

# Lectures Notes

## CS-E4740 Federated Learning

Dipl.-Ing. Dr.techn. Alexander Jung\*

February 6, 2024

### Abstract

This course discusses theory and algorithms for federated learning (FL). FL exploits similarities between local datasets to train local (or personalized) models collaboratively. Two core mathematical objects of this course are empirical graphs and generalized total variation minimization (GTVMin). We use empirical graphs to store and process local datasets and parameters of local models. GTVMin formulates FL as an instance of regularized empirical risk minimization. As the regularizer, we use quantitative measures for the variation of local models across the edges of the empirical graph. We can obtain practical FL systems by applying distributed optimization methods to solve GTVMin.

---

\*AJ is currently Associate Professor for Machine Learning at Aalto University (Finland). This work has been partially funded by the Academy of Finland (decision numbers 331197, 331197) and the European Union (grant number 952410).

# Contents

<b>1</b>	<b>Lecture - “Welcome and Intro”</b>	<b>1</b>
1.1	Learning Goals . . . . .	1
1.2	Introduction . . . . .	1
1.3	Prerequisites . . . . .	3
1.4	Related Courses . . . . .	4
1.5	Main Goal of the Course . . . . .	6
1.6	Outline of the Course . . . . .	7
1.7	Assignments and Grading . . . . .	9
1.8	Student Project . . . . .	9
1.9	Schedule . . . . .	9
1.10	Ground Rules . . . . .	10
<b>2</b>	<b>Lecture - “ML Basics”</b>	<b>1</b>
2.1	Learning Goals . . . . .	1
2.2	Three Components and a Design Principle . . . . .	1
2.3	Computational Aspects of ERM . . . . .	5
2.4	Statistical Aspects of ERM . . . . .	6
2.5	Validation and Diagnosis of ML . . . . .	8
2.6	Regularization . . . . .	13
2.7	Overview of Coding Assignment . . . . .	16
<b>3</b>	<b>Lecture - “FL Design Principle”</b>	<b>1</b>
3.1	Learning Goals . . . . .	1
3.2	Empirical Graphs and Their Laplacian . . . . .	1
3.3	Generalized Total Variation Minimization . . . . .	6

3.3.1	Computational Aspects of GTVMin . . . . .	9
3.3.2	Statistical Aspects of GTVMin . . . . .	11
3.4	Overview of Coding Assignment . . . . .	13
<b>4</b>	<b>Lecture - “Gradient Methods”</b>	<b>1</b>
4.1	Learning Goals . . . . .	1
4.2	Gradient Descent . . . . .	1
4.3	Learning Rate . . . . .	4
4.4	When to Stop? . . . . .	5
4.5	Perturbed Gradient Step . . . . .	9
4.6	Handling Constraints - Projected Gradient Descent . . . . .	10
4.7	Overview of Coding Assignment . . . . .	12
<b>5</b>	<b>Lecture - “FL Algorithms”</b>	<b>1</b>
5.1	Learning Goals . . . . .	1
5.2	Gradient Step for GTVMin . . . . .	1
5.3	Message Passing Implementation . . . . .	3
5.4	FedSGD . . . . .	4
5.5	FedAvg . . . . .	4
5.6	Overview of Coding Assignment . . . . .	4
<b>6</b>	<b>Lecture - “FL Main Flavours”</b>	<b>1</b>
6.1	Learning Goals . . . . .	1
6.2	Centralized FL . . . . .	1
6.3	Clustered FL . . . . .	1
6.4	Horizontal FL . . . . .	2
6.5	Vertical FL . . . . .	2

6.6	Assignment . . . . .	2
<b>7</b>	<b>Lecture - “Graph Learning”</b>	<b>1</b>
7.1	Learning Goals . . . . .	1
7.2	Measuring (Dis-)Similarity Between Datasets . . . . .	1
7.3	Graph Learning Methods . . . . .	2
7.4	Assignment . . . . .	3
<b>8</b>	<b>Lecture - “Trustworthy FL”</b>	<b>1</b>
8.1	Learning Goals . . . . .	1
<b>9</b>	<b>Lecture - “Privacy-Protection in FL”</b>	<b>1</b>
9.1	Learning Goals . . . . .	1
9.2	Assignment . . . . .	1
<b>10</b>	<b>Lecture - “Data and Model Poisoning in FL”</b>	<b>1</b>
10.1	Learning Goals . . . . .	1
10.2	Data Poisoning . . . . .	1
10.3	Model Poisoning . . . . .	1
10.4	Assignment . . . . .	1
	<b>Glossary</b>	<b>1</b>

# Lists of Symbols

## Sets and Functions

$a \in \mathcal{A}$	This statement indicates that the object $a$ is an element of the set $\mathcal{A}$ .
$a := b$	This statement defines $a$ to be shorthand for $b$ .
$ \mathcal{A} $	The cardinality (number of elements) of a finite set $\mathcal{A}$ .
$\mathcal{A} \subseteq \mathcal{B}$	$\mathcal{A}$ is a subset of $\mathcal{B}$ .
$\mathcal{A} \subset \mathcal{B}$	$\mathcal{A}$ is a strict subset of $\mathcal{B}$ .
$\mathbb{N}$	The set of natural numbers $1, 2, \dots$
$\mathbb{R}$	The set of real numbers $x$ [1].
$\mathbb{R}_+$	The set of non-negative real numbers $x \geq 0$ .
$\mathbb{R}_{++}$	The set of positive real numbers $x > 0$ .
$h(\cdot): \mathcal{A} \rightarrow \mathcal{B} : a \mapsto h(a)$	A function (map) that accepts any element $a \in \mathcal{A}$ from a set $\mathcal{A}$ as input and delivers a well-defined element $h(a) \in \mathcal{B}$ of a set $\mathcal{B}$ . The set $\mathcal{A}$ is the domain of the function $h$ and the set $\mathcal{B}$ is the codomain of $h$ . ML aims at finding (or learning) a function $h$ (“hypothesis”) that reads in the features $\mathbf{x}$ of a data point and delivers a prediction $h(\mathbf{x})$ for its label $y$ .

$\{0, 1\}$	The binary set that consists of the two real numbers 0 and 1.
$[0, 1]$	The closed interval of real numbers $x$ with $0 \leq x \leq 1$ .
$\operatorname{argmin} f(\mathbf{w})$	The set of minimizers for a real-valued function $f(\mathbf{w})$ .
$\log a$	The logarithm of the positive number $a \in \mathbb{R}_{++}$ .

## Matrices and Vectors

$\mathbf{I}_{l \times d}$	A generalized identity matrix with $l$ rows and $d$ columns. The entries of $\mathbf{I}_{l \times d} \in \mathbb{R}^{l \times d}$ are equal to 1 along the main diagonal and equal to 0 otherwise.
$\mathbf{I}$	A square identity matrix whose shape should be clear from the context.
$\mathbb{R}^d$	The set of vectors $\mathbf{x} = (x_1, \dots, x_d)^T$ consisting of $d$ real-valued entries $x_1, \dots, x_d \in \mathbb{R}$ .
$\mathbf{x} = (x_1, \dots, x_d)^T$	A vector of length $d$ . The $j$ th entry of the vector is denoted $x_j$ .
$\ \mathbf{x}\ _2$	The Euclidean (or “ $\ell_2$ ”) norm of the vector $\mathbf{x} = (x_1, \dots, x_d)^T \in \mathbb{R}^d$ given as $\ \mathbf{x}\ _2 := \sqrt{\sum_{j=1}^d x_j^2}$ .
$\ \mathbf{x}\ $	Some norm of the vector $\mathbf{x} \in \mathbb{R}^d$ [2]. Unless specified otherwise, we mean the Euclidean norm $\ \mathbf{x}\ _2$ .
$\mathbf{x}^T$	The transpose of a vector $\mathbf{x}$ that is considered a single column matrix. The transpose is a single-row matrix $(x_1, \dots, x_d)$ .
$\mathbf{X}^T$	The transpose of a matrix $\mathbf{X} \in \mathbb{R}^{m \times d}$ . A square real-valued matrix $\mathbf{X} \in \mathbb{R}^{m \times m}$ is called symmetric if $\mathbf{X} = \mathbf{X}^T$ .
$\mathbf{0} = (0, \dots, 0)^T$	The vector in $\mathbb{R}^d$ with each entry equal to zero.
$\mathbf{1} = (1, \dots, 1)^T$	The vector in $\mathbb{R}^d$ with each entry equal to one.

$(\mathbf{v}^T, \mathbf{w}^T)^T$	The vector of length $d + d'$ obtained by concatenating the entries of vector $\mathbf{v} \in \mathbb{R}^d$ with the entries of $\mathbf{w} \in \mathbb{R}^{d'}$ .
$\text{span}\{\mathbf{B}\}$	The span of a matrix $\mathbf{B} \in \mathbb{R}^{a \times b}$ , which is the subspace of all linear combinations of columns of $\mathbf{B}$ , $\text{span}\{\mathbf{B}\} = \{\mathbf{B}\mathbf{a} : \mathbf{a} \in \mathbb{R}^b\} \subseteq \mathbb{R}^a$ .
$\mathbb{S}_+^d$	The set of all positive semi-definite (psd) matrices of size $d \times d$ .
$\det(\mathbf{C})$	The determinant of the matrix $\mathbf{C}$ .
$\mathbf{A} \otimes \mathbf{B}$	The Kronecker product of $\mathbf{A}$ and $\mathbf{B}$ [3].



# Probability Theory

$\mathbb{E}_p\{f(\mathbf{z})\}$  The expectation of a function  $f(\mathbf{z})$  of a RV  $\mathbf{z}$  whose probability distribution is  $p(\mathbf{z})$ . If the probability distribution is clear from context we just write  $\mathbb{E}\{f(\mathbf{z})\}$ .

$p(\mathbf{x}, y)$  A (joint) probability distribution of a RV whose realizations are data points with features  $\mathbf{x}$  and label  $y$ .

$p(\mathbf{x}|y)$  A conditional probability distribution of a RV  $\mathbf{x}$  given the value of another RV  $y$  [4, Sec. 3.5].

$p(\mathbf{x}; \mathbf{w})$  A parametrized probability distribution of a RV  $\mathbf{x}$ . The probability distribution depends on a parameter vector  $\mathbf{w}$ . For example,  $p(\mathbf{x}; \mathbf{w})$  could be a multivariate normal distribution with the parameter vector  $\mathbf{w}$  given by the entries of the mean vector  $\mathbb{E}\{\mathbf{x}\}$  and the covariance matrix  $\mathbb{E}\left\{(\mathbf{x} - \mathbb{E}\{\mathbf{x}\})(\mathbf{x} - \mathbb{E}\{\mathbf{x}\})^T\right\}$ .

$\mathcal{N}(\mu, \sigma^2)$  The probability distribution of a scalar normal (“Gaussian”) RV  $x \in \mathbb{R}$  with mean (or expectation)  $\mu = \mathbb{E}\{x\}$  and variance  $\sigma^2 = \mathbb{E}\{(x - \mu)^2\}$ .

$\mathcal{N}(\boldsymbol{\mu}, \mathbf{C})$  The multivariate normal distribution of a vector-valued Gaussian RV  $\mathbf{x} \in \mathbb{R}^d$  with mean (or expectation)  $\boldsymbol{\mu} = \mathbb{E}\{\mathbf{x}\}$  and covariance matrix  $\mathbf{C} = \mathbb{E}\{(\mathbf{x} - \boldsymbol{\mu})(\mathbf{x} - \boldsymbol{\mu})^T\}$ .

# Machine Learning

$r$	An index $r = 1, 2, \dots$ , that enumerates data points.
$m$	The number of data points in (the size of) a dataset.
$\mathcal{D}$	A dataset $\mathcal{D} = \{\mathbf{z}^{(1)}, \dots, \mathbf{z}^{(m)}\}$ is a list of individual data points $\mathbf{z}^{(r)}$ , for $r = 1, \dots, m$ .
$d$	Number of features that characterize a data point.
$x_j$	The $j$ th feature of a data point. The first feature of a given data point is denoted $x_1$ , the second feature $x_2$ and so on.
$\mathbf{x}$	The feature vector $\mathbf{x} = (x_1, \dots, x_d)^T$ of a data point whose entries are the individual features of a data point.
$\mathcal{X}$	The feature space $\mathcal{X}$ is the set of all possible values that the features $\mathbf{x}$ of a data point can take on.
$\mathbf{z}$	Beside the symbol $\mathbf{x}$ , we sometimes use $\mathbf{z}$ as another symbol to denote a vector whose entries are features of a data point. We need two different symbols to distinguish between “raw” or “original” and learnt features [5, Ch. 9].
$\mathbf{x}^{(r)}$	The feature vector of the $r$ th data point within a dataset.
$x_j^{(r)}$	The $j$ th feature of the $r$ th data point within a dataset.
$\mathcal{B}$	A mini-batch (subset) of randomly chosen data points.
$B$	The size of (the number of data points in) a mini-batch.

$y$  The label (quantity of interest) of a data point.

$y^{(r)}$  The label of the  $r$ th data point.

$(\mathbf{x}^{(r)}, y^{(r)})$  The features and label of the  $r$ th data point.

The label space  $\mathcal{Y}$  of a ML method consists of all potential label values that a data point can have. We often use label spaces that are larger than the set of different label values arising in a give dataset (e.g., a training set). We refer to ML problems (methods) using a numeric label space, such as  $\mathcal{Y} = \mathbb{R}$  or  $\mathcal{Y} = \mathbb{R}^3$ , as regression problems (methods). ML problems (methods) that use a discrete label space, such as  $\mathcal{Y} = \{0, 1\}$  or  $\mathcal{Y} = \{\text{“cat”}, \text{“dog”}, \text{“mouse”}\}$  are referred to as classification problems (methods).

$\alpha$  learning rate (step-size) used by gradient-based methods.

$h(\cdot)$  A hypothesis map that reads in features  $\mathbf{x}$  of a data point and delivers a prediction  $\hat{y} = h(\mathbf{x})$  for its label  $y$ .

$\mathcal{Y}^{\mathcal{X}}$  Given two sets  $\mathcal{X}$  and  $\mathcal{Y}$ , we denote by  $\mathcal{Y}^{\mathcal{X}}$  the set of all possible hypothesis maps  $h : \mathcal{X} \rightarrow \mathcal{Y}$ .

$\mathcal{H}$  A hypothesis space or model used by a ML method. The hypothesis space consists of different hypothesis maps  $h : \mathcal{X} \rightarrow \mathcal{Y}$  between which the ML method has to choose .

$d_{\text{eff}}(\mathcal{H})$  The effective dimension of a hypothesis space  $\mathcal{H}$ .

$B^2$	<p>The squared bias of a learnt hypothesis <math>\hat{h}</math> delivered by a ML algorithm that is fed with data points which are modelled as realizations of RVs. If data is modelled as realizations of RVs, also the delivered hypothesis <math>\hat{h}</math> is the realization of a RV.</p>
$V$	<p>The variance of the (parameters of the) hypothesis delivered by a ML algorithm. If the input data for this algorithm is interpreted as realizations of RVs, so is the delivered hypothesis a realization of a RV.</p>
$L((\mathbf{x}, y), h)$	<p>The loss incurred by predicting the label <math>y</math> of a data point using the prediction <math>\hat{y} = h(\mathbf{x})</math>. The prediction <math>\hat{y}</math> is obtained from evaluating the hypothesis <math>h \in \mathcal{H}</math> for the feature vector <math>\mathbf{x}</math> of the data point.</p>
$E_v$	<p>The validation error of a hypothesis <math>h</math>, which is its average loss incurred over a validation set.</p>
$\hat{L}(h \mathcal{D})$	<p>The empirical risk or average loss incurred by the predictions of hypothesis <math>h</math> for the data points in the dataset <math>\mathcal{D}</math>.</p>
$E_t$	<p>The training error of a hypothesis <math>h</math>, which is its average loss incurred over a training set.</p>
$t$	<p>A discrete-time index <math>t = 0, 1, \dots</math> used to enumerate a sequence to sequential events (“time instants”).</p>
$t$	<p>An index that enumerates learning tasks within a multi-task learning problem.</p>

$\lambda$	A regularization parameter that controls the amount of regularization.
$\lambda_j(\mathbf{Q})$	The $j$ th eigenvalue (sorted either ascending or descending) of a psd matrix $\mathbf{Q}$ . We also use the shorthand $\lambda_j$ if the corresponding matrix is clear from context.
$\sigma(\cdot)$	The activation function used by an artificial neuron within an artificial neural network (ANN).
$\mathcal{R}_{\hat{y}}$	A decision region within a feature space.
$\mathbf{w}$	A parameter vector $\mathbf{w} = (w_1, \dots, w_d)^T$ whose entries are parameters of a model. These parameters could be feature weights in linear maps, the weights in ANNs or the thresholds used for splits in decision trees.
$h^{(\mathbf{w})}(\cdot)$	A hypothesis map that involves tunable model parameters $w_1, \dots, w_d$ , stacked into the vector $\mathbf{w} = (w_1, \dots, w_d)^T$ .
$\nabla f(\mathbf{w})$	The gradient of a differentiable real-valued function $f : \mathbb{R}^d \rightarrow \mathbb{R}$ is the vector $\nabla f(\mathbf{w}) = (\frac{\partial f}{\partial w_1}, \dots, \frac{\partial f}{\partial w_d})^T \in \mathbb{R}^d$ [6, Ch. 9].
$\phi(\cdot)$	A feature map $\phi : \mathcal{X} \rightarrow \mathcal{X}' : \mathbf{x} \mapsto \mathbf{x}' := \phi(\mathbf{x}) \in \mathcal{X}'$ .

