) \\
 &= w^{(t)} - \eta \nabla f(w^{(t)})
 \end{aligned}$$

where parameter  $\eta > 0$  controls the trade off in (3.5).

*Note 11.* Given  $T$  iterations of GD algorithm, the output of GD can be (but not a exclusively),

(1) the average (after discarding the first few iterations of  $w^{(t)}$  for stability reasons)

$$(3.6) \quad w_{\text{GD}}^{(T)} = \frac{1}{T} \sum_{t=1}^T w^{(t)}$$

(2) or the best value discovered

$$w_{\text{GD}}^{(T)} = \arg \min_{\forall w_t} \left( f(w^{(t)}) \right)$$

(3) or the last value discovered

$$w_{\text{GD}}^{(T)} = w^{(T)}$$

*Note 12.* GD output (e.g. in Note 11) converges to a local minimum,  $w_{\text{GD}}^{(T)} \rightarrow w_*$  (in some sense), under different sets of regularity conditions (some are weaker other stronger). Section 4 has a brief analysis.

*Note 13.* The parameter  $\eta_t$  is called learning rate (or step size, gain). It determines the size of the steps GD takes to reach a (local) minimum.  $\{\eta_t\}$  is a non-negative sequence and it is chosen by the practitioner. In principle, regularity conditions (Note 12) often imply restrictions on the decay of  $\{\eta_t\}$  which guide the practitioner to parametrize it properly. Some popular choices of learning rate  $\eta_t$  are:

- (1) constant;  $\eta_t = \eta$ , for where  $\eta > 0$  is a small value. The rationale is that GD chain  $\{w_t\}$  performs constant small steps towards the (local) minimum  $w_*$  and then oscillate around it.
- (2) decreasing and converging to zero;  $\eta_t \searrow$  with  $\lim_{t \rightarrow \infty} \eta_t = 0$ . E.g.  $\eta_t = \left(\frac{C}{t}\right)^\varsigma$  where  $\varsigma \in [0.5, 1]$  and  $C > 0$ . The rationale is that GD algorithm starts by performing larger steps (controlled by  $C$ ) at the beginning to explore the area for discovering possible minima. Also it reduces the size of those steps with the iterations (controlled by  $\varsigma$ ) such that eventually when the chain  $\{w_t\}$  is close to a possible minimum  $w_*$  value to converge and do not overshoot.
- (3) decreasing and converging to a tiny value  $\tau_*$ ;  $\eta_t \searrow$  with  $\lim_{t \rightarrow \infty} \eta_t = \tau_*$  E.g.  $\eta_t = \left(\frac{C}{t}\right)^\varsigma + \tau_*$  with  $\varsigma \in (0.5, 1]$ ,  $C > 0$ , and  $\tau_* \approx 0$ . Same as previously, but the algorithm aims at oscillating around the detected local minimum.
- (4) constant until an iteration  $T_0$  and then decreasing; Eg  $\eta_t = \left(\frac{C}{\max(t, T_0)}\right)^\varsigma$  with  $\varsigma \in [0.5, 1]$  and  $C > 0$ , and  $T_0 < T$ . The rationale is that at the first stage of the iterations (when  $t \leq T_0$ ) the algorithm may need a constant large steps for a significant number of iterations

$T_0$  in order to explore the domain; and hence in order for the chain  $\{w_t\}$  to reach the area around the (local) minimum  $w_*$ . In the second stage, hoping that the chain  $\{w_t\}$  may be in close proximity to the (local) minimum  $w_*$  the algorithm progressively performs smaller steps to converge towards the minimum  $w_*$ . The first stage ( $t \leq T_0$ ) is called burn-in; the values  $\{w_t\}$  produced during the burn-in ( $t \leq T_0$ ) are often discarded/ignored from the output of the GD algorithm.

- Parameters  $C, \varsigma, \tau_*, T_0$  may be chosen based on pilot runs against a small fraction of the training data set.

*Note 14.* There are several practical termination criteria that can be used in GD Algorithm 8(step 2). They aim to terminate the recursion in practice. Some popular termination criteria are

- (1) terminate when the gradient is sufficiently close to zero; i.e. if  $\|\nabla f(w^{(t)})\| \leq \epsilon$ , for some pre-specified tiny  $\epsilon > 0$  then STOP
- (2) terminate when the chain  $w^{(t)}$  does not change; i.e. if  $\|w^{(t+1)} - w^{(t)}\| \leq \epsilon \|w^{(t)}\|$  for some pre-specified tiny  $\epsilon > 0$  then STOP
- (3) terminate when a pre-specified number of iterations  $T$  is performed; i.e. if  $t \geq T$  then STOP

Here (1) may be deceive if the chain is in a flat area, (2) may be deceived if the learning rate become too small, (3) is obviously a last resort.

#### 4. ANALYSIS OF GRADIENT DESCENT (ALGORITHM 8)

*Note 15.* Recall we address the minimization Problem 7 under Assumptions 16.

**Assumption 16.** *For the sake of the analysis of the GD, let us consider:*

- (1) *The function  $f(\cdot)$  is convex and Lipschitz*
- (2) *GD has a constant learning rate  $\eta_t = \eta$ ,*
- (3) *GD output  $w_{GD}^{(T)} = \frac{1}{T} \sum_{t=1}^T w^{(t)}$*

**Lemma 17.** *Let  $\{v_t; t = 1, \dots, T\}$  be a sequence of vectors. Any algorithm with  $w^{(1)} = 0$  and  $w^{(t+1)} = w^{(t)} - \eta v_t$  for  $t = 1, \dots, T$  satisfies*

No need to memorize

$$(4.1) \quad \sum_{t=1}^T \langle w^{(t)} - w^*, v_t \rangle \leq \frac{\|w^*\|^2}{2\eta} + \frac{\eta}{2} \sum_{t=1}^T \|v_t\|^2$$

*Proof.* Omitted; see the Exercise ?? in the Exercise sheet 1. □

*Note 18.* To find an upper bound of the GD error, we try to bound the error  $f(w_{GD}^{(T)}) - f(w^*)$  with purpose to use Lemma 17.

*Note 19.* Consider the minimization problem (3.1). Given Assumptions 16, the error can be bounded as

$$(4.2) \quad f(w_{GD}^{(T)}) - f(w^*) \leq \frac{\|w^*\|^2}{2\eta T} + \frac{\eta}{2} \frac{1}{T} \sum_{t=1}^T \|v_t\|^2$$

where  $v_t \in \partial f(w^{(t)})$ . If  $f(\cdot)$  is differentiable then  $v_t = \nabla f(w^{(t)})$



*Proof.* It is<sup>1</sup>

$$\begin{aligned}
 f(w_{\text{GD}}^{(T)}) - f(w^*) &= f\left(\frac{1}{T} \sum_{t=1}^T w_t\right) - f(w^*) \\
 (4.3) \quad &\leq \frac{1}{T} \sum_{t=1}^T (f(w_t) - f(w^*)) && \text{(by Jensen's inequality)} \\
 &\leq \frac{1}{T} \sum_{t=1}^T \langle w^{(t)} - w^*, v_t \rangle && \text{(by convexity of } f(\cdot) \text{)} \\
 (4.4) \quad &\leq \frac{\|w^*\|^2}{2\eta T} + \frac{\eta}{2} \frac{1}{T} \sum_{t=1}^T \|v_t\|^2 && \text{(by roceeding Lemma)}
 \end{aligned}$$

□

*Note 20.* Note 19 shows that it is important to bound the (sub-)gradient in (4.2) in a meaningful manner. Lemma 21 shows that if we assume Lipschitzness as well, the (sub-)gradient has the so-called self-bounded behavior.

**Lemma 21.** <sup>2</sup>  $f : S \rightarrow \mathbb{R}$  is  $\rho$ -Lipschitz over an open convex set  $S$  if and only if for all  $w \in S$  and  $v \in \partial f(w)$  it is  $\|v\| \leq \rho$ .

*Proof.*  $\implies$  Let  $f : S \rightarrow \mathbb{R}$  be  $\rho$ -Lipschitz over convex set  $S$ ,  $w \in S$  and  $v \in \partial f(w)$ .

- Since  $S$  is open we get that there exist  $\epsilon > 0$  such as  $u := w + \epsilon \frac{v}{\|v\|}$  where  $u \in S$ . So  $\langle u - w, v \rangle = \epsilon \|v\|$  and  $\|u - w\| = \epsilon$ .
- From the subgradient definition we get

$$f(u) - f(w) \geq \langle u - w, v \rangle = \epsilon \|v\|$$

- From the Lipschitzness of  $f(\cdot)$  we get

$$f(u) - f(w) \leq \rho \|u - w\| = \rho \epsilon$$

Therefore  $\|v\| \leq \rho$ .