## Federated Learning

$\mathcal{G} = (\mathcal{V}, \mathcal{E})$	Empirical graph whose nodes $i \in \mathcal{V}$ carry local datasets and local models.
$i \in \mathcal{V}$	A node in the empirical graph that represents a local dataset and a corresponding local model. It might also be useful to think of node $i$ as a small computer that can collect data and execute computations to train ML models.
$\mathcal{D}^{(i)}$	The local dataset $\mathcal{D}^{(i)}$ at node $i \in \mathcal{V}$ of an empirical graph.
$m_i$	The number of data points (sample size) contained in the local dataset $\mathcal{D}^{(i)}$ at node $i \in \mathcal{V}$ .
$\mathcal{N}^{(i)}$	The neighbourhood of the node $i$ in an empirical graph.
$\mathbf{x}^{(i,r)}$	The features of the $r$ -th data point in the local dataset $\mathcal{D}^{(i)}$ .
$y^{(i,r)}$	The label of the $r$ -th data point in the local dataset $\mathcal{D}^{(i)}$ .
$L^{(d)}(\mathbf{x}, h(\mathbf{x}), h'(\mathbf{x}))$	The loss incurred by a “external” hypothesis $h'$ on a data point with features $\mathbf{x}$ and predicted label $h(\mathbf{x})$ that is obtained from some local hypothesis.
$\text{stack}\{\mathbf{w}^{(i)}\}_{i=1}^n$	The vector $\left( (\mathbf{w}^{(1)})^T, \dots, (\mathbf{w}^{(n)})^T \right)^T \in \mathbb{R}^{dn}$ that is obtained by vertically stacking the local model parameters $\mathbf{w}^{(i)} \in \mathbb{R}^d$ .

# 1 Lecture - “Welcome and Intro”

February 6, 2024

Welcome to the course CS-E4740 Federated Learning. This course can be completed fully remote. Any on-site event will be recorded and made available to students via this YouTube channel. The basic variant (5 credits) of this course consists of lectures (schedule here) and corresponding coding assignments (schedule here). We test your completion of the coding assignments via quizzes (implemented on the MyCourses page). You can upgrade the course to an extended variant (10 credits) by completing a student project (see Section 1.8).

## 1.1 Learning Goals

This lecture offers

- introduction of course topic and positioning in wider curricula
- discussion of learning goals, assignments and student project
- overview of course schedule

## 1.2 Introduction

We are surrounded by devices (e.g. smartphones, wearables, sensors) that generate decentralized collections of local datasets [7–11]. An application-specific network structure relates these local datasets. For example, the high-precision management of pandemics uses contact networks to relate local datasets generated by patients. Network medicine relates data about diseases

via co-morbidity networks [12]. Social science uses notions of acquaintance to relate data collected from be-friended individuals [13].

Federated learning (FL) is an umbrella term for distributed optimization techniques to train machine learning (ML) models from decentralized collections of local datasets [14–18]. These methods carry out computations, such as gradient steps (see Lecture 4), for ML model training at the location of data generation. This design philosophy is different from a naive application of ML techniques, which is first to collect all local datasets at a single location (computer). We can then feed this pooled data into a conventional ML method like linear regression.

The distributed training of ML models, at locations close to the actual data generation, can be beneficial for several reasons [19]:

- **Privacy.** FL methods are appealing for applications involving sensitive data (such as healthcare) as they do not require the exchange of raw data but only model (parameter) updates [16, 17]. By exchanging only model updates, FL methods are considered privacy-friendly in the sense of not leaking (too much) sensitive information that is contained in the local datasets (see Lecture 9).
- **Robustness.** By relying on decentralized data and computation, FL methods offer robustness (to some extent) against hardware failures (such as “stragglers”) and data poisonings (see Lecture 10).
- **Parallel Computing.** Many ML systems are based on mobile networks, consisting of humans equipped with smartphones. We can interpret a mobile network as a parallel computer which is constituted by smart-



phones that can communicate via radio links. This parallel computer allows to speed up computational tasks such as the computation of gradients required to train ML models (see Lecture 4).

- **Trading Computation against Communication.** Consider a FL application where local datasets are generated by low-complexity devices at remote locations that cannot be easily accessed. The cost of communicating raw local datasets to some central unit (which then trains a single global ML model) might be much higher than the computational cost incurred by using the low-complexity devices to (partially) train ML models [20].
- **Personalization.** FL can be used to train personalized ML models for collections of local datasets, which might be generated by smartphones (and their users) [21]. A key challenge for ensuring personalization is the heterogeneity of local datasets [22, 23]. Indeed, the statistical properties of different local datasets might vary significantly such they cannot be well modelled as independent and identically distributed (i.i.d.). Each local dataset induces a separate learning task that consists of learning useful parameter values for a local model. This course discusses FL methods to train personalized models via combining the information carried in decentralized and heterogeneous data (see Lecture 6).

### 1.3 Prerequisites

The main mathematical structure used to study and design FL algorithms is the Euclidean space  $\mathbb{R}^d$ . We therefore expect some familiarity with the

algebraic and geometric structure of  $\mathbb{R}^d$ . By algebraic structure, we mean the (real) vector space obtained from the elements (“vectors”) in  $\mathbb{R}^d$  along with the usual definitions of vector addition and multiplication by scalars in  $\mathbb{R}$  [24, 25]. We will make heavy use of concepts from linear algebra to represent and manipulate data and ML models.

The metric structure of  $\mathbb{R}^d$  will be used to study the (convergence) behaviour of FL algorithms. In particular, we will study FL algorithms that are obtained as fixed-point iterations of some non-linear operator on  $\mathbb{R}^d$  which depends on the data (distribution) and ML models used within a FL system. A prime example for such a non-linear operator is the gradient step of gradient-based methods (see Lecture 4). The computational properties (such as convergence speed) of these FL algorithms can then be characterized via the contraction properties of the underlying operator [26].

A main tool for the design the FL algorithms are variants of gradient descent (GD). These gradient-based methods are based on approximating a differentiable function  $f(\mathbf{x})$  locally by a linear function given by the gradient  $\nabla f(\mathbf{x})$ . We therefore expect some familiarity with multivariable calculus [6].

## 1.4 Related Courses

In what follows we briefly explain how this course CS-E4740 relates to selected courses at Aalto University.

- **CS-EJ3211 - Machine Learning with Python.** Teaches the application of basic ML methods using the Python package (library) `scikit-learn` [27]. CS-E4740 couples a network of basic ML methods using regularization techniques to obtain tailored (personalized) ML

models for local datasets. This coupling is required to adaptive pool local datasets obtain a sufficiently large training set for the personalized ML model.

- **CS-E4510 - Distributed Algorithms.** Teaches basic mathematical tools for the study and design of distributed algorithms that are implemented via distributed systems (computers) [28]. FL is enabled by distributed algorithms to train ML models from decentralized data (see Lecture 5).
- **CS-C3240 - Machine Learning (spring 2022 edition).** Teaches basic theory of ML models and methods [5]. CS-E4740 combines the components of basic ML methods, such as data representation and models, with network models. In particular, instead of a single dataset and a single model (such as a decision tree), we will study networks of local datasets and local models.
- **ABL-E2606 - Data Protection.** This course discusses important legal constraints (“laws”), including the European general data protection regulation (GDPR), for the use of data and, in turn, for the design of trustworthy FL methods.
- **MS-C2105 - Introduction to Optimization.** This course teaches basic optimisation theory and how to model applications as (linear, integer, and non-linear) optimization problems. CS-E4740 uses optimization theory and methods to formulate FL problems (see Lecture 3) and design FL methods (see Lecture 5).

- **ELEC-E5424 - Convex Optimization.** This course teaches advanced optimisation theory for the important class of convex optimization problems [29]. Convex optimization theory and methods can be used for the study and design of FL algorithms.

## 1.5 Main Goal of the Course

The overarching goal of the course is to demonstrate how to apply concepts from graph theory and mathematical optimization to analyze and design FL algorithms. Students will learn to formulate a given FL application as an optimization problem over an undirected empirical graph  $\mathcal{G} = (\mathcal{V}, \mathcal{E})$  whose nodes  $i \in \mathcal{V}$  represent individual local datasets. We refer to this graph as the empirical graph of a collection of local datasets (see Lecture 3).

This course uses only undirected empirical graphs with a finite number  $n$  of nodes, which we identify with the first  $n$  positive integers:

$$\mathcal{V} := \{1, \dots, n\}.$$

An edge  $\{i, i'\} \in \mathcal{E}$  in the empirical graph  $\mathcal{G}$  connects two different local datasets if they have similar statistical properties. We quantify the amount of similarity by the positive edge weight  $A_{i,i'} > 0$ .

We can formalize a FL application as an optimization problem associated with an empirical graph,

$$\min_{\mathbf{w}^{(i)}} \sum_{i \in \mathcal{V}} L_i(\mathbf{w}^{(i)}) + \lambda \sum_{\{i,i'\} \in \mathcal{E}} A_{i,i'} d(\mathbf{w}^{(i)}, \mathbf{w}^{(i')}). \quad (1.1)$$

We refer to this problem as GTV minimization (GTVMIn) and devote much of the course to its computational and statistical properties. The optimization

variables  $\mathbf{w}^{(i)}$  in (1.1) are local model parameters at the nodes  $i \in \mathcal{V}$  of an empirical graph. The objective function in (1.1) consists of two components: The first component is a sum over all nodes of the loss values  $L_i(\mathbf{w}^{(i)})$  incurred by local model parameters at each node  $i$ . The second component is the sum of local model parameters discrepancies  $d(\mathbf{w}^{(i)}, \mathbf{w}^{(i')})$  across the edges  $\{i, i'\}$  of the empirical graph.

## 1.6 Outline of the Course

Our course is roughly divided into three parts:

- **Part I: ML Refresher.** Lecture 2 introduces data, models and loss functions as three main components of ML. This lecture also explains how these components are combined within empirical risk minimization (ERM). We also discuss how regularization of ERM can be achieved via manipulating its three main components. We then explain when and how to solve regularized ERM via simple GD methods in Lecture 4. Overall, this part serves two main purposes: (i) to briefly recap basic concepts of ML in a simple centralized setting and (ii) highlight ML techniques (such as regularization) that are particularly relevant for the design and analysis of FL methods.
- **Part II: FL Theory and Methods.** Lecture 3 introduces the empirical graph as our main mathematical structure for representing collections of local datasets and corresponding tailored models. The undirected and weighted edges of the empirical graph represent statistical similarities between local datasets. Lecture 3 also formulates FL as an instance of

regularized empirical risk minimization (RERM) which we refer to as GTVMin. GTVMin uses the variation of personalized model parameters across edges in the empirical graph as regularizer. We will see that GTVMin couples the training of tailored (or “personalized”) ML models such that well-connected nodes (clusters) in the empirical graph will obtain similar trained models. Lecture 4 discusses variations of gradient descent as our main algorithmic toolbox for solving GTVMin. Lecture 5 shows how FL algorithms can be obtained in a principled fashion by applying optimization methods, such as gradient-based methods, to GTVMin. We will obtain FL algorithms that can be implemented as iterative message passing methods for the distributed training of tailored (“personalized”) models. Lecture 6 derives some main flavours of FL as special cases of GTVMin. The usefulness of GTVMin crucially depends on the choice for the weighted edges in the empirical graph. Lecture 7 discusses graph learning methods that determine a useful empirical graph via different notions of statistical similarity between local datasets.

- **Part III: Trustworthy AI.** Lecture 8 enumerates seven key requirements for trustworthy artificial intelligence (AI) that have been put forward by the European Union. These key requirements include the protection of privacy as well as robustness against (intentional) perturbations of data or computation. We then discuss how FL algorithms can ensure privacy protection in Lecture 9. Lecture 10 discusses how to evaluate and ensure robustness of FL methods against intentional perturbations (poisoning) of local dataset.

## 1.7 Assignments and Grading

The course includes coding assignments that require you to implement concepts from the lecture in a Python notebook. We will use MyCourses quizzes to test your understanding of lecture contents and solutions to the coding assignments. For each quiz, you can earn around 10 points. We will then sum up the points from all quizzes and determine your grade according to: grade 1: 50-59 points; grade 2: 60-69; grade 3: 70-79; grade 4: 80-89; 5: grade 5: at least 90 points.

## 1.8 Student Project

You can extend the basic variant (which is worth 5 credits) to 10 credits by completing a student project and peer review. This project requires you to formulate an application of your choice as a FL problem using the concepts from this course. You then have to solve this FL problem using the FL algorithms taught in this course. The main deliverable will be a project report which must follow the structure indicated in the template. You will then peer-review the reports of your fellow students by answering a detailed questionnaire.

## 1.9 Schedule

The course lectures are held on Mo. and Wed. at 16.15, during 28-Feb-2024 until 30-Apr-2024. You can find the detailed schedule and lecture halls following this link. As the course can be completed fully remote, we will record each lecture and add the recording to the YouTube playlist here in a timely fashion.

After each lecture, we will release the corresponding assignment at this site. You will have then at least one week to work on the assignment before we open the corresponding quiz on the MyCourses page of the course (click me).

## 1.10 Ground Rules

Note that as a student following this course, you must act according to the Code of Conduct of Aalto University. In particular, the main ground rules for this course are:

- **BE HONEST.** This course includes many tasks that require independent work, including the coding assignments, the working on student projects and the peer review of student projects. You must not use other's work inappropriately. For example, it is not allowed to copy other's solutions to coding assignments. We will randomly choose students who have to explain their solutions (and corresponding answers to quiz questions).
- **BE RESPECTFUL.** My personal wish is that this course provides a safe space for an enjoyable learning experience. Any form of disrespectful behaviour, including any course-related communication platforms, will be sanctioned rigorously (including reporting to university authorities).



## 2 Lecture - “ML Basics”

February 6, 2024

This lecture covers basic ML techniques that are instrumental for FL. This lecture is significantly more extensive content-wise compared to the following lectures. However, this lecture should be significantly easier to follow than the following lectures as it mainly refreshes pre-requisite knowledge.

### 2.1 Learning Goals

After this lecture, you should

- be familiar with the concept of data points (their features and labels), model and loss function,
- be familiar with ERM as a design principle for ML systems,
- know why and how validation is performed,
- be able to diagnose ML methods by comparing training error with validation error,
- be able to regularize ERM via modifying data, model and loss.

### 2.2 Three Components and a Design Principle

Machine Learning (ML) revolves around learning a hypothesis map  $h$  out of a hypothesis space  $\mathcal{H}$  that allows to accurately predict the label of a data point solely from its features. One of the most crucial steps in applying ML methods to a given application domain is the definition or choice of what precisely a data point is. Coming up with a good choice or definition of data

points is not trivial as it influences the overall performance of a ML method in many different ways.

During this course we will focus mainly on one specific choice for the data points. In particular, we will consider data points that represent the daily weather condition around a weather station of the Finnish Meteorological Institute (FMI). We denote a specific data point by  $\mathbf{z}$ . It is characterized by the following features:

- name of the FMI weather station, e.g., “TurkuRajakari”
- latitude `lat` and longitude `lon` of the weather station, e.g., `lat := 60.37788`, `lon := 22.0964`,
- date of the day in format DDMMYYYY, e.g., 01022022
- minimum daytime temperature.

It is convenient to stack the features into a feature vector  $\mathbf{x}$ . The label  $y \in \mathbb{R}$  of such a data point is the maximum daytime temperature.

We predict the label by the function value hypothesis  $h(\mathbf{x})$ . The prediction will typically be not perfect, i.e.,  $h(\mathbf{x}) \neq y$ . We measure the prediction error by a loss function such as the squared error loss  $L(\mathbf{z}, h) := (y - h(\mathbf{x}))^2$ . It seems natural to choose (or learn) a hypothesis that incurs minimum average loss (or empirical risk) on a given set of data points  $\mathcal{D} := \{(\mathbf{x}^{(1)}, y^{(1)}), \dots, (\mathbf{x}^{(m)}, y^{(m)})\}$ . This is known as ERM,

$$\hat{h} \in \operatorname{argmin}_{h \in \mathcal{H}} (1/m) \sum_{r=1}^m (y^{(r)} - h(\mathbf{x}^{(r)}))^2 \quad (2.1)$$

As our notation indicates (using the symbol “ $\in$ ” instead of “ $:=$ ”), there might be several different solutions to the optimization problem (2.1). Unless

specified otherwise,  $\hat{h}$  can be used to denote any hypothesis in  $\mathcal{H}$  that has minimum average loss over  $\mathcal{D}$ .

Several important machine learning (ML) methods use a parameterized model  $\mathcal{H}$ : Each hypothesis  $h \in \mathcal{H}$  is defined by parameters  $\mathbf{w} \in \mathbb{R}^d$ , often indicated by the notation  $h^{(\mathbf{w})}$ . A prominent instance of such a parameterized model is the linear model [5, Sec. 3.1],

$$\mathcal{H}^{(d)} := h(\mathbf{x}) := \mathbf{w}^T \mathbf{x}. \quad (2.2)$$

Linear regression, for example, determines the parameters of a linear model by minimizing the average squared error loss. For linear regression, ERM becomes an optimization over the parameter space  $\mathbb{R}^d$ ,

$$\hat{\mathbf{w}}^{(\text{LR})} \in \underset{\mathbf{w} \in \mathbb{R}^d}{\operatorname{argmin}} \underbrace{(1/m) \sum_{r=1}^m (y^{(r)} - \mathbf{w}^T \mathbf{x}^{(r)})^2}_{:=f(\mathbf{w})}. \quad (2.3)$$

Note that (2.3) amounts to finding the minimum of a smooth and convex function

$$f(\mathbf{w}) = (1/m) \left[ \mathbf{w}^T \mathbf{X}^T \mathbf{X} \mathbf{w} - 2 \mathbf{y}^T \mathbf{X} \mathbf{w} + \mathbf{y}^T \mathbf{y} \right] \quad (2.4)$$

$$\text{with the feature matrix } \mathbf{X} := (\mathbf{x}^{(1)}, \dots, \mathbf{x}^{(m)})^T \quad (2.5)$$

$$\text{and the label vector } \mathbf{y} := (y^{(1)}, \dots, y^{(m)})^T \text{ of the training set } \mathcal{D}. \quad (2.6)$$

Inserting (2.4) into (2.3) allows to formulate linear regression as

$$\hat{\mathbf{w}}^{(\text{LR})} \in \underset{\mathbf{w} \in \mathbb{R}^d}{\operatorname{argmin}} \mathbf{w}^T \mathbf{Q} \mathbf{w} + \mathbf{w}^T \mathbf{q} \quad (2.7)$$

$$\text{with } \mathbf{Q} := (1/m) \mathbf{X}^T \mathbf{X}, \mathbf{q} := -(2/m) \mathbf{X}^T \mathbf{y}.$$



Figure 2.1: ERM (2.1) for linear regression minimizes a convex quadratic function  $\mathbf{w}^T \mathbf{Q} \mathbf{w} + \mathbf{w}^T \mathbf{q}$ .

The matrix  $\mathbf{Q} \in \mathbb{R}^{d \times d}$  is psd with corresponding eigenvalue decomposition (EVD),

$$\mathbf{Q} = \sum_{j=1}^d \lambda_j(\mathbf{Q}) \mathbf{u}^{(j)} (\mathbf{u}^{(j)})^T. \quad (2.8)$$

The EVD (2.8) involves non-negative eigenvalues

$$0 \leq \lambda_1(\mathbf{Q}) \leq \dots \leq \lambda_d(\mathbf{Q}). \quad (2.9)$$

To train a ML model  $\mathcal{H}$  means to solve ERM (2.1) (or (2.3) for linear regression); the dataset  $\mathcal{D}$  is therefore referred to as a training set. The trained model results in the learnt hypothesis  $\hat{h}$ . We obtain practical ML methods by applying optimization algorithms to solve (2.1). Two key questions studied in ML are:

- **computational aspects** How much computation do we need to solve (2.1) ?
- **statistical aspects** How useful is the solution  $\hat{h}$  to (2.1) in general,

i.e., how accurate is the prediction  $\hat{h}(\mathbf{x})$  for the label  $y$  of an **arbitrary** data point with features  $\mathbf{x}$ ?

## 2.3 Computational Aspects of ERM

ML methods use optimization algorithms to solve (2.1) in order to learn a hypothesis  $\hat{h}$ . Within this course, we use optimization algorithms that are iterative methods: Starting from an initial choice  $h^{(0)}$ , they construct a sequence

$$h^{(0)}, h^{(1)}, h^{(2)}, \dots,$$

which are hopefully increasingly accurate approximations to a solution  $\hat{h}$  of (2.1). The computational complexity of such a ML method can be measured by the number of iterations required to guarantee some prescribed level of approximation.

For a parameterized model and a smooth loss function, we can solve (2.3) by gradient-based methods: Starting from an initial parameters  $\mathbf{w}^{(0)}$ , we iterate the gradient step:

$$\begin{aligned} \mathbf{w}^{(k)} &:= \mathbf{w}^{(k-1)} - \alpha \nabla f(\mathbf{w}^{(k-1)}) \\ &= \mathbf{w}^{(k-1)} + (2\alpha/m) \sum_{r=1}^m \mathbf{x}^{(r)} (y^{(r)} - (\mathbf{w}^{(k-1)})^T \mathbf{x}^{(r)}). \end{aligned} \quad (2.10)$$

How much computation do we need for one iteration of (2.10)? How many iterations do we need? We will try to answer the latter question in Lecture 4. The first question can be answered more easily for typical computational infrastructure (e.g., “Python running on a commercial Laptop”). Indeed, a naive evaluation of (2.10) requires around  $m$  arithmetic operations (addition, multiplication).

It is instructive to consider the special case of a linear model which does not use any feature, i.e.,  $h(\mathbf{x}) = w$ . For this extreme case, the ERM (2.3) has a simple closed-form solution:

$$\hat{w} = (1/m) \sum_{r=1}^m x^{(r)}. \quad (2.11)$$

Thus, for this special case of the linear model, solving (2.11) amounts to summing  $m$  numbers  $x^{(1)}, \dots, x^{(m)}$ . It seems reasonable to assume that the amount of computation required to compute (2.11) is proportional to  $m$ .

## 2.4 Statistical Aspects of ERM

We can train a linear model on a given training set as ERM (2.3). But how useful is the solution  $\hat{\mathbf{w}}$  of (2.3) for predicting the labels of data points outside the training set? Consider applying the learnt hypothesis  $h^{(\hat{\mathbf{w}})}$  to an arbitrary data point not contained in the training set. What can we say about the resulting prediction error  $y - h^{(\hat{\mathbf{w}})}(\mathbf{x})$  in general? In other words, how well does  $h^{(\hat{\mathbf{w}})}$  generalize beyond the training set.

Maybe the most widely used approach to study generalization of ML methods is via probabilistic models. Here, we interpret each data point as a realization of an i.i.d. RV with probability distribution  $p(\mathbf{x}, y)$ . Under this i.i.d. assumption, we can evaluate the overall performance of a hypothesis  $h \in \mathcal{H}$  via the expected loss (or risk)

$$\mathbb{E}\{L((\mathbf{x}, y), h)\}. \quad (2.12)$$

One example for a probability distribution  $p(\mathbf{x}, y)$  is obtained via relating

the label  $y$  with the features  $\mathbf{x}$  of a data point as

$$y = \bar{\mathbf{w}}^T \mathbf{x} + \varepsilon \text{ with } \mathbf{x} \sim \mathcal{N}(\mathbf{0}, \mathbf{I}), \varepsilon \sim \mathcal{N}(0, \sigma^2). \quad (2.13)$$

A simple calculation reveals the expected squared error loss of a given linear hypothesis  $h(\mathbf{x}) = \mathbf{x}^T \hat{\mathbf{w}}$  as

$$\mathbb{E}\{(y - h(\mathbf{x}))^2\} = \|\bar{\mathbf{w}} - \hat{\mathbf{w}}\|^2 + \sigma^2. \quad (2.14)$$

The component  $\sigma^2$  can be interpreted as intrinsic noise level of the label  $y$ . We cannot hope to find a hypothesis with expected loss smaller than this level. The first component of the RHS in (2.14) is the estimation error  $\|\bar{\mathbf{w}} - \hat{\mathbf{w}}\|^2$  of a ML method that reads in the training set and delivers an estimate  $\hat{\mathbf{w}}$  (e.g., via (2.3)) for the parameters of a linear hypothesis.

We next study the estimation error  $\bar{\mathbf{w}} - \hat{\mathbf{w}}$  incurred by the specific estimate  $\hat{\mathbf{w}} = \hat{\mathbf{w}}^{(\text{LR})}$  (2.7) delivered by linear regression methods. To this end, we first use the probabilistic model (2.13) to decompose the label vector  $\mathbf{y}$  in (2.6) as

$$\mathbf{y} = \mathbf{X}\bar{\mathbf{w}} + \mathbf{n}, \text{ with } \mathbf{n} := (\varepsilon^{(1)}, \dots, \varepsilon^{(m)})^T. \quad (2.15)$$

Inserting (2.15) into (2.7) yields

$$\hat{\mathbf{w}}^{(\text{LR})} \in \underset{\mathbf{w} \in \mathbb{R}^d}{\operatorname{argmin}} \mathbf{w}^T \mathbf{Q} \mathbf{w} + \mathbf{w}^T \mathbf{q}' + \mathbf{w}^T \mathbf{e} \quad (2.16)$$

$$\text{with } \mathbf{Q} := (1/m) \mathbf{X}^T \mathbf{X}, \mathbf{q}' := -(2/m) \mathbf{X}^T \mathbf{X} \bar{\mathbf{w}}, \text{ and } \mathbf{e} := -(2/m) \mathbf{X}^T \mathbf{n}. \quad (2.17)$$

Figure 2.2 depicts the objective function of (2.16). It is a perturbation of the convex quadratic function  $\mathbf{w}^T \mathbf{Q} \mathbf{w} + \mathbf{w}^T \mathbf{q}'$ , which is minimized at  $\mathbf{w} = \bar{\mathbf{w}}$ . In general, the minimizer  $\hat{\mathbf{w}}^{(\text{LR})}$  delivered by linear regression is different from  $\bar{\mathbf{w}}$  due the perturbation term  $\mathbf{w}^T \mathbf{e}$  in (2.16). The following result bounds

the deviation between  $\widehat{\mathbf{w}}^{(\text{LR})}$  and  $\overline{\mathbf{w}}$  under the assumption that the matrix  $\mathbf{Q} = (1/m)\mathbf{X}^T\mathbf{X}$  is invertible.<sup>1</sup>

**Proposition 2.1.** *Consider a solution  $\widehat{\mathbf{w}}^{(\text{LR})}$  to the ERM instance (2.16) that is applied to the dataset (2.15). We can then upper bound the squared Euclidean norm of the difference  $\widehat{\mathbf{w}}^{(\text{LR})} - \overline{\mathbf{w}}$  as*

$$\|\widehat{\mathbf{w}}^{(\text{LR})} - \overline{\mathbf{w}}\|_2^2 \leq \|\mathbf{e}\|_2^2 / \lambda_1^2 \stackrel{(2.17)}{=} (4/m^2) \|\mathbf{X}^T \mathbf{n}\|_2^2 / \lambda_1^2. \quad (2.18)$$

*Proof.* Let us rewrite (2.16) as

$$\widehat{\mathbf{w}}^{(\text{LR})} \in \underset{\mathbf{w} \in \mathbb{R}^d}{\operatorname{argmin}} f(\mathbf{w}) \text{ with } f(\mathbf{w}) := (\mathbf{w} - \overline{\mathbf{w}})^T \mathbf{Q}(\mathbf{w} - \overline{\mathbf{w}}) + \mathbf{e}^T(\mathbf{w} - \overline{\mathbf{w}}). \quad (2.19)$$

Clearly  $f(\overline{\mathbf{w}}) = 0$  and, in turn,  $f(\widehat{\mathbf{w}}) = \min_{\mathbf{w} \in \mathbb{R}^d} f(\mathbf{w}) \leq 0$ . On the other hand,

$$\begin{aligned} f(\mathbf{w}) &\stackrel{(2.19)}{=} (\mathbf{w} - \overline{\mathbf{w}})^T \mathbf{Q}(\mathbf{w} - \overline{\mathbf{w}}) + \mathbf{e}^T(\mathbf{w} - \overline{\mathbf{w}}) \\ &\stackrel{(a)}{\geq} (\mathbf{w} - \overline{\mathbf{w}})^T \mathbf{Q}(\mathbf{w} - \overline{\mathbf{w}}) - \|\mathbf{e}\|_2 \|\mathbf{w} - \overline{\mathbf{w}}\|_2 \\ &\stackrel{(b)}{\geq} \lambda_1 \|\mathbf{w} - \overline{\mathbf{w}}\|_2^2 - \|\mathbf{e}\|_2 \|\mathbf{w} - \overline{\mathbf{w}}\|_2. \end{aligned} \quad (2.20)$$

Step (a) used Cauchy–Schwarz inequality and (b) used the EVD (2.8) of  $\mathbf{Q}$ . Evaluating (2.20) for  $\mathbf{w} = \widehat{\mathbf{w}}$  and combining with  $f(\widehat{\mathbf{w}}) \leq 0$  yields (2.18).  $\square$

## 2.5 Validation and Diagnosis of ML

The above analysis of the generalization error started from postulating a probabilistic model for the generation of data points. However, this probabilistic

---

<sup>1</sup>Can you think of sufficient conditions on the feature matrix of the training set that ensure  $\mathbf{Q} = (1/m)\mathbf{X}^T\mathbf{X}$  is invertible?



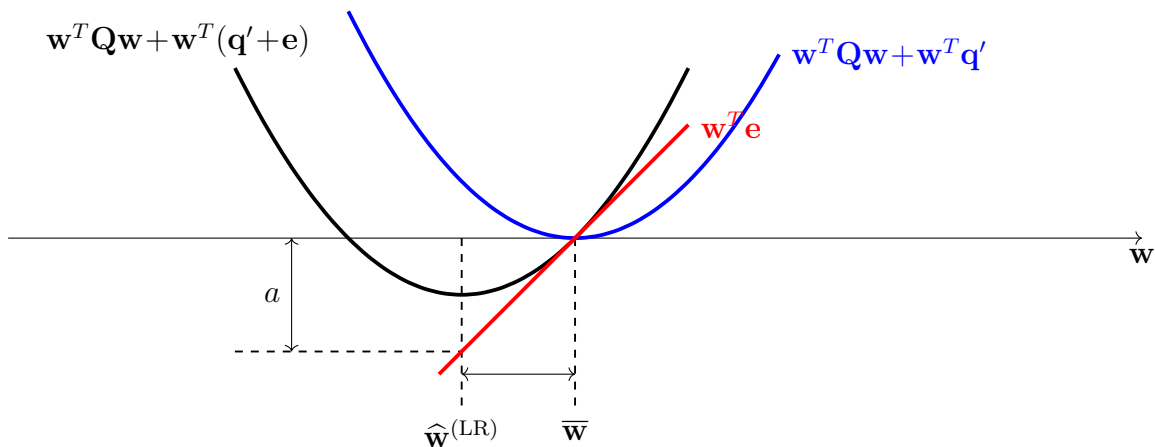


Figure 2.2: The estimation error of linear regression is determined by the effect of the perturbation term  $w^T e$  on the minimizer of the convex quadratic function  $w^T Q w + w^T q'$ .

model might be wrong and the bound (2.18) does not apply. Thus, we might want to use a more data-driven approach for assessing the usefulness of a learnt hypothesis.

Validation methods try to find out if a learnt hypothesis  $\hat{h}$ , does well outside the training set. In its most basic form, model validation amounts to computing the average loss of a learnt hypothesis  $\hat{h}$  on some data points not included in the training set. We refer to these data points as the validation set.

The most basic workflow of ML model training and validation can be summarized as follows:

1. gather a dataset and choose a model  $\mathcal{H}$
2. split dataset into a training set  $\mathcal{D}^{(\text{train})}$  and a validation set  $\mathcal{D}^{(\text{val})}$

3. learn a hypothesis via solving ERM

$$\hat{h} \in \operatorname{argmin}_{h \in \mathcal{H}} \sum_{(\mathbf{x}, y) \in \mathcal{D}^{(\text{train})}} L((\mathbf{x}, y), h) \quad (2.21)$$

4. compute resulting training error

$$E_t := (1/|\mathcal{D}^{(\text{train})}|) \sum_{(\mathbf{x}, y) \in \mathcal{D}^{(\text{train})}} L((\mathbf{x}, y), \hat{h})$$

5. compute validation error

$$E_v := (1/|\mathcal{D}^{(\text{val})}|) \sum_{(\mathbf{x}, y) \in \mathcal{D}^{(\text{val})}} L((\mathbf{x}, y), \hat{h})$$

We can diagnose a ERM-based ML method by comparing its training error with its validation error. This diagnosis is further enabled if we know a baseline  $E^{(\text{ref})}$ . One important source for a baseline  $E^{(\text{ref})}$  are probabilistic models for the data points (see Section 2.4).

Given a probabilistic model  $p(\mathbf{x}, y)$ , we can compute the minimum achievable risk (2.12). Indeed, the minimum achievable risk is precisely the expected loss of the Bayes estimator  $\hat{h}(\mathbf{x})$  of the label  $y$ , given the features  $\mathbf{x}$  of a data point. The Bayes estimator  $\hat{h}(\mathbf{x})$  is fully determined by the probability distribution  $p(\mathbf{x}, y)$  [30, Chapter 4].

A further potential source for a baseline  $E^{(\text{ref})}$  is an existing, but for some reason unsuitable, ML method. This existing ML method might be computationally too expensive to be used for the ML application at end. However, we might still use its statistical properties as a benchmark.

We can also use the performance of human experts as a baseline. If we want to develop a ML method that detects certain type of skin cancers from

images of the skin, a benchmark might be the current classification accuracy achieved by experienced dermatologists [31].

We can diagnose a ML method by comparing the training error  $E_t$  with the validation error  $E_v$  and (if available) the benchmark  $E^{(\text{ref})}$ .

- $E_t \approx E_v \approx E^{(\text{ref})}$ : The training error is on the same level as the validation error and the baseline. There is not much to improve here since the validation error is already close to the baseline. Moreover, the training error is not much smaller than the validation error which indicates that there is no overfitting.
- $E_v \gg E_t$ : The validation error is significantly larger than the training error. This is an indicator for overfitting. We can address overfitting by reducing the effective dimension of the hypothesis space or by increasing the size of the training set. We can reduce the effective dimension of the hypothesis space by using fewer features, a smaller maximum depth of decision trees or fewer layers in an ANN. An alternative to this discrete model selection, we can also reduce the effective dimension of a hypothesis space via regularization.
- $E_t \approx E_v \gg E^{(\text{ref})}$ : The training error is on the same level as the validation error and both are significantly larger than the baseline. Thus, the learnt hypothesis seems to not overfit the training set. However, the training error achieved by the learnt hypothesis is significantly larger than the baseline. There can be several reasons for this to happen. First, it might be that the hypothesis space is too small, i.e., it does not include a hypothesis that provides a good approximation for the

relation between features and label of a data point. One remedy to this situation is to use a larger hypothesis space, e.g., by including more features in a linear model, using higher polynomial degrees in polynomial regression, using deeper decision trees or ANNs (deep ANN (deep net)s). Second, besides the model being too small, another reason for a large training error could be that the optimization algorithm used to solve ERM (2.21) is not working properly (see Lecture 4).