For  $\Leftarrow$  see Exercise 4 in the Exercise sheet. □

*Note 22.* The following summaries Note 19 and Lemma 21 with respect to the GD algorithm satisfying Assumption 16.

*Note 23.* Let  $f(\cdot)$  be a convex and  $\rho$ -Lipschitz function. If we run GD algorithm of  $f$  with learning rate  $\eta > 0$  for  $T$  steps the output  $w_{\text{GD}}^{(T)} = \frac{1}{T} \sum_{t=1}^T w^{(t)}$  satisfies

$$f(w_{\text{GD}}^{(T)}) - f(w^*) \leq \frac{\|w^*\|^2}{2\eta T} + \frac{\eta}{2} \frac{1}{T} \sum_{t=1}^T \|v_t\|^2$$

<sup>1</sup>Jensen's inequality for convex  $f(\cdot)$  is  $f(\mathbb{E}(x)) \leq \mathbb{E}(f(x))$

<sup>2</sup>If this was a Homework there would be a Hint:

- If  $S$  is open there exist  $\epsilon > 0$  such as  $u = w + \epsilon \frac{v}{\|v\|}$  such as  $u \in S$

where  $\|v_t\| \leq \rho$ ,  $v_t \in \partial f(w^{(t)})$ . If  $f(\cdot)$  is differentiable then  $v_t = \nabla f(w^{(t)})$ .

*Proof.* Straightforward from Lemma 17 and Note 19.  $\square$

*Note 24.* The following shows that a given learning rate depending on the iteration  $t$ , we can reduce the upper bound of the error as well as find the number of required iterations to achieve convergence.

*Note 25.* (Cont Prop. 23) Let  $f(\cdot)$  be a convex and  $\rho$ -Lipschitz function, and let  $\mathcal{H} = \{w \in \mathbb{R} : \|w\| \leq B\}$ . Assume we run GD algorithm of  $f(\cdot)$  with learning rate  $\eta_t = \sqrt{\frac{B^2}{\rho^2 T}}$  for  $T$  steps, and output  $w_{\text{GD}}^{(T)} = \frac{1}{T} \sum_{t=1}^T w^{(t)}$ . Then

(1) upper bound on the sub-optimality is

$$(4.5) \quad f(w_{\text{GD}}^{(T)}) - f(w^*) \leq \frac{B\rho}{\sqrt{T}}$$

(2) a given level off accuracy  $\varepsilon$  such that  $f(w_{\text{GD}}^{(T)}) - f(w^*) \leq \varepsilon$  can be achieved after  $T$  iterations

$$T \geq \frac{B^2 \rho^2}{\varepsilon^2}.$$

*Proof.* Part 1 is a simple substitution from Proposition 23, and part 2 is implied from part 1.  $\square$

The result on Proposition 25 heavily relies on setting suitable values for  $B$  and  $\rho$  which is rather a difficult task to be done in very complicated learning problems (e.g., learning a neural network).

*Note 26.* The above results from the analysis of the GD also hold for the GD with subgradients; just replace  $\nabla f(\cdot)$  with any  $v_t$  such that  $v_t \in \partial f(\cdot)$ .

## 5. EXAMPLES <sup>3</sup>

**Example 27.** Consider the simple Normal linear regression problem where the dataset  $\{z_i = (y_i, x_i)\}_{i=1}^n \in \mathcal{S}$  is generated from a Normal data generating model

$$(5.1) \quad \begin{pmatrix} y_i \\ x_i \end{pmatrix} \stackrel{\text{iid}}{\sim} \text{N} \left( \begin{pmatrix} \mu_y \\ \mu_x \end{pmatrix}, \begin{bmatrix} \sigma_y^2 & \rho \sqrt{\sigma_y^2 \sigma_x^2} \\ \rho \sqrt{\sigma_y^2 \sigma_x^2} & \sigma_x^2 \end{bmatrix} \right)$$

for  $i = 1, \dots, n$ . Consider a hypothesis space  $\mathcal{H}$  of linear functions  $h : \mathbb{R}^2 \rightarrow \mathbb{R}$  with  $h(w) = w_1 + w_2 x$ . The exact solution (which we pretend we do not know) is given as

$$(5.2) \quad \begin{pmatrix} w_1^* \\ w_2^* \end{pmatrix} = \begin{pmatrix} \mu_y - \rho \frac{\sigma_y}{\sigma_x} \mu_x \\ \rho \frac{\sigma_y}{\sigma_x} \end{pmatrix}.$$