- $E_t \gg E_v$ : The training error is significantly larger than the validation error. The idea of ERM (2.21) is to approximate the risk (2.12) of a hypothesis by its average loss on a training set  $\mathcal{D} = \{(\mathbf{x}^{(r)}, y^{(r)})\}_{r=1}^m$ . The mathematical underpinning for this approximation is the law of large numbers which characterizes the average of (realizations of) i.i.d. RVs. The accuracy of this approximation depends on the validity of two conditions: First, the data points used for computing the average loss “should behave” like realizations of i.i.d. RVs with a common probability distribution. Second, the number of data points used for computing the average loss must be sufficiently large.

Whenever the training set or validation set differs significantly from realizations of i.i.d. RVs, the interpretation (and comparison) of the training error and the validation error of a learnt hypothesis becomes more difficult. As an extreme case, the validation set might consist of data points for which every hypothesis incurs small average loss (see Figure 2.3). Here, we might try to increase the size of the validation set by collecting more labeled data points or by using data augmentation (see Section 2.6). If the size of training set and validation set are large

but we still obtain  $E_t \gg E_v$ , one should verify if data points in these sets conform to the i.i.d. assumption. There are principled statistical test for the validity of the i.i.d. assumption for a given dataset (see [32] and references therein).

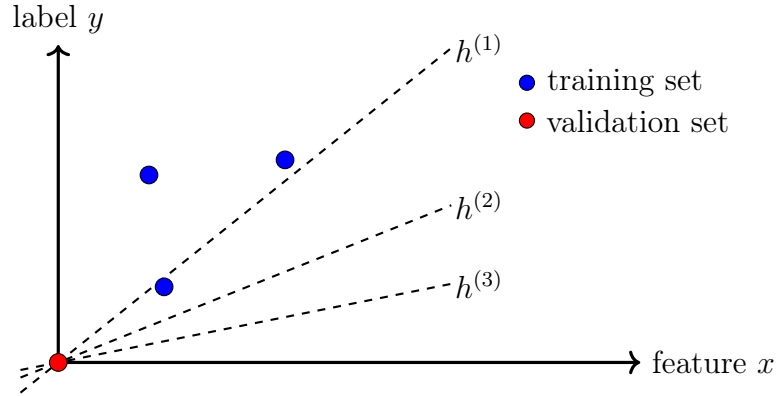


Figure 2.3: Example for an unlucky split into training set and validation set for the model  $\mathcal{H} := \{h^{(1)}, h^{(2)}, h^{(3)}\}$ .

## 2.6 Regularization

Consider a ERM-based ML method using a hypothesis space  $\mathcal{H}$  and dataset  $\mathcal{D}$  (we assume all data points are used for training). A key parameter for such a ML method is the ratio  $d_{\text{eff}}(\mathcal{H})/|\mathcal{D}|$  between the model size  $d_{\text{eff}}(\mathcal{H})$  and the number  $|\mathcal{D}|$  of data points. The tendency of the ML method to overfit increases with the ratio  $d_{\text{eff}}(\mathcal{H})/|\mathcal{D}|$ .

Regularization techniques reduce the ratio  $d_{\text{eff}}(\mathcal{H})/|\mathcal{D}|$  via three (essentially equivalent) approaches:

- collect more data points, possibly via data augmentation (see Fig. 2.4),
- add penalty term  $\lambda \mathcal{R}\{h\}$  to average loss in ERM (2.1) (see Fig. 2.4),
- shrink the hypothesis space, e.g., by adding constraints on the model parameters such as  $\|\mathbf{w}\|_2 \leq 10$ .

[5, Ch. 7] discusses the equivalence between these three perspectives on regularization in somewhat more detail.

One important example for regularization via adding a penalty term to the average loss is ridge regression. In particular, ridge regression uses the regularizer  $\mathcal{R}\{h\} := \|\mathbf{w}\|_2^2$  for a linear hypothesis  $h(\mathbf{x}) := \mathbf{w}^T \mathbf{x}$ . Thus, ridge regression learns the parameters of a linear hypothesis via solving

$$\hat{\mathbf{w}}^{(\lambda)} \in \operatorname{argmin}_{\mathbf{w} \in \mathbb{R}^d} \left[ (1/m) \sum_{r=1}^m (y^{(r)} - \mathbf{w}^T \mathbf{x}^{(r)})^2 + \lambda \|\mathbf{w}\|_2^2 \right]. \quad (2.22)$$

The objective function in (2.22) can be interpreted as the objective function of linear regression applied to a modification of the training set  $\mathcal{D}$ : We replace each data point  $(\mathbf{x}, y) \in \mathcal{D}$  by a sufficient large number of i.i.d. realizations of

$$(\mathbf{x} + \mathbf{n}, y) \text{ with } \mathbf{n} \sim \mathcal{N}(\mathbf{0}, \lambda \mathbf{I}). \quad (2.23)$$

Thus, ridge regression (2.22) is equivalent to linear regression applied to an augmented variant  $\mathcal{D}'$  of  $\mathcal{D}$ . The augmentation  $\mathcal{D}'$  is obtained by replacing each data point  $(\mathbf{x}, y) \in \mathcal{D}$  with a sufficiently large number of noisy copies. Each copy is obtained by adding a i.i.d. realization  $\mathbf{n}$  of a zero-mean Gaussian noise with covariance matrix  $\lambda \mathbf{I}$  to the features  $\mathbf{x}$  (see (2.23)). The label of each copy is equal to  $y$ , i.e., the label is not perturbed.

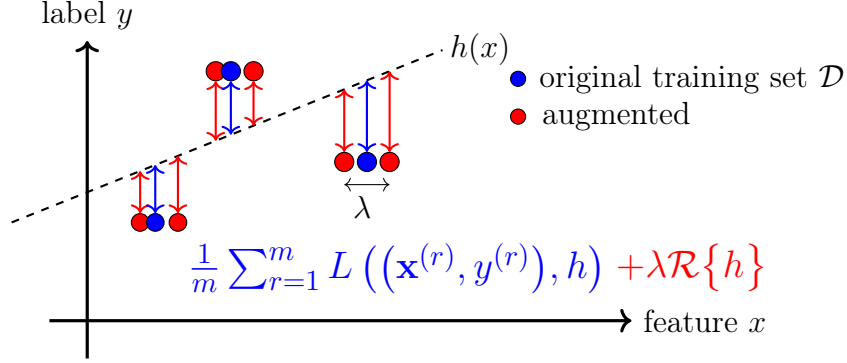


Figure 2.4: Equivalence between data augmentation and loss penalization.

To study the computational aspects of ridge regression, let us rewrite (2.22) as

$$\begin{aligned} \hat{\mathbf{w}}^{(\lambda)} &\in \operatorname{argmin}_{\mathbf{w} \in \mathbb{R}^d} \mathbf{w}^T \mathbf{Q} \mathbf{w} + \mathbf{w}^T \mathbf{q} \\ \text{with } \mathbf{Q} &:= (1/m) \mathbf{X}^T \mathbf{X} + \lambda \mathbf{I}, \mathbf{q} := (-2/m) \mathbf{X}^T \mathbf{y}. \end{aligned} \quad (2.24)$$

Thus, like linear regression (2.7), also ridge regression minimizes a convex quadratic function. A main difference between linear regression (2.7) and ridge regression (for  $\lambda > 0$ ) is that the matrix  $\mathbf{Q}$  in (2.24) is guaranteed to be invertible for any training set  $\mathcal{D}$ . In contrast, the matrix  $\mathbf{Q}$  in (2.7) for linear regression might be singular for some training sets.<sup>2</sup>

The statistical aspects of the solutions to (2.24) (i.e., the parameters learnt by ridge regression) crucially depends on the value of  $\lambda$ . This choice can be guided by an error analysis using a probabilistic model for the data (see Proposition 2.1). Instead of using a probabilistic model, we can also compare

---

<sup>2</sup>Consider the extreme case where all features of each data point in the training set  $\mathcal{D}$  are zero.

the training error and validation error of the hypothesis  $h(\mathbf{x}) = (\widehat{\mathbf{w}}^{(\lambda)})^T \mathbf{x}$  learnt by ridge regression with different values of  $\lambda$ .

## 2.7 Overview of Coding Assignment

**Source Code.** `Assignment_MLBasics.py`

**Data File.** `Assignment_MLBasicsData.csv`

**Description.** The coding assignment revolves around weather data collected by the FMI and stored in a csv file. This file contains temperature measurements at different locations in Finland. Each temperature measurement is a data point, characterized by  $d = 7$  features  $\mathbf{x} = (x_1, \dots, x_7)^T$  and a label  $y$  which is the temperature measurement itself. The features are (normalized) values of the latitude and longitude of the FMI station as well as the (normalized) year, month, day, hour, minute during which this measurements has been taken. Your tasks include:

- Generate `numpy` arrays `X, y`, whose  $r$ -th row hold the features  $\mathbf{x}^{(r)}$  and label  $y^{(r)}$ , respectively, of the  $r$ -th data point in the csv file.
- Split the dataset into a training set and validation set. The size of the training set should be 100.
- Train a linear model, using the `LinearRegression` class of the `scikit-learn` package, on the training set and determine the resulting training error and validation error
- Train and validate a linear model using feature augmentation via polynomial combinations (see `PolynomialFeatures` class). Try out different



different choices of the maximal degree of these polynomial combinations.

- Using a fixed value for the polynomial degree for the feature augmentation step, train and validate a linear model using ridge regression (2.22) via the `Ridge` class. For each choice of  $\lambda$  in (2.22), determine the resulting training error and validation error.

## 3 Lecture - “FL Design Principle”

February 6, 2024

Lecture 2 reviewed ML methods that use numeric arrays to store data and model parameters. We have also discussed ERM as a design principle for practical ML systems. This lecture will extend these concepts to FL applications. Section 3.2 introduces empirical graphs to store collections of local datasets and corresponding parameters of local models. Section 3.3 presents our main design principle for FL systems. This principle uses the variation of local model parameters across the edges of an empirical graph for the coupling (or regularization) of the individual local models.

### 3.1 Learning Goals

After this lecture, you should

- be familiar with the concept of an empirical graph,
- know how connectivity is related to spectrum of Laplacian matrix,
- know some measures for the variation of local models,
- be familiar with the concept of GTVMin.

### 3.2 Empirical Graphs and Their Laplacian

Consider a FL application that involves a collection of local datasets  $\mathcal{D}^{(1)}, \dots, \mathcal{D}^{(2)}$ . Our goal is to train a personalized model  $\mathcal{H}^{(i)}$  for each local dataset  $\mathcal{D}^{(i)}$ , with  $i = 1, \dots, n$ . We represent such a collection of local datasets and (personal)



Figure 3.1: Example of an empirical graph whose nodes  $i \in \mathcal{V}$  carry local datasets  $\mathcal{D}^{(i)}$  and local models that are parametrized by local model parameters  $\mathbf{w}^{(i)}$ .

local models, along with their relations, by an empirical graph. Figure 3.1 depicts an example for an empirical graph.

We model the local datasets generated in a FL application using an empirical graph. The empirical graph is an undirected weighted graph  $\mathcal{G} = (\mathcal{V}, \mathcal{E})$  with nodes  $\mathcal{V} := \{1, \dots, n\}$ . Each node  $i \in \mathcal{V}$  of the empirical graph  $\mathcal{G}$  carries a local dataset

$$\mathcal{D}^{(i)} := \{(\mathbf{x}^{(i,1)}, y^{(i,1)}), \dots, (\mathbf{x}^{(i,m_i)}, y^{(i,m_i)})\}. \quad (3.1)$$

Here,  $\mathbf{x}^{(i,r)}$  and  $y^{(i,r)}$  denote, respectively, the features and the label of the  $r$ th data point in the local dataset  $\mathcal{D}^{(i)}$ . Note that the size  $m_i$  of the local dataset might vary between different nodes  $i \in \mathcal{V}$ .

It is convenient to collect the feature vectors  $\mathbf{x}^{(i,r)}$  and labels  $y^{(i,r)}$  into a feature matrix  $\mathbf{X}^{(i)}$  and label vector  $\mathbf{y}^{(i)}$ , respectively,

$$\mathbf{X}^{(i)} := (\mathbf{x}^{(i,1)}, \dots, \mathbf{x}^{(i,m_i)})^T, \text{ and } \mathbf{y} := (y^{(1)}, \dots, y^{(m_i)})^T. \quad (3.2)$$

The local dataset  $\mathcal{D}^{(i)}$  can then be represented compactly by the matrix  $\mathbf{X}^{(i)} \in \mathbb{R}^{m_i \times d}$  and the vector  $\mathbf{y}^{(i)} \in \mathbb{R}^{m_i}$ .

Besides its local dataset  $\mathcal{D}^{(i)}$ , each node  $i \in \mathcal{G}$  also carries a local model  $\mathcal{H}^{(i)}$ . Within this course, we focus on local models that are parametrized by local model parameters  $\mathbf{w}^{(i)} \in \mathbb{R}^d$ , for  $i = 1, \dots, n$ . The usefulness of a specific choice for the local model parameter  $\mathbf{w}^{(i)}$  is measured by a local loss function  $L_i(\mathbf{w}^{(i)})$ , for  $i = 1, \dots, n$ .

An undirected edge  $\{i, i'\} \in \mathcal{E}$  between two different nodes  $i, i' \in \mathcal{V}$  couples the training of the corresponding local models  $\mathcal{H}^{(i)}, \mathcal{H}^{(i')}$ . We quantify the strength of this coupling by a positive edge weight  $A_{i,i'} > 0$ . The coupling will be implemented by penalizing the discrepancy between local model parameters  $\mathbf{w}^{(i)}$  and  $\mathbf{w}^{(i')}$  (see Section 3.3). Unless noted otherwise, we measure this discrepancy by the squared Euclidean distance  $\|\mathbf{w}^{(i)} - \mathbf{w}^{(i')}\|_2^2$ . The total variation of local model parameters is then obtained by

$$\sum_{i,i' \in \mathcal{V}} A_{i,i'} \|\mathbf{w}^{(i)} - \mathbf{w}^{(i')}\|_2^2. \quad (3.3)$$

We can characterize the connectivity of an empirical graph via the eigenvalues and eigenvectors of its Laplacian matrix  $\mathbf{L} \in \mathbb{R}^{n \times n}$ . The Laplacian matrix is defined element-wise as (see Fig. 3.2)

$$L_{i,i'} := \begin{cases} -A_{i,i'} & \text{for } i \neq i', \{i, i'\} \in \mathcal{E} \\ \sum_{i'' \neq i} A_{i,i''} & \text{for } i = i' \\ 0 & \text{else.} \end{cases} \quad (3.4)$$

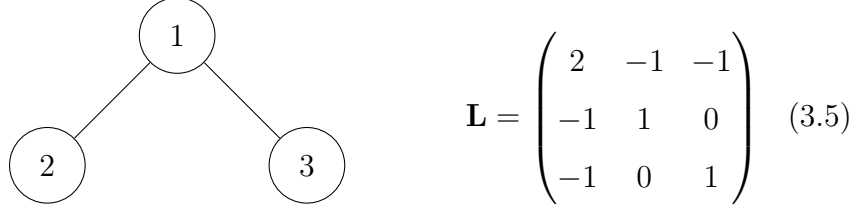


Figure 3.2: Left: Example for an empirical graph  $\mathcal{G}$  with three nodes  $i = 1, 2, 3$ . Right: Laplacian matrix  $\mathbf{L} \in \mathbb{R}^{3 \times 3}$  of  $\mathcal{G}$ .

The Laplacian matrix is symmetric and psd which follows from the identity

$$\begin{aligned} \mathbf{w}^T \mathbf{L} \mathbf{w} &= \sum_{\{i, i'\} \in \mathcal{E}} A_{i, i'} \left\| \mathbf{w}^{(i)} - \mathbf{w}^{(i')} \right\|_2^2 \\ \text{for any } \mathbf{w} &:= \underbrace{\left( (\mathbf{w}^{(1)})^T, \dots, (\mathbf{w}^{(n)})^T \right)^T}_{=:\text{stack}\left\{\mathbf{w}^{(i)}\right\}_{i=1}^n}. \end{aligned} \quad (3.6)$$

As a psd matrix,  $\mathbf{L}$  possesses an EVD

$$\mathbf{L} = \sum_{j=1}^n \lambda_j \mathbf{u}^{(j)} (\mathbf{u}^{(j)})^T, \quad (3.7)$$

with increasingly ordered eigenvalues

$$0 = \lambda_1(\mathbf{L}) \leq \dots \leq \lambda_n(\mathbf{L}). \quad (3.8)$$

According to (3.6), we can measure the total variation of local model parameters by stacking them into a single vector  $\mathbf{w} \in \mathbb{R}^{nd}$  and computing the quadratic form  $\mathbf{w}^T \mathbf{L} \mathbf{w}$ .

One immediate consequence of (3.6) is that any collection of identical local model parameters,  $\mathbf{w}^{(i)} = \mathbf{w}^{(i')}$  results in an eigenvector

$$\mathbf{c} = \left( (\mathbf{w}^{(1)})^T, \dots, (\mathbf{w}^{(n)})^T \right)^T. \quad (3.9)$$

with corresponding eigenvalue  $\lambda_1 = 0$  (see (3.8)). Thus, the Laplacian matrix of an empirical graph is always singular (non-invertible).

The second eigenvalue  $\lambda_2$  of the Laplacian matrix provides a great deal of information about the connectivity structure of  $\mathcal{G}$ . Consider the case  $\lambda_2 = 0$ , i.e., besides  $\mathbf{c}$  there is another eigenvector (not belonging to the  $\{a\mathbf{c} : a \in \mathbb{R}\}$ ) with zero eigenvalue. In this case, the graph  $\mathcal{G}$  is not connected, i.e., we can find two subsets (components) of nodes that do not have any edge between them.

On the other hand, if  $\lambda_2 > 0$  then  $\mathcal{G}$  is connected. Moreover, the larger the value of  $\lambda_2$ , the stronger the connectivity between the nodes in  $\mathcal{G}$ . We next show how to make this vague statement more precise via the identity (3.6).