To learn the optimal  $w^* = (w_1^*, w_2^*)^\top$ , we consider a loss  $\ell(w, z_i = (x_i, y_i)^\top) = (y_i - [w_1 + w_2 x_i])^2$ , which leads to the minimization problem

$$w^* = \arg \min_w \left( \hat{R}_{\mathcal{S}}(w) \right) = \arg \min_w \left( \frac{1}{n} \sum_{i=1}^n (y_i - w_1 - w_2 x_i)^2 \right)$$

<sup>3</sup>Code is available in [https://github.com/georgios-stats/Machine\\_Learning\\_and\\_Neural\\_Networks\\_III\\_Epiphany\\_2024/tree/main/Lecture\\_handouts/code/04.Gradient\\_descent/example\\_1.R](https://github.com/georgios-stats/Machine_Learning_and_Neural_Networks_III_Epiphany_2024/tree/main/Lecture_handouts/code/04.Gradient_descent/example_1.R)

The GD Algorithm 8 with learning rate  $\eta$  is

For  $t = 1, 2, 3, \dots$  iterate:

(1) compute

$$(5.3) \quad w^{(t+1)} = w^{(t)} - \eta v_t, \quad \text{where } v_t = \begin{pmatrix} 2w_1^{(t)} + 2w_2^{(t)}\bar{x} - 2\bar{y} \\ 2w_1^{(t)}\bar{x} + 2w_2^{(t)}\bar{x}^2 - 2y^\top x \end{pmatrix}$$

(2) terminate if a termination criterion is satisfied, e.g.

If  $t \geq T$  then STOP

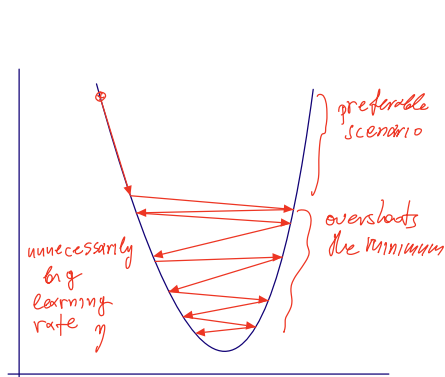
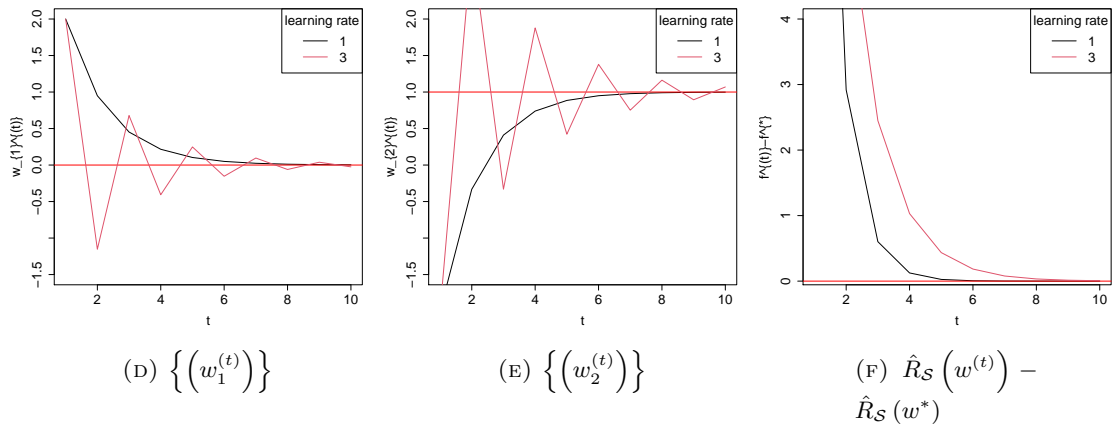
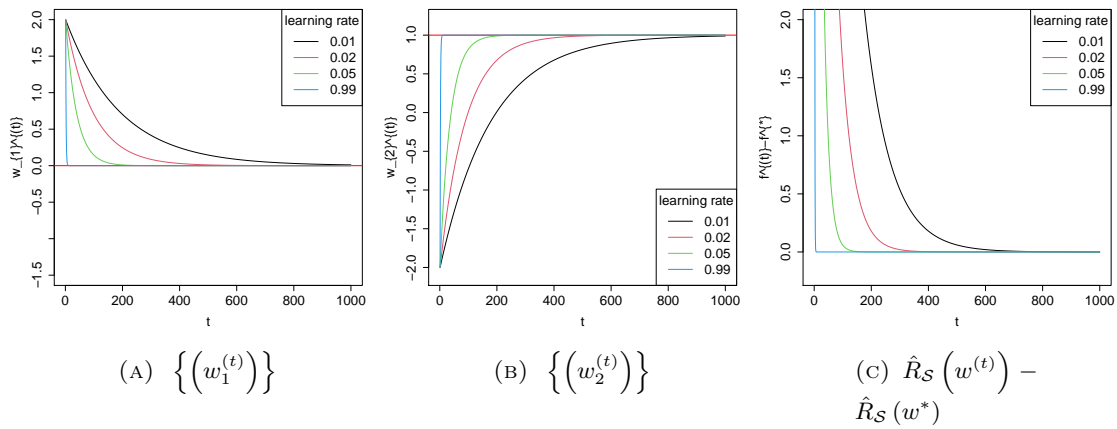
This is because  $\hat{R}_{\mathcal{D}}(w)$  is differentiable in  $\mathbb{R}^2$  so  $\partial \hat{R}_{\mathcal{D}}(w) = \{\nabla \hat{R}_{\mathcal{D}}(w)\}$  and because