The total variation on the RHS (3.6) is a measure for the connectivity. Indeed, if we assume that the local model parameters  $\mathbf{w}^{(i)}$  are different, then adding an edge will increase the total variation. We can lower bound the total variation as [33]

$$\sum_{\{i,i'\} \in \mathcal{E}} A_{i,i'} \left\| \mathbf{w}^{(i)} - \mathbf{w}^{(i')} \right\|_2^2 \geq \lambda_2 \sum_{i=1}^n \left\| \mathbf{w}^{(i)} - \mathbf{c} \right\|_2^2. \quad (3.10)$$

Here,  $\mathbf{c} := (1/n) \sum_{i=1}^n \mathbf{w}^{(i)}$  is the average of all local model parameters. The quantity  $\sum_{i=1}^n \left\| \mathbf{w}^{(i)} - \mathbf{c} \right\|_2^2$  has a geometric interpretation: It is the squared Euclidean norm of the projection of the stacked local model parameters  $\mathbf{w} := \left( (\mathbf{w}^{(1)})^T, \dots, (\mathbf{w}^{(n)})^T \right)^T$  on the orthogonal complement of the subspace

$$\left\{ \mathbf{1} \otimes \mathbf{a} : \mathbf{a} \in \mathbb{R}^d \right\} = \left\{ (\mathbf{a}^T, \dots, \mathbf{a}^T)^T, \text{ for some } \mathbf{a} \in \mathbb{R}^d \right\} \subseteq \mathbb{R}^{dn}. \quad (3.11)$$

It might be convenient to replace a given empirical graph  $\mathcal{G}$  with an



Figure 3.3: Left: Some empirical graph  $\mathcal{G}$  consisting of  $n = 4$  nodes. Right: Equivalent fully connected empirical graph  $\mathcal{G}'$  with the same nodes and non-zero edge weights  $A'_{i,i'} = A_{i,i'}$  and  $A'_{i,i'} = 0$  for  $\{i, i'\} \notin \mathcal{E}$ .

equivalent fully connected empirical graph  $\mathcal{G}'$  (see Figure 3.3). The graph  $\mathcal{G}'$  has an edge between each pair of different nodes  $i, i'$ ,

$$\mathcal{E}' = \{ \{i, i'\} , \text{ with some } i, i' \in \mathcal{V}, i \neq i' \}.$$

The edge weights are chosen  $A'_{i,i'} = A_{i,i'}$  for any edge  $\{i, i'\} \in \mathcal{E}$  and  $A'_{i,i'} = 0$  otherwise.

Note that the undirected edges  $\mathcal{E}$  of an empirical graph encode a symmetric notion of similarity between local datasets: If the local dataset  $\mathcal{D}^{(i)}$  at node  $i$  is similar to the local dataset  $\mathcal{D}^{(i')}$  at node  $i'$ , i.e.,  $\{i, i'\} \in \mathcal{E}$ , then also the local dataset  $\mathcal{D}^{(i')}$  is similar to the local dataset  $\mathcal{D}^{(i)}$ .

### 3.3 Generalized Total Variation Minimization

Consider data with empirical graph  $\mathcal{G}$  whose nodes  $i \in \mathcal{V}$  carry local datasets  $\mathcal{D}^{(i)}$  and local model parametrized by the vector  $\mathbf{w}^{(i)}$ . We learn these local model parameters by minimizing their local loss and at the same time enforce a small total variation and, in turn, similar local model parameters at well-connected nodes. To optimally balance local loss and total variation, we solve

generalized total variation (GTV) minimization,

$$\{\widehat{\mathbf{w}}^{(i)}\}_{i=1}^n \in \operatorname{argmin}_{\{\mathbf{w}^{(i)}\}} \sum_{i \in \mathcal{V}} L_i(\mathbf{w}^{(i)}) + \lambda \sum_{i, i' \in \mathcal{V}} A_{i, i'} \left\| \mathbf{w}^{(i)} - \mathbf{w}^{(i')} \right\|_2^2 \quad (\text{GTVMin}). \quad (3.12)$$

Note that GTVMin is an instance of RERM: The regularizer is the total variation of local model parameters over weighted edges  $A_{i, i'}$  of the empirical graph. Clearly, the empirical graph is an important design choice for GTVMin-based methods. This choice can be guided by computational aspects and statistical aspects of GTVMin-based FL systems.

Some application domains allow to leverage domain expertise to guess a useful choice for the empirical graph. If local datasets are generated at different geographic locations, we might use nearest-neighbour graphs based on geodesic distances between data generators (e.g., FMI weather stations). Lecture 7 will also discuss empirical graph learning methods that determine the edge weights  $A_{i, i'}$  in a fully data-driven fashion.

Let us now consider the special case of GTVMin with local models being a linear model. For each node  $i \in \mathcal{V}$  of the empirical graph, we want to learn the parameters  $\mathbf{w}^{(i)}$  of a linear hypothesis  $h^{(i)}(\mathbf{x}) := (\mathbf{w}^{(i)})^T \mathbf{x}$ . We measure the quality of the parameters via the average squared error loss

$$\begin{aligned} L_i(\mathbf{w}^{(i)}) &:= (1/m_i) \sum_{r=1}^{m_i} \left( y^{(i,r)} - (\mathbf{w}^{(i)})^T \mathbf{x}^{(i,r)} \right)^2 \\ &\stackrel{(3.2)}{=} (1/m_i) \left\| \mathbf{y}^{(i)} - \mathbf{X}^{(i)} \mathbf{w}^{(i)} \right\|_2^2. \end{aligned} \quad (3.13)$$

Inserting (3.13) into (3.12), yields the following instance of GTVMin to



train local linear models,

$$\{\widehat{\mathbf{w}}^{(i)}\}_{i=1}^n \in \operatorname{argmin}_{\{\mathbf{w}^{(i)}\}} \sum_{i \in \mathcal{V}} (1/m_i) \|\mathbf{y}^{(i)} - \mathbf{X}^{(i)} \mathbf{w}^{(i)}\|_2^2 + \lambda \sum_{i, i' \in \mathcal{V}} A_{i, i'} \|\mathbf{w}^{(i)} - \mathbf{w}^{(i')}\|_2^2. \quad (3.14)$$

The identity (3.6) allows to rewrite the GTVMin instance (3.14) as

$$\{\widehat{\mathbf{w}}^{(i)}\}_{i=1}^n \in \operatorname{argmin}_{\mathbf{w} = \operatorname{stack}\{\mathbf{w}^{(i)}\}_{i=1}^n} \sum_{i \in \mathcal{V}} (1/m_i) \|\mathbf{y}^{(i)} - \mathbf{X}^{(i)} \mathbf{w}^{(i)}\|_2^2 + \lambda \mathbf{w}^T \mathbf{L} \mathbf{w}. \quad (3.15)$$

Let us rewrite the objective function in (3.15) as

$$\mathbf{w}^T \left( \begin{pmatrix} \mathbf{Q}^{(1)} & 0 & \dots & 0 \\ 0 & \mathbf{Q}^{(2)} & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & \mathbf{Q}^{(n)} \end{pmatrix} + \lambda \mathbf{L} \otimes \mathbf{I} \right) \mathbf{w} + ((\mathbf{q}^{(1)})^T, \dots, (\mathbf{q}^{(n)})^T) \mathbf{w} \quad (3.16)$$

with  $\mathbf{Q}^{(i)} = (1/m_i)(\mathbf{X}^{(i)})^T \mathbf{X}^{(i)}$ , and  $\mathbf{q}^{(i)} := (-2/m_i)(\mathbf{X}^{(i)})^T \mathbf{y}^{(i)}$ .

Thus, like linear regression (2.7) and ridge regression (2.24), also GTVMin (3.15) (for local linear models  $\mathcal{H}^{(i)}$ ) minimizes a convex quadratic function,

$$\{\widehat{\mathbf{w}}^{(i)}\}_{i=1}^n \in \operatorname{argmin}_{\mathbf{w} = \operatorname{stack}\{\mathbf{w}^{(i)}\}_{i=1}^n} \mathbf{w}^T \mathbf{Q} \mathbf{w} + \mathbf{q}^T \mathbf{w}. \quad (3.17)$$

Here, we used the psd matrix

$$\mathbf{Q} := \begin{pmatrix} \mathbf{Q}^{(1)} & 0 & \dots & 0 \\ 0 & \mathbf{Q}^{(2)} & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & \mathbf{Q}^{(n)} \end{pmatrix} + \lambda \mathbf{L} \otimes \mathbf{I} \text{ with } \mathbf{Q}^{(i)} := (1/m_i)(\mathbf{X}^{(i)})^T \mathbf{X}^{(i)} \quad (3.18)$$

and the vector

$$\mathbf{q} := ((\mathbf{q}^{(1)})^T, \dots, (\mathbf{q}^{(n)})^T)^T, \text{ with } \mathbf{q}^{(i)} := (-2/m_i)(\mathbf{X}^{(i)})^T \mathbf{y}^{(i)}. \quad (3.19)$$

### 3.3.1 Computational Aspects of GTVMin

Lecture 5 will apply optimization methods to solve GTVMin, resulting in practical FL algorithms. Different instances of GTVMin favour different classes of optimization methods. For example, using a differentiable loss function allows to apply gradient-based methods (see Lecture 4) to solve GTVMin.

Another important class of loss functions are those for which we can efficiently compute the proximity operator

$$\mathbf{prox}_{L,\rho}(\mathbf{w}) := \underset{\mathbf{w}'}{\operatorname{argmin}} L(\mathbf{w}') + (\rho/2) \|\mathbf{w} - \mathbf{w}'\|_2^2 \text{ for some } \rho > 0.$$

Some authors refer to functions  $L$  for which  $\mathbf{prox}_{L,\rho}(\mathbf{w})$  can be computed easily as *simple* or *proximable* [34]. GTVMin with proximable loss functions can be solved quite efficiently via proximal algorithms [35].

Besides influencing the choice of optimization method, the design choices underlying GTVMin also determine the amount of computation that is required by a given optimization method. For example, using an empirical graph with relatively few edges (“sparse graphs”) typically results in a smaller computational complexity. Indeed, Lecture 5 discusses GTVMin-based algorithms requiring an amount of computation that is proportional to the number of edges in the empirical graph.

Let us now consider the computational aspects of GTVMin (3.14) to train local linear models. As discussed above, this instance is equivalent to solving

(3.17). Any solution  $\widehat{\mathbf{w}}$  of (3.17) (and, in turn, (3.14)) is characterized by the zero-gradient condition

$$\mathbf{Q}\widehat{\mathbf{w}} = -(1/2)\mathbf{q}, \quad (3.20)$$

with  $\mathbf{Q}, \mathbf{q}$  as defined in (3.18) and (3.19). If the matrix  $\mathbf{Q}$  in (3.20) is invertible, the solution to (3.20) and, in turn, to the GTVMin instance (3.14) is unique and given by  $\widehat{\mathbf{w}} = (-1/2)\mathbf{Q}^{-1}\mathbf{q}$ .

The size of the matrix  $\mathbf{Q}$  (see (3.18)) is proportional to the number of nodes in the empirical graph  $\mathcal{G}$ , which might be in the order of millions in some applications (such as social networks). For such large systems, we typically cannot use direct matrix inversion methods (e.g., based on Gaussian elimination) to compute  $\mathbf{Q}^{-1}$ .<sup>3</sup> Instead, we typically need to resort to iterative methods [36, 37].

Instead of using (3.20) to compute solutions to (3.17), we can also directly apply gradient-based methods (see Lecture 4) to solve (3.17). Starting from an initial choice for the local model parameters  $\widehat{\mathbf{w}}_0 = (\widehat{\mathbf{w}}_0^{(1)}, \dots, \widehat{\mathbf{w}}_0^{(n)})$ , we iterate the gradient step,

$$\widehat{\mathbf{w}}_{k+1} := \widehat{\mathbf{w}}_k - \alpha(2\mathbf{Q}\widehat{\mathbf{w}}_k + \mathbf{q}) \text{ for } k = 0, 1, \dots$$

The gradient step results in the updated local model parameters  $\widehat{\mathbf{w}}^{(i)}$  which we stacked into

$$\widehat{\mathbf{w}}_{k+1} := \left( (\widehat{\mathbf{w}}^{(1)})^T, \dots, (\widehat{\mathbf{w}}^{(n)})^T \right)^T.$$

We repeat the gradient step for a sufficient number of times, according to some stopping criterion (see Lecture 4).

---

<sup>3</sup>How many arithmetic operations (addition, multiplication) do you think are required to invert an arbitrary matrix  $\mathbf{Q}^{d \times d}$ ?

### 3.3.2 Statistical Aspects of GTVMin

What can we say about FL system that use the solutions of GTVMin (3.12) as local model parameters? To answer such a question, we use - as for the statistical analysis of ERM in Lecture 2 - a probabilistic model for the local datasets.

In what follows we focus on the GTVMin instance (3.14) to learn the parameters  $\mathbf{w}^{(i)}$  of a local linear model for each node  $i \in \mathcal{V}$ . For each local dataset  $\mathcal{D}^{(i)}$ , we assume that features and labels of its data points are realizations of i.i.d. RVs

$$\mathbf{y}^{(i)} = \underbrace{(\mathbf{x}^{(i,1)}, \dots, \mathbf{x}^{(i,m_i)})^T}_{\text{local feature matrix } \mathbf{X}^{(i)}} \bar{\mathbf{w}}^{(i)} + \boldsymbol{\epsilon}^{(i)} \text{ with } \mathbf{x}^{(i,r)} \stackrel{\text{i.i.d.}}{\sim} \mathcal{N}(\mathbf{0}, \mathbf{I}), \boldsymbol{\epsilon}^{(i)} \sim \mathcal{N}(\mathbf{0}, \sigma^2 \mathbf{I}). \quad (3.21)$$

In contrast to the probabilistic model (2.13) for the analysis of ERM, the probabilistic model involves node-specific parameters  $\bar{\mathbf{w}}^{(i)}$ , for  $i \in \mathcal{V}$ .

For a reasonable choice for empirical graph, the parameters  $\bar{\mathbf{w}}^{(i)}, \bar{\mathbf{w}}^{(i')}$  at connected nodes  $\{i, i'\} \in \mathcal{E}$  should be similar. However, we cannot choose the edge weights based on parameters  $\bar{\mathbf{w}}^{(i)}$  as they are unknown. We can only use (noisy) estimates for  $\bar{\mathbf{w}}^{(i)}$  the features and labels of the data points in the local datasets (see Lecture 7).

Consider a given (design) choice for the empirical graph (and its edge weights  $A_{i,i'}$ ) for local datasets that conform to the probabilistic model (3.21) with true underlying parameters  $\bar{\mathbf{w}}^{(i)}$ . For ease of exposition, we assume that

$$\bar{\mathbf{w}}^{(i)} = \bar{\mathbf{c}}, \text{ for some } \bar{\mathbf{c}} \in \mathbb{R}^d \text{ and all } i \in \mathcal{V}. \quad (3.22)$$

To study the deviation between the solutions  $\hat{\mathbf{w}}^{(i)}$  of (3.14) and the true

underlying parameters  $\overline{\mathbf{w}}^{(i)}$ , we decompose it as

$$\widehat{\mathbf{w}}^{(i)} =: \widetilde{\mathbf{w}}^{(i)} + (1/n) \sum_{i=1}^n \widehat{\mathbf{w}}^{(i)}. \quad (3.23)$$

The component  $(1/n) \sum_{i=1}^n \widehat{\mathbf{w}}^{(i)}$  is identical at all nodes  $i \in \mathcal{V}$ . The component  $\widetilde{\mathbf{w}}^{(i)} := \widehat{\mathbf{w}}^{(i)} - (1/n) \sum_{i=1}^n \widehat{\mathbf{w}}^{(i)}$  averages to the zero vector,  $(1/n) \sum_{i=1}^n \widetilde{\mathbf{w}}^{(i)} = \mathbf{0}$ .

**Proposition 3.1.** *Consider a connected empirical graph, i.e.,  $\lambda_2 > 0$  (see (3.8)), and the solution (3.23) to GTVMin (3.14) for the local datasets (3.21). If the true local model parameters in (3.21) are identical (see (3.22)), we can upper bound the component  $\widetilde{\mathbf{w}}^{(i)} := \widehat{\mathbf{w}}^{(i)} - (1/n) \sum_{i=1}^n \widehat{\mathbf{w}}^{(i)}$  as*

$$\sum_{i=1}^n \|\widetilde{\mathbf{w}}^{(i)}\|_2^2 \leq \frac{1}{\lambda_2 \lambda} \sum_{i=1}^n (1/m_i) \|\boldsymbol{\varepsilon}^{(i)}\|_2^2. \quad (3.24)$$

*Proof.* Let us introduce the shorthand  $f(\mathbf{w}^{(i)})$  for the objective function of the GTVMin instance (3.14). We verify the bound (3.24) by showing that if it does not hold, the choice for the local model parameters  $\mathbf{w}^{(i)} := \overline{\mathbf{w}}^{(i)}$  (see (3.21)) results in a smaller objective function value,  $f(\overline{\mathbf{w}}^{(i)}) < f(\widehat{\mathbf{w}}^{(i)})$ . This would contradict the fact that  $\widehat{\mathbf{w}}^{(i)}$  is a solution to (3.14).

First, note that

$$\begin{aligned} f(\overline{\mathbf{w}}^{(i)}) &= \sum_{i \in \mathcal{V}} (1/m_i) \|\mathbf{y}^{(i)} - \mathbf{X}^{(i)} \overline{\mathbf{w}}^{(i)}\|_2^2 + \lambda \sum_{i, i' \in \mathcal{V}} A_{i, i'} \|\overline{\mathbf{w}}^{(i)} - \overline{\mathbf{w}}^{(i')}\|_2^2 \\ &\stackrel{(3.22)}{=} \sum_{i \in \mathcal{V}} (1/m_i) \|\mathbf{y}^{(i)} - \mathbf{X}^{(i)} \overline{\mathbf{w}}^{(i)}\|_2^2 \\ &\stackrel{(3.21)}{=} \sum_{i \in \mathcal{V}} (1/m_i) \|\mathbf{X}^{(i)} \overline{\mathbf{w}}^{(i)} + \boldsymbol{\varepsilon}^{(i)} - \mathbf{X}^{(i)} \overline{\mathbf{w}}^{(i)}\|_2^2 \\ &= \sum_{i \in \mathcal{V}} (1/m_i) \|\boldsymbol{\varepsilon}^{(i)}\|_2^2. \end{aligned} \quad (3.25)$$

Inserting (3.23) into (3.14),

$$\begin{aligned}
f(\widehat{\mathbf{w}}^{(i)}) &= \underbrace{\sum_{i \in \mathcal{V}} (1/m_i) \|\mathbf{y}^{(i)} - \mathbf{X}^{(i)} \widehat{\mathbf{w}}^{(i)}\|_2^2}_{\geq 0} + \lambda \sum_{i, i' \in \mathcal{V}} A_{i, i'} \underbrace{\|\widehat{\mathbf{w}}^{(i)} - \widehat{\mathbf{w}}^{(i')}\|_2^2}_{=\|\widetilde{\mathbf{w}}^{(i)} - \widetilde{\mathbf{w}}^{(i')}\|_2^2} \\
&\geq \lambda \sum_{i, i' \in \mathcal{V}} A_{i, i'} \|\widetilde{\mathbf{w}}^{(i)} - \widetilde{\mathbf{w}}^{(i')}\|_2^2 \\
&\stackrel{(3.10)}{\geq} \lambda \lambda_2 \sum_{i=1}^n \|\widetilde{\mathbf{w}}^{(i)}\|_2^2.
\end{aligned} \tag{3.26}$$

If the bound (3.24) would not hold, then by (3.26) and (3.25) we would obtain  $f(\widehat{\mathbf{w}}^{(i)}) > f(\overline{\mathbf{w}}^{(i)})$ . This is a contradiction to the fact that  $\widehat{\mathbf{w}}^{(i)}$  solves (3.14).  $\square$

The empirical graph should contain sufficient number of edges between nodes that carry statistically similar local datasets. This allows regularization techniques to adaptively pool local datasets into clusters of (approximately) homogeneous data (see Section 6.3).

Statistically, we want the loss function to favour local model parameters that result in a robust and accurate trained local model, with model parameters  $\widehat{\mathbf{w}}^{(i)}$ , for each node  $i \in \mathcal{V}$ .

### 3.4 Overview of Coding Assignment

**Data File.** `Assignment_MLBasicsData.csv`

**Python source.** `Assignment_FLDDesignPrinciple.py`

This assignment revolves around a collection of temperature measurements that we store in the empirical graph  $\mathcal{G}^{(\text{FMI})}$ . Each node  $i \in \mathcal{V}$  represents a FMI weather station at latitude  $\text{lat}^{(i)}$  and longitude  $\text{lon}^{(i)}$ . The local dataset  $\mathcal{D}^{(i)}$  contains  $m_i$  temperature measurements  $y^{(i,1)}, \dots, y^{(i,m_i)}$  at the station  $i$ .

The edges of  $\mathcal{G}^{(\text{FMI})}$  are obtained using the Python function `add_edges()`. Each FMI station  $i$  is connected to its nearest neighbours  $i'$ , using the Euclidean distance between the corresponding vectors  $(\text{lat}^{(i)}, \text{lon}^{(i)})^T \in \mathbb{R}^2$ . The number of neighbours is controlled by the input parameter `numneighbors`. All edges  $\{i, i'\} \in \mathcal{E}$  have the same edge weight  $A_{i,i'} = 1$ .

For each station  $i \in \mathcal{V}$ , you need to learn the single parameter  $w^{(i)} \in \mathbb{R}$  of a hypothesis  $h(x) = w^{(i)}$  that predicts the temperature. We measure the quality of a hypothesis by the average squared error loss  $L_i(w^{(i)}) = (1/m_i) \sum_{r=1}^{m_i} (y^{(i,r)} - w^{(i)})^2$ . You should learn the parameters  $w^{(i)}$  via balancing the local loss with the total variation of  $w^{(i)}$ ,

$$\hat{w}^{(i)} \in \underset{\{w^{(i)}\}_{i=1}^n}{\text{argmin}} \sum_{i=1}^n L_i(w^{(i)}) + \lambda \sum_{\{i,i'\} \in \mathcal{E}} (w^{(i)} - w^{(i')})^2. \quad (3.27)$$

Your tasks involve

- Reformulate (3.27) as (3.14) using a suitable choice for features  $\mathbf{x}^{(i,r)}$ ,
- The computation of solutions  $\hat{w}^{(i)}$  to (3.27) via (3.20). To this end, you should determine the matrix  $\mathbf{Q}$  and vector  $\mathbf{q}$  in terms of local datasets  $\mathcal{D}^{(i)}$  and the Laplacian matrix  $\mathbf{L}^{(\text{FMI})}$  of the empirical graph  $\mathcal{G}^{(\text{FMI})}$ .
- Studying the effect of varying values of  $\lambda$  in (3.27) on the local loss and total variation of the corresponding solutions  $\hat{w}^{(i)}$ .

## 4 Lecture - “Gradient Methods”

February 6, 2024

Lecture 3 introduced GTVMin as a central design principle for FL methods. Many important instances of GTVMin require to minimize a smooth objective function  $f(\mathbf{w})$  over the parameter space  $\mathbb{R}^d$ . This lecture explores gradient-based methods, a widely used family of iterative algorithms to find the minimum of a smooth function. These methods approximate the objective function locally using its gradient at the current model parameters. Lecture 5 focuses on FL algorithms obtained from the application of gradient-based methods to solve GTVMin.

### 4.1 Learning Goals

After this lecture, you should

- have some intuition about the effect of a gradient step,
- understand the role of the step size (or learning rate),
- know some examples for a stopping criterion,
- be able to analyze the effect of perturbations in the gradient step,
- know about projected GD to cope with constraints on model parameters.

### 4.2 Gradient Descent

Unless stated otherwise, we consider an objective function of form

$$f(\mathbf{w}) = \mathbf{w}^T \mathbf{Q} \mathbf{w} + \mathbf{q}^T \mathbf{w}. \quad (4.1)$$



Note that (4.1) defines a family of convex quadratic functions. Each member of this family is specified by a psd matrix  $\mathbf{Q} \in \mathbb{R}^{d \times d}$  and a vector  $\mathbf{q} \in \mathbb{R}^d$ .

We have already encountered some ML and FL methods that involve an objective function of the form (4.1): Linear regression (2.3) and ridge regression (2.24) in Lecture 2 as well as GTVMin (3.14) for local linear models in Lecture 3. Moreover, (4.1) might serve as a useful approximation for the objective functions arising for larger classes of ML methods [38–40].

Given model parameters  $\mathbf{w}^{(r)}$ , we want to update them towards a minimum of (4.1). To this end, we use the gradient  $\nabla f(\mathbf{w}^{(r)})$  to locally approximate  $f(\mathbf{w})$  (see Figure 4.1). The gradient  $\nabla f(\mathbf{w}^{(r)})$  indicates the direction in which the function  $f(\mathbf{w})$  maximally increases. Therefore, it seems reasonable to update  $\mathbf{w}^{(r)}$  in the opposite direction of  $\nabla f(\mathbf{w}^{(r)})$ ,

$$\begin{aligned} \mathbf{w}^{(r+1)} &:= \mathbf{w}^{(r)} - \alpha \nabla f(\mathbf{w}^{(r)}) \\ &\stackrel{(4.1)}{=} \mathbf{w}^{(r)} - \alpha (2\mathbf{Q}\mathbf{w}^{(r)} + \mathbf{q}). \end{aligned} \tag{4.2}$$

The gradient step (4.2) involves the factor  $\alpha$  which we refer to as step-size or learning rate. Algorithm 1 summarizes the most basic instance of gradient-based methods which simply repeats (iterates) (4.2) until some stopping criterion is met.

The usefulness of gradient-based methods crucially depends on the ability to efficiently evaluate the gradient  $\nabla f(\mathbf{w})$ . Evaluating the gradient of a fully specified function has been made convenient by modern software libraries for automatic differentiation [41]. However, besides the actual computation of the gradient, it might be already challenging to gather the required data points which define the objective function  $f(\mathbf{w})$ . Indeed, the matrix  $\mathbf{Q}$  and

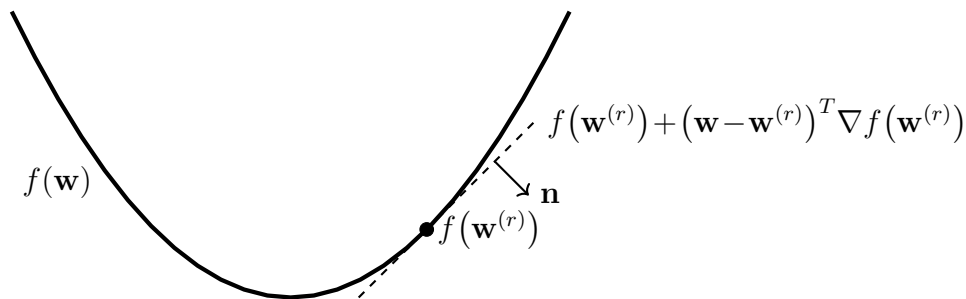


Figure 4.1: We can approximate a differentiable function  $f(\mathbf{w})$  locally around a point  $\mathbf{w}^{(r)} \in \mathbb{R}^d$  using a hyperplane. The normal vector  $\mathbf{n} = (\nabla f(\mathbf{w}^{(r)}), -1)^T \in \mathbb{R}^{d+1}$  of this approximating hyperplane is determined by the gradient  $\nabla f(\mathbf{w}^{(r)})$  [6].

vector  $\mathbf{q}$  in (4.1) are constructed from the features and labels of data points in the training set (see, e.g., (2.24)).

---

**Algorithm 1** A blueprint for gradient-based methods

---

**Input:** function  $f(\mathbf{w})$  ; learning rate  $\alpha > 0$ ; some stopping criterion;

**Initialize:** set  $\mathbf{w}^{(0)} := \mathbf{0}$ ; set iteration counter  $r := 0$

1: **repeat**

2:      $r := r + 1$  (increase iteration counter)

3:      $\mathbf{w}^{(r)} := \mathbf{w}^{(r-1)} - \alpha \nabla f(\mathbf{w}^{(r-1)})$  (do a gradient step (4.2))

4: **until** stopping criterion is met

**Output:**  $\hat{\mathbf{w}} := \mathbf{w}^{(r)}$  (hopefully  $f(\hat{\mathbf{w}}) \approx \min_{\mathbf{w}} f(\mathbf{w})$ )

---

Note that Algorithm 1, as most other gradient-based methods, involves two hyper-parameters: (i) the learning rate  $\alpha$  used for the gradient step and (ii) a stopping criterion to decide when to stop repeating the gradient step.

We next discuss some popular strategies for choosing these hyper-parameters.

### 4.3 Learning Rate

The learning rate must not be too large to avoid overshooting or moving away from the optimum (see Figure 4.2-(b)). On the other hand, if the learning rate is chosen too small, the gradient step makes too little progress towards the solutions of (4.1) (see Figure 4.2-(a)). Note that in practice we can only afford to repeat the gradient step for a finite number of iterations.

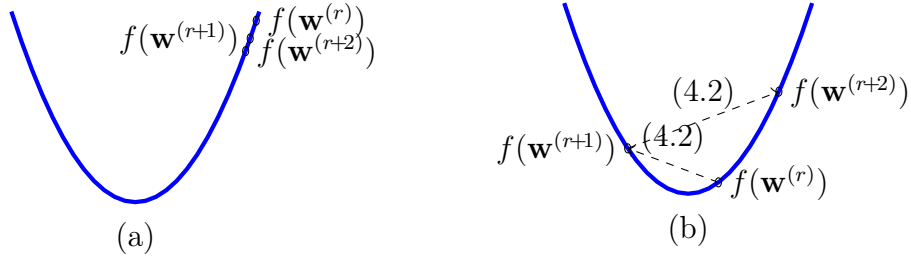


Figure 4.2: Effect of inadequate learning rates  $\alpha$  in the gradient step (4.2). (a) If  $\alpha$  is too small, the gradient steps make very little progress towards the optimum or even fail to reach the optimum at all. (b) If  $\alpha$  is too large, the gradient steps might “overshoot” such that the iterates  $\mathbf{w}^{(r)}$  might diverge from the optimum, i.e.,  $f(\mathbf{w}^{(r+1)}) > f(\mathbf{w}^{(r)})$ !

One approach to choose the learning rate is to start with some initial value (first guess) and monitor the decrease of the objective function. If this decrease does not agree with the decrease predicted by the (local linear approximation using the) gradient, we decrease the learning rate by a constant factor. After we decrease the learning rate, we re-consider the decrease of the

objective function. We repeat this procedure until a sufficient decrease of the objective function is achieved [42, Sec 6.1].

Alternatively, we can use a prescribed sequence (schedule)  $\alpha_r$ , for  $r = 1, 2, \dots$ , of learning rates that vary across successive gradient steps [43]. We can guarantee convergence of (4.2) (under mild assumptions on the objective function  $f(\mathbf{w})$ ) by using a learning rate schedule that satisfies [42, Sec. 6.1]

$$\lim_{r \rightarrow \infty} \alpha_r = 0, \quad \sum_{r=1}^{\infty} \alpha_r = \infty, \quad \text{and} \quad \sum_{r=1}^{\infty} \alpha_r^2 < \infty. \quad (4.3)$$

The first condition (4.3) requires that the learning rate eventually become sufficiently small to avoid overshooting. The third condition (4.3) requires that the learning rate decays sufficiently fast. Note that the first and third condition in (4.3) could be satisfied by the trivial learning rate schedule  $\alpha_r = 0$  which is clearly not useful as the gradient step has no effect. This trivial schedule is prohibited by the middle condition of (4.3) which requires that the learning rate  $\alpha_r$  is large enough such that the gradient step makes sufficient progress.

## 4.4 When to Stop?

For the stopping criterion we might use a fixed number  $r_{\max}$  of iterations. This hyper-parameter  $r_{\max}$  might be dictated by limited resources (such as computational time) for implementing GD or tuned via validation techniques.

We can obtain another stopping criterion from monitoring the decrease in the objective function  $f(\mathbf{w}^{(r)})$ : we stop repeating the gradient step (4.2) whenever  $|f(\mathbf{w}^{(r)}) - f(\mathbf{w}^{(r+1)})| \leq \eta$  for a given tolerance  $\eta$ . The tolerance level  $\eta$  is a hyper-parameter of the resulting ML method which could be

chosen via validation techniques (see Lecture 2).

The above techniques for choosing the learning rate  $\alpha$  and deciding when to stop the gradient steps might be useful in practice. However, they might result in sub-optimal use of computational resources for situations where we have some information about the psd matrix  $\mathbf{Q}$  in (4.1). Indeed, the choice for the learning rate  $\alpha$  and the stopping criterion can be guided by the eigenvalues

$$0 \leq \lambda_1(\mathbf{Q}) \leq \dots \leq \lambda_d(\mathbf{Q}). \quad (4.4)$$

Even if we do not know these eigenvalues precisely, we might know (or be able to ensure via feature learning) some upper and lower bounds,

$$0 \leq L \leq \lambda_1(\mathbf{Q}) \leq \dots \leq \lambda_d(\mathbf{Q}) \leq U. \quad (4.5)$$

In what follows, we assume that  $\mathbf{Q}$  is invertible and we know some positive lower bound  $L > 0$  (see (4.5)).<sup>4</sup> The objective function (4.1) has then a unique solution  $\widehat{\mathbf{w}}$ . It turns out that a gradient step (4.2) reduces the distance  $\|\mathbf{w}^{(r)} - \widehat{\mathbf{w}}\|_2$  to  $\widehat{\mathbf{w}}$  by a constant factor [42, Ch. 6],

$$\|\mathbf{w}^{(r+1)} - \widehat{\mathbf{w}}\|_2 \leq \kappa^{(\alpha_r)}(\mathbf{Q}) \|\mathbf{w}^{(r)} - \widehat{\mathbf{w}}\|_2. \quad (4.6)$$

Here, we used the contraction factor

$$\kappa^{(\alpha)}(\mathbf{Q}) := \max\{|1 - \alpha 2\lambda_1|, |1 - \alpha 2\lambda_d|\}. \quad (4.7)$$

The contraction factor depends on the learning rate  $\alpha$  which is a hyperparameter of gradient-based methods that we can control. However, the

---

<sup>4</sup>What are sufficient conditions for the local datasets and the edge weights used in GTVMin such that  $\mathbf{Q}$  in (3.18) is invertible?

contraction factor also depends on the eigenvalues of the matrix  $\mathbf{Q}$  in (4.1). In ML and FL applications, this matrix typically depends on data and can be controlled only to some extent, e.g., using feature transformation [5, Ch. 5]. We can ensure  $\kappa^{(\alpha)}(\mathbf{Q}) < 1$  if we use a positive learning rate  $\alpha_r < 1/U$ .