$$\nabla \hat{R}_{\mathcal{D}}(w) = \begin{pmatrix} \frac{d}{dw_1} \hat{R}_{\mathcal{S}}(w) \\ \frac{d}{dw_2} \hat{R}_{\mathcal{S}}(w) \end{pmatrix} = \dots = \begin{pmatrix} 2w_1^{(t)} + 2w_2^{(t)}\bar{x} - 2\bar{y} \\ 2w_1^{(t)}\bar{x} + 2w_2^{(t)}\bar{x}^2 - 2y^\top x \end{pmatrix}$$

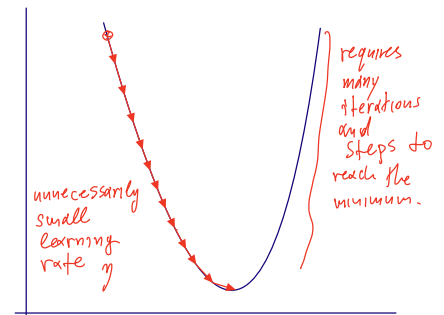
Consider data size  $n = 100$ , and parameters  $\rho = 0.2$ ,  $\sigma_y^2 = 1$  and  $\sigma_x^2 = 1$ . Then the real value (5.2) that I need to learn equals to  $w^* = (0, 1)^\top$ . Consider a GD seed  $w_0 = (2, -2)$ , and total number of iterations  $T = 1000$ .

Figures 5.1a, 5.1b, and 5.1c present trace plots of the chain  $\{(w^{(t)})\}$  and error  $\hat{R}_{\mathcal{S}}(w^{(t)}) - \hat{R}_{\mathcal{S}}(w^*)$  produced by running GD for  $T = 1000$  total iterations and for different (each time) constant learning rates  $\eta \in \{0.01, 0.02, 0.05, 0.99\}$ . We observe that the larger learning rates under consideration were able to converge faster to the minimum  $w^*$ . This is because they perform larger steps and can learn faster -this is not a panacea.

Figures 5.1d, 5.1e, and 5.1f present trace plots of the chain  $\{(w^{(t)})\}$ , and of the error  $\hat{R}_{\mathcal{S}}(w^{(t)}) - \hat{R}_{\mathcal{S}}(w^*)$  produced by running GD for  $T = 1000$  total iterations and for learning rate  $\eta = 1.0$  (previously considered) and a very big learning rate  $\eta = 3.0$ . We observe that the very big learning rate  $\eta = 3.0$  presents slower convergence to the minimum  $w^*$ . This is because it creates unreasonably big steps in (3.2) that the produced chain overshoots the global minimum; see the cartoon in Figures 5.1g and 5.1h.



(G) Unnecessarily large learning rate



(H) Unnecessarily small learning rate

FIGURE 5.1