For a contraction factor  $\kappa^{(\alpha)}(\mathbf{Q}) < 1$ , a sufficient condition on the number  $r^{(\eta)}$  of gradient steps required to ensure an optimization error  $\|\mathbf{w}^{(r+1)} - \hat{\mathbf{w}}\|_2 \leq \eta$  is (see (4.6))

$$r^{(\eta)} \geq \log (\|\mathbf{w}^{(0)} - \hat{\mathbf{w}}\|_2 / \eta) / \log (1 / \kappa^{(\alpha)}(\mathbf{Q})). \quad (4.8)$$

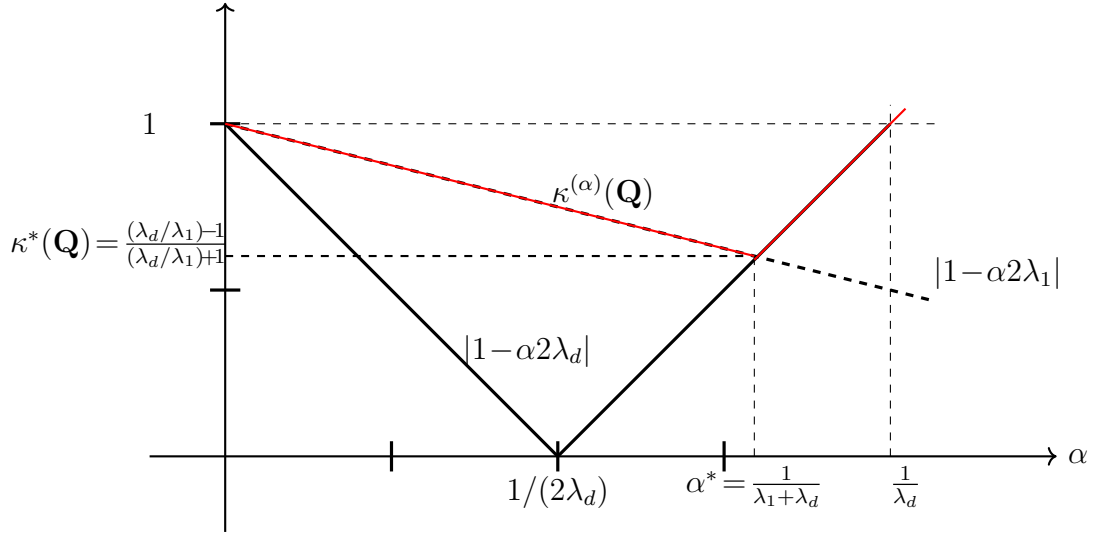


Figure 4.3: The contraction factor  $\kappa^{(\alpha)}(\mathbf{Q})$  (4.7), used in the upper bound (4.6), as a function of the learning rate  $\alpha$ . Note that  $\kappa^{(\alpha)}(\mathbf{Q})$  also depends on the eigenvalues of the matrix  $\mathbf{Q}$  in (4.1).

According to (4.6), smaller values of the contraction factor  $\kappa^{(\alpha)}(\mathbf{Q})$  guarantee a faster convergence of (4.2) towards the solution of (4.1). Figure 4.3 illustrates the dependence of  $\kappa^{(\alpha)}(\mathbf{Q})$  on the learning rate  $\alpha$ . Thus, choosing a small  $\alpha$  (close to 0) will typically result in a larger  $\kappa^{(\alpha)}(\mathbf{Q})$  and, in turn, require more iterations to ensure optimization error level  $\eta$  via (4.6).

We can minimize this contraction factor using the learning rate (see Figure 4.3)

$$\alpha^{(*)} := \frac{1}{\lambda_1 + \lambda_d}. \quad (4.9)$$

[Note that evaluating (4.9) requires to know the extremal eigenvalues  $\lambda_1, \lambda_d$  of  $\mathbf{Q}$ .] Inserting the optimal learning rate (4.9) into (4.6),

$$\|\mathbf{w}^{(r+1)} - \widehat{\mathbf{w}}\|_2 \leq \underbrace{\frac{(\lambda_d/\lambda_1) - 1}{(\lambda_d/\lambda_1) + 1}}_{:=\kappa^*(\mathbf{Q})} \|\mathbf{w}^{(r)} - \widehat{\mathbf{w}}\|_2. \quad (4.10)$$

Carefully note that the formula (4.10) is valid only if the matrix  $\mathbf{Q}$  in (4.1) is invertible, i.e., if  $\lambda_1 > 0$ . If the matrix  $\mathbf{Q}$  is singular ( $\lambda_1 = 0$ ), the convergence of (4.2) towards a solution of (4.1) is much slower than the decrease of the bound (4.10). However, we can still ensure converge of gradient steps by using a fixed learning rate  $\alpha_r = \alpha$  that satisfies [44, Thm. 2.1.14]

$$0 < \alpha < 1/\lambda_d(\mathbf{Q}). \quad (4.11)$$

It is interesting to note that for linear regression, the matrix  $\mathbf{Q}$  depends only on the features  $\mathbf{x}^{(r)}$  of the data points in the training set (see (2.17)) but not on their labels  $y^{(r)}$ . Thus, the convergence of gradient steps is only affected by the features, whereas the labels are irrelevant. The same is true for ridge regression and GTVMin (using local linear models).

Note that both, the optimal learning rate (4.9) and the optimal contraction factor

$$\kappa^*(\mathbf{Q}) := \frac{(\lambda_d/\lambda_1) - 1}{(\lambda_d/\lambda_1) + 1} \quad (4.12)$$

depend on the eigenvalues of the matrix  $\mathbf{Q}$  in (4.1). According to (4.10), the ideal case is when all eigenvalues are identical which leads, in turn, to a contraction factor  $\kappa^*(\mathbf{Q}) = 0$ . Here, a single gradient step is enough to arrive at a solution of (4.1).

In general, we do not have full control over the matrix  $\mathbf{Q}$  and its eigenvalues. For example, the matrix  $\mathbf{Q}$  arising in linear regression (2.7) is determined by the features of data points in the training set. These features might be obtained from sensing devices and therefore beyond our control. However, other applications might allow for some design freedom in the choice of feature vectors. We might also use feature transformations that nudge the resulting  $\mathbf{Q}$  in (2.7) more towards a scaled identity matrix.

## 4.5 Perturbed Gradient Step

Consider the gradient step (4.2) used to find a minimum of (4.1). We again assume that the matrix  $\mathbf{Q}$  in (4.1) is invertible ( $\lambda_1(\mathbf{Q}) > 0$ ) and, in turn, (4.1) has a unique solution  $\hat{\mathbf{w}}$ .

In some applications, it might be difficult to evaluate the gradient  $\nabla f(\mathbf{w}) = \mathbf{Q}\mathbf{w} + \mathbf{q}$  of (4.1) exactly. For example, this evaluation might require to gather data points from distributed storage locations. These storage locations might become unavailable during the computation of  $\nabla f(\mathbf{w})$  due to software or hardware failures (e.g., limited connectivity).

We can model imperfections during the computation of (4.2) as the



perturbed gradient step

$$\begin{aligned}\mathbf{w}^{(r+1)} &:= \mathbf{w}^{(r)} - \alpha \nabla f(\mathbf{w}^{(r)}) + \boldsymbol{\varepsilon}^{(r)} \\ &\stackrel{(4.1)}{=} \mathbf{w}^{(r)} - \alpha(2\mathbf{Q}\mathbf{w}^{(r)} + \mathbf{q}) + \boldsymbol{\varepsilon}^{(r)}.\end{aligned}\tag{4.13}$$

We can use the contraction factor (4.7) to upper bound the deviation between  $\mathbf{w}^{(r)}$  and the optimum  $\hat{\mathbf{w}}$  as (see (4.6))

$$\|\mathbf{w}^{(r)} - \hat{\mathbf{w}}\|_2 \leq (\kappa^{(\alpha)}(\mathbf{Q}))^r \|\mathbf{w}^{(0)} - \hat{\mathbf{w}}\|_2 + \sum_{r'=1}^r (\kappa^{(\alpha)}(\mathbf{Q}))^{r'} \|\boldsymbol{\varepsilon}^{(r-r')}\|_2. \tag{4.14}$$

This bound applies for any number of iterations  $r = 1, 2, \dots$  of the perturbed gradient step (4.13).

## 4.6 Handling Constraints - Projected Gradient Descent

Many important ML and FL methods amount to the minimization of an objective function of the form (4.1). The optimization variable  $\mathbf{w}$  in (4.1) represents some model parameters.

Sometimes we might require the parameters  $\mathbf{w}$  to belong to a subset  $\mathcal{C} \subset \mathbb{R}^d$ . One example is regularization via model pruning (see Lecture 2). Another example are FL methods that learn identical local model parameters  $\mathbf{w}^{(i)}$  at all nodes  $i \in \mathcal{V}$  of an empirical graph. This can be implemented by requiring the stacked local model parameters  $\mathbf{w} = (\mathbf{w}^{(1)}, \dots, \mathbf{w}^{(n)})^T$  to belong to the subset

$$\mathcal{C} = \left\{ (\mathbf{w}^{(1)}, \dots, \mathbf{w}^{(n)})^T : \mathbf{w}^{(1)} = \dots = \mathbf{w}^{(n)} \right\}.$$

Let us now show how to adapt the gradient step (4.2) to solve the constrained problem

$$f^* = \min_{\mathbf{w} \in \mathcal{C}} \mathbf{w}^T \mathbf{Q} \mathbf{w} + \mathbf{q}^T \mathbf{w}. \tag{4.15}$$

We assume that the constraint set  $\mathcal{C} \subseteq \mathbb{R}^d$  is such that we can efficiently compute the projection

$$P_{\mathcal{C}}(\mathbf{w}) = \operatorname{argmin}_{\mathbf{w}' \in \mathcal{C}} \|\mathbf{w} - \mathbf{w}'\|_2 \text{ for any } \mathbf{w} \in \mathbb{R}^d. \quad (4.16)$$

A suitable modification of the gradient step (4.2) to solve the constrained variant (4.15) is [42]

$$\begin{aligned} \mathbf{w}^{(r+1)} &:= P_{\mathcal{C}}(\mathbf{w}^{(r)} - \alpha \nabla f(\mathbf{w}^{(r)})) \\ &\stackrel{(4.1)}{=} P_{\mathcal{C}}(\mathbf{w}^{(r)} - \alpha(2\mathbf{Q}\mathbf{w}^{(r)} + \mathbf{q})). \end{aligned} \quad (4.17)$$

The projected GD step (4.17) amounts to

1. compute ordinary gradient step  $\mathbf{w}^{(r)} \mapsto \mathbf{w}^{(r)} - \alpha \nabla f(\mathbf{w}^{(r)})$  and
2. project back to the constraint set  $\mathcal{C}$ .

Note that we re-obtain the basic gradient step (4.2) from the projected gradient step (4.17) for the specific constraint set  $\mathcal{C} = \mathbb{R}^d$ .

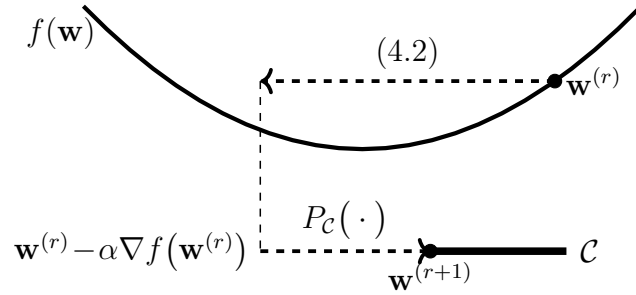


Figure 4.4: Projected GD augments a basic gradient step with a projection back onto the constraint set  $\mathcal{C}$ .

The approaches for choosing the learning rate  $\alpha$  and stopping criterion for basic gradient step (4.2) explained in Sections 4.3 and 4.4 work also for

the projected gradient step (4.17). In particular, somewhat surprisingly, the convergence speed of the projected gradient step is also characterized by (4.6) [42, Ch. 6].

Thus, the convergence speed of projected GD, in terms of number of iterations required to ensure a given level of optimization error, is essentially the same as that of basic GD. However, the bound (4.6) is only telling about the number of projected gradient steps (4.17) required to achieve a guaranteed level of sub-optimality  $|f(\mathbf{w}^{(r)}) - f^*|$ . The iteration (4.17) of projected GD might require significantly more computation than the basic gradient step, as it requires to compute the projection (4.16).

## 4.7 Overview of Coding Assignment

**Source Code.** `Assignment_GradientMethods.py`

**Data File.** `Assignment_MLBasicsData.csv`

**Description.** This assignment builds on the assignment for Lecture 2 which used ready-made `Python` implementations of linear regression and ridge regression. Now you have to implement ridge regression “from scratch”, by applying Algorithm 1 to solve the ridge regression problem (2.24).

The features are (normalized) values of the latitude, longitude of the FMI station as well as the (normalized) year, month, day, hour, minute during which this measurements has been taken. Your tasks include

- Generate `numpy` arrays  $\mathbf{X}, \mathbf{y}$ , whose  $r$ -th row hold the features  $\mathbf{x}^{(r)}$  and label  $y^{(r)}$ , respectively, of the  $r$ -th data point in the csv file.
- Split the dataset into a training set and validation set. The size of the

training set should be 100.

- Train a linear model, using the `RidgeRegression` class of the `scikit-learn` package, on the training set and determine the resulting training error and validation error
- Implement the GD Algorithm 1 for the objective function (2.24). Use the initialization  $\mathbf{w}^{(0)} = \mathbf{0}$ . Try out different choices for the learning rate  $\alpha$  and the (fixed) number  $r_{\max}$  of iterations.
- For each choice of  $\alpha$  and  $r_{\max}$ , monitor and plot the objective function value  $f(\mathbf{w}^{(r)})$  for the model parameters as a function of the iteration counter  $r$  in Algorithm 1.

## 5 Lecture - “FL Algorithms”

Lecture 3 introduced GTVMin as a central design principle for FL methods. The solutions of GTVMin are local model parameters that strike a balance between the loss incurred on local datasets and the total variation. This lecture applies the gradient-based methods from Lecture 4 to solve GTVMin. The resulting FL algorithms can be implemented by message passing over the edges of the empirical graph. We will also use the analysis of gradient-based methods to study the computational aspects and statistical aspects of the resulting algorithms.

### 5.1 Learning Goals

After this lecture, you should

- be able to derive the gradient for GTVMin with local linear models.
- be able to implement the gradient step for GTVMin as message passing

### 5.2 Gradient Step for GTVMin

Consider a collection of  $n$  local datasets represented by the nodes  $\mathcal{V} = \{1, \dots, n\}$  of an empirical graph  $\mathcal{G} = (\mathcal{V}, \mathcal{E})$ . Each undirected edge  $\{i, i'\} \in \mathcal{E}$  in empirical graph  $\mathcal{G}$  has a known edge weight  $A_{i,i'}$ . We want to learn local model parameters  $\mathbf{w}^{(i)}$  of a personalized linear model for each node

$i = 1, \dots, n$ . To this end, we solve the GTVMin instance

$$\{\widehat{\mathbf{w}}^{(i)}\}_{i=1}^n \in \underset{\{\mathbf{w}^{(i)}\}}{\operatorname{argmin}} \underbrace{\sum_{i \in \mathcal{V}} (1/m_i) \|\mathbf{y}^{(i)} - \mathbf{X}^{(i)} \mathbf{w}^{(i)}\|_2^2 + \lambda \sum_{i, i' \in \mathcal{V}} A_{i, i'} \|\mathbf{w}^{(i)} - \mathbf{w}^{(i')}\|_2^2}_{=: f(\mathbf{w})}. \quad (5.1)$$

As discussed in Lecture 3, the objective function in (5.1) - viewed as a function of the stacked local model parameters  $\mathbf{w} := \operatorname{stack}\{\mathbf{w}^{(i)}\}_{i=1}^n$  - is a quadratic function of the form (4.1). In particular,

$$f(\mathbf{w}) = \mathbf{w}^T \left( \begin{pmatrix} \mathbf{Q}^{(1)} & 0 & \dots & 0 \\ 0 & \mathbf{Q}^{(2)} & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & \mathbf{Q}^{(n)} \end{pmatrix} + \lambda \mathbf{L} \otimes \mathbf{I} \right) \mathbf{w} + ((\mathbf{q}^{(1)})^T, \dots, (\mathbf{q}^{(n)})^T) \mathbf{w} \quad (5.2)$$

with  $\mathbf{Q}^{(i)} = (1/m_i) (\mathbf{X}^{(i)})^T \mathbf{X}^{(i)}$ , and  $\mathbf{q}^{(i)} := (-2/m_i) (\mathbf{X}^{(i)})^T \mathbf{y}^{(i)}$ .

Consider the gradient step

$$\mathbf{w}^{(r+1)} := \mathbf{w}^{(r)} - \alpha \nabla f(\mathbf{w}^{(r)}). \quad (5.3)$$

The iterate  $\mathbf{w}^{(r)}$  contains local model parameters  $\mathbf{w}^{(i,r)}$ ,

$$\mathbf{w}^{(r)} =: \operatorname{stack}\{\mathbf{w}^{(i,r)}\}_{i=1}^n. \quad (5.4)$$

We can express the gradient  $\nabla f(\mathbf{w}^{(r)})$  and the corresponding gradient step

directly in terms of  $\mathbf{w}^{(i,r)}$ ,

$$\begin{aligned} \mathbf{w}^{(i,r+1)} := & \mathbf{w}^{(i,r)} + \underbrace{(2\alpha/m_i)(\mathbf{X}^{(i)})^T(\mathbf{y}^{(i)} - \mathbf{X}^{(i)}\mathbf{w}^{(i,r)})}_{\text{(I)}} \\ & + \underbrace{2\lambda\alpha \sum_{i' \in \mathcal{V} \setminus \{i\}} A_{i,i'}(\mathbf{w}^{(i',r)} - \mathbf{w}^{(i,r)})}_{\text{(II)}}. \end{aligned} \quad (5.5)$$

The update (5.5) consists of two components, denoted (I) and (II). The purpose of (I) is to minimize the local loss. The purpose of (II) is to force the local model parameters to be similar across an edge  $\{i, i'\}$  with large weight  $A_{i,i'}$ .

### 5.3 Message Passing Implementation

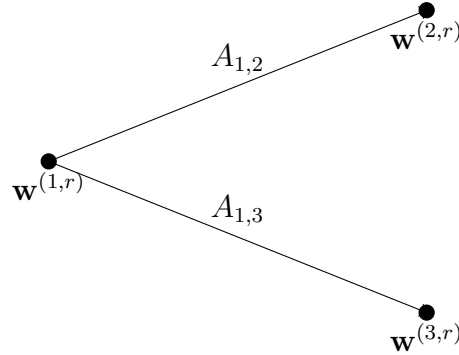


Figure 5.1: At the beginning of iteration  $r$ , node  $i = 1$  collects the current local model parameters  $\mathbf{w}^{(2,r)}$  and  $\mathbf{w}^{(3,r)}$ . Then, it computes the gradient step (5.5) to obtain the new local model parameters  $\mathbf{w}^{(1,r)}$ .

**5.4 FedSGD**

**5.5 FedAvg**

**5.6 Overview of Coding Assignment**



## 6 Lecture - “FL Main Flavours”

February 6, 2024

Lecture 3 discussed GTVMin as a main design principle for FL algorithms that have been obtained in Lecture 5 by applying some of the gradient-based methods from Lecture 4. This lecture discusses some important special cases of GTVMin that are obtained for specific choices for the underlying empirical graph.

### 6.1 Learning Goals

After this lecture, you should know about the following main flavours of FL:

- centralized FL
- clustered FL (generalization of clustering methods)
- horizontal FL (relation to semi-supervised learning)
- personalized FL/multi-task learning
- vertical FL

### 6.2 Centralized FL

### 6.3 Clustered FL

Many applications generate local datasets which do not carry sufficient statistical power to guide learning of model parameters  $\mathbf{w}^{(i)}$  (see Section ??). As a case in point, consider a local dataset  $\mathcal{D}^{(i)}$  of the form (3.1), with feature

vectors  $\mathbf{x}^{(r)} \in \mathbb{R}^d$  with  $m_i \ll d$ . We would like to learn the parameter vector  $\mathbf{w}^{(i)}$  of a linear hypothesis  $h(\mathbf{x}) = \mathbf{x}^T \mathbf{w}^{(i)}$ .

## **6.4 Horizontal FL**

## **6.5 Vertical FL**

## **6.6 Assignment**

## 7 Lecture - “Graph Learning”

Lecture 3 discussed GTVMin as a main design principle for FL algorithms. The computational and statistical properties of these algorithms crucially depend on the choice for the empirical graph. In some applications, domain expertise can guide the choice for the empirical graph. However, it might be useful to learn the empirical graph in a data-driven fashion. This lecture discusses some of these graph learning techniques.

### 7.1 Learning Goals

After this lecture, you should

- understand the role of empirical graphs as a crucial design choice for GTVMin-based methods (computational aspects, statistical aspects)
- know some quantitative measures for the similarity between local datasets
- be able to learn a graph form given pairwise similarities and structural constraints (e.g., bounded node degree)

### 7.2 Measuring (Dis-)Similarity Between Datasets

The above informal notion of similarity between local datasets. can be made precise via a probabilistic model. Here, we interpret the local dataset  $\mathcal{D}^{(i)}$  as realizations of RVs with some parametrized probability distribution  $p^{(i)}(\mathcal{D}^{(i)}; \mathbf{w}^{(i)})$ .

The discrepancy (or lack of similarity) between local datasets  $\mathcal{D}^{(i)}$  and  $\mathcal{D}^{(i')}$  could then be defined via the Euclidean distance

$$d^{(i,i')} := \left\| \mathbf{w}^{(i)} - \mathbf{w}^{(i')} \right\|_2,$$

between the parameters of the probability distributions.

If local datasets consist of a single numeric measurement  $y^{(i)}$ , we can use the discrepancy measure  $d^{(i,i')} := |y^{(i)} - y^{(i')}|$  [45].

### 7.3 Graph Learning Methods

Assume we have constructed a useful measure  $d^{(i,i')} \in \mathbb{R}_+$  for the discrepancy between local datasets  $\mathcal{D}^{(i)}, \mathcal{D}^{(i')}$ . We can then formulate the problem of learning the edge weights  $A_{i,i'} \in \mathbb{R}_+$  as the optimization problem

$$\min_{A_{i,i'}} A_{i,i'} d^{(i,i')}. \quad (7.1)$$

Unfortunately, the formulation (7.1) is not useful as it can be solved by the trivial choice  $A_{i,i'}$ . We therefore need to enforce the presence of some edges (with positive weight) by adding constraints to (7.1). For example, we might require

$$A_{i,i} = 0, \sum_{i' \neq i} A_{i,i'} = d_{\max} \text{ for all } i \in \mathcal{V}, A_{i,i'} \in [0, 1] \text{ for all } i, i' \in \mathcal{V}. \quad (7.2)$$

The constraints (7.2) require that each node  $i$  is connected with other nodes using total edge weight  $\sum_{i' \neq i} A_{i,i'} = d_{\max}$ . We can interpret the parameter  $d_{\max}$  as an effective node degree.

We combine the constraints (7.2) with (7.1) to obtain the following graph

learning principle,

$$\widehat{A}_{i,i'} \in \underset{A_{i,i'}}{\operatorname{argmin}} A_{i,i'} d^{(i,i')} \quad (7.3)$$

$$A_{i,i'} \in [0, 1] \text{ for all } i, i' \in \mathcal{V},$$

$$A_{i,i} = 0 \text{ for all } i \in \mathcal{V},$$

$$\sum_{i' \neq i} A_{i,i'} = d_{\max} \text{ for all } i \in \mathcal{V}.$$

## 7.4 Assignment

## 8 Lecture - “Trustworthy FL”

This lecture discusses some key requirements for trustworthy AI that have been put forward by the European Union. We will also see how these requirements might guide the design choices for GTVMin. Our focus will be on the four design criteria: robustness, privacy protection and explainability. This lecture discusses the robustness and explainability of basic linear regression that we encountered in Lecture 2. We will see that regularization techniques allow to navigate robustness-explainability-accuracy trade-offs.

### 8.1 Learning Goals

After this lecture, you should

- know some key requirements for trustworthy AI
- be familiar with quantitative measures of robustness and explainability
- have some intuition about how robustness, privacy and transparency guides design choices for local models, loss functions and empirical graph in GTVMin

We can use the upper bound (2.18) to study the effect of perturbing features and labels of data points.

## 9 Lecture - “Privacy-Protection in FL”

FL is inherently based on sharing information. Without any information sharing between the owners (or generators) of local datasets, FL is not possible.

### 9.1 Learning Goals

Afer this lecture, you should

- be aware of threats to privacy and the need to protect it,
- know some quantitative measures for privacy leakage,
- understand the effect of GTVMin design choices on user privacy,
- be able to implement FL algorithms with privacy guarantees.

### 9.2 Assignment

## 10 Lecture - “Data and Model Poisoning in FL”

This lecture discusses the robustness of FL systems against data poisoning which are a specific type of cyber attacks.

### 10.1 Learning Goals

After this lecture, you should

1. be aware of threats posed by data and model poisoning
2. understand how GTVMin design choices result in more or less safe FL algorithms

### 10.2 Data Poisoning

### 10.3 Model Poisoning

There is a trade-off between privacy protection and robustness against model poisoning attacks. From [46]: *Without secure aggregation, privacy is lost, but the aggregator may attempt to filter out “anomalous” contributions. Since the weights of a model created using*

### 10.4 Assignment



# Glossary

**activation function** Each artificial neuron within an ANN consists of an activation function that maps the inputs of the neuron to a single output value. In general, an activation function is a non-linear map of the weighted sum of neuron inputs (this weighted sum is the activation of the neuron). 13

**artificial intelligence** Artificial intelligence aims to develop systems that behave rational in the sense of maximizing a long-term reward. 8

**artificial neural network** An artificial neural network is a graphical (signal-flow) representation of a map from features of a data point at its input to a predicted label at its output. 1, 4, 5, 11–13, 16, 23

**baseline** A reference value or benchmark for the average loss incurred by a hypothesis when applied to the data points generated in a specific ML application. Such a reference value might be obtained from human performance (e.g., error rate of dermatologists diagnosing cancer from visual inspection of skin areas) or other ML methods (“competitors”) 10, 11

**Bayes estimator** A hypothesis  $h$  whose Bayes risk is minimal [30]. 1, 10

**Bayes risk** We use the term Bayes risk as a synonym for the risk or expected loss of a hypothesis. Some authors reserve the term Bayes risk for the risk of a hypothesis that achieves minimum risk, such a hypothesis being referred to as a Bayes estimator [30]. 1

**bias** Consider some unknown quantity  $\bar{w}$ , e.g., the true weight in a linear model  $y = \bar{w}x + e$  relating feature and label of a data point. We might use an ML method (e.g., based on ERM) to compute an estimate  $\hat{w}$  for the  $\bar{w}$  based on a set of data points that are realizations of RVs. The (squared) bias incurred by the estimate  $\hat{w}$  is typically defined as  $B^2 := (\mathbb{E}\{\hat{w}\} - \bar{w})^2$ . We extend this definition to vector-valued quantities using the squared Euclidean norm  $B^2 := \|\mathbb{E}\{\hat{\mathbf{w}}\} - \bar{\mathbf{w}}\|_2^2$ . 12

**classification** Classification is the task of determining a discrete-valued label  $y$  of a data point based solely on its features  $\mathbf{x}$ . The label  $y$  belongs to a finite set, such as  $y \in \{-1, 1\}$ , or  $y \in \{1, \dots, 19\}$  and represents a category to which the corresponding data point belongs to. 11

**computational aspects** By computational aspects of a ML method, we mainly refer to the computational resources required for its implementation. For example, if a ML method uses iterative optimization techniques to solve ERM, then its computational aspects include (i) how many arithmetic operations are needed to implement a single iteration (gradient step) and (ii) how many iterations are needed to obtain useful model parameters. One important example for an iterative optimization technique is GD. 1, 4, 7, 9, 13, 15

**connected graph** An undirected graph  $\mathcal{G} = (\mathcal{V}, \mathcal{E})$  is connected if we cannot find a (non-empty) subset  $\mathcal{V}' \subset \mathcal{V}$  with no edges leaving  $\mathcal{V}'$ . 5

**convex** A set  $\mathcal{C} \subseteq \mathbb{R}^d$  is convex if it contains the line segment between any two points of that set. We define a function as convex if its epigraph is a convex set [29]. 2–4, 7–9, 15, 18, 19, 24

**covariance matrix** The covariance matrix of a RV  $\mathbf{x} \in \mathbb{R}^d$  is defined as

$$\mathbb{E}\left\{(\mathbf{x} - \mathbb{E}\{\mathbf{x}\})(\mathbf{x} - \mathbb{E}\{\mathbf{x}\})^T\right\}. \quad 9, 14, 15$$

**data** A (indexed) set of data points. 1, 2, 4, 7, 13, 18

**data augmentation** Data augmentation methods add synthetic data points to an existing set of data points. These synthetic data points might be obtained by perturbations (adding noise) or transformations (rotations of images) of the original data points. 12, 14, 15

**data point** A data point is any object that conveys information [47]. Data points might be students, radio signals, trees, forests, images, RVs, real numbers or proteins. We characterize data points using two types of properties. One type of property is referred to as a feature. Features are properties of a data point that can be measured or computed in an automated fashion. Another type of property is referred to as labels. The label of a data point represents some higher-level fact (or quantity of interest). In contrast to features, determining the label of a data point typically requires human experts (domain experts). Roughly speaking, ML aims at predicting the label of a data point based solely on its features. 1–17, 20–24

**data poisoning** FL methods allow to leverage the information contained in local datasets generated by other parties to improve the training of a tailored model. Depending on how much we trust the other parties, FL can be compromised by data poisoning. Data poisoning refers to the intentional manipulation (or fabrication) of local datasets to steer the training of a specific local model [48, 49]. 2

**dataset** With a slight abuse of notation we use the terms “dataset“ or “set of data points” to refer to an indexed list of data points  $\mathbf{z}^{(1)}, \mathbf{z}^{(2)}, \dots$ . Thus, there is a first data point  $\mathbf{z}^{(1)}$ , a second data point  $\mathbf{z}^{(2)}$  and so on. Strictly speaking a dataset is a list and not a set [50]. By using indexed lists of data points we avoid some of the challenges arising in concept of an abstract set. 4, 6–10, 12–14, 16, 17

**decision region** Consider a hypothesis map  $h$  that delivers values from a finite set  $\mathcal{Y}$ . We refer to the set of features  $\mathbf{x} \in \mathcal{X}$  that result in the same output  $h(\mathbf{x}) = a$  as a decision region of the hypothesis  $h$ . 13

**decision tree** A decision tree is a flow-chart like representation of a hypothesis map  $h$ . More formally, a decision tree is a directed graph which reads in the feature vector  $\mathbf{x}$  of a data point at its root node. The root node then forwards the data point to one of its children nodes based on some elementary test on the features  $\mathbf{x}$ . If the receiving children node is not a leaf node, i.e., it has itself children nodes, it represents another test. Based on the test result, the data point is further pushed to one of its neighbours. This testing and forwarding of the data point is repeated until the data point ends up in a leaf node (having no children nodes). The leaf nodes represent sets (decision regions) constituted by feature vectors  $\mathbf{x}$  that are mapped to the same function value  $h(\mathbf{x})$ . 5, 11–13

**deep net** We refer to an ANN with a (relatively) large number of hidden layers as a deep ANN or “deep net”. Deep nets are used to represent the hypothesis spaces of deep learning methods [51]. 12

**differentiable** A function  $f : \mathbb{R}^d \rightarrow \mathbb{R}$  is differentiable if it has a gradient

$\nabla f(\mathbf{x})$  everywhere (for every  $\mathbf{x} \in \mathbb{R}^d$ ) [6]. 3, 9, 13, 21

**discrepancy** Consider a FL application with networked data represented by an empirical graph. FL methods use a discrepancy measure to compare hypothesis maps from local models at nodes  $i, i'$  connected by an edge in the empirical graph. 2, 3

**edge weight** Each edge  $\{i, i'\}$  of an empirical graph is assigned a non-negative edge weight  $A_{i,i'} \geq 0$ . A zero weight  $A_{i,i'} = 0$  indicates the absence of an edge between nodes  $i, i' \in \mathcal{V}$ . 1–3, 6, 7, 11, 14

**effective dimension** The effective dimension  $d_{\text{eff}}(\mathcal{H})$  of an infinite hypothesis space  $\mathcal{H}$  is a measure of its size. Loosely speaking, the effective dimension is equal to the number of “independent” tunable parameters of the model. These parameters might be the coefficients used in a linear map or the weights and bias terms of an ANN. 11

**eigenvalue** We refer to a number  $\lambda \in \mathbb{R}$  as eigenvalue of a square matrix  $\mathbf{A} \in \mathbb{R}^{d \times d}$  if there is a non-zero vector  $\mathbf{x} \in \mathbb{R}^d \setminus \{\mathbf{0}\}$  such that  $\mathbf{A}\mathbf{x} = \lambda\mathbf{x}$ . 3–9, 13

**eigenvalue decomposition** The eigenvalue decomposition for a square matrix  $\mathbf{A} \in \mathbb{R}^{d \times d}$  is a factorization of the form

$$\mathbf{A} = \mathbf{V}\mathbf{\Lambda}\mathbf{V}^{-1}.$$

The columns of the matrix  $\mathbf{V} = (\mathbf{v}^{(1)}, \dots, \mathbf{v}^{(d)})$  are the eigenvectors of the matrix  $\mathbf{V}$ . The diagonal matrix  $\mathbf{\Lambda} = \text{diag}\{\lambda_1, \dots, \lambda_d\}$  contains the eigenvalues  $\lambda_j$  corresponding to the eigenvectors  $\mathbf{v}^{(j)}$ . Note that the above decomposition exists only if the matrix  $\mathbf{A}$  is diagonalizable. 4, 8

**eigenvector** An eigenvector of a matrix  $\mathbf{A}$  is a non-zero vector  $\mathbf{x} \in \mathbb{R}^d \setminus \{\mathbf{0}\}$  such that  $\mathbf{Ax} = \lambda\mathbf{x}$  with some eigenvalue  $\lambda$ . 3–5

**empirical graph** Empirical graphs represent collections of local datasets and corresponding local models [52]. An empirical graph is an undirected weighted empirical graph whose nodes carry local datasets and models. FL methods learn a local hypothesis  $h^{(i)}$ , for each node  $i \in \mathcal{V}$ , such that it incurs small loss on the local datasets. 1–14, 23

**empirical risk** The empirical risk of a given hypothesis on a given set of data points is the average loss of the hypothesis computed over all data points in that set. 2, 6, 12, 16, 23

**empirical risk minimization** Empirical risk minimization is the optimization problem of finding the hypothesis with minimum average loss (or empirical risk) on a given set of data points (the training set). Many ML methods are special cases of empirical risk. 1–4, 6–8, 10–14, 16, 20, 23, 24

**estimation error** Consider data points with feature vectors  $\mathbf{x}$  and label  $y$ . In some applications we can model the relation between features and label of a data point as  $y = \bar{h}(\mathbf{x}) + \varepsilon$ . Here we used some true hypothesis  $\bar{h}$  and a noise term  $\varepsilon$  which might represent modelling or labelling errors. The estimation error incurred by a ML method that learns a hypothesis  $\hat{h}$ , e.g., using ERM, is defined as  $\hat{h} - \bar{h}$ . For a parametrized hypothesis space, consisting of hypothesis maps that are determined by a parameter vector  $\mathbf{w}$ , we define the estimation error in terms of parameter vectors as  $\Delta\mathbf{w} = \hat{\mathbf{w}} - \bar{\mathbf{w}}$ . first 7, 9

**Euclidean space** The Euclidean space  $\mathbb{R}^d$  of dimension  $d$  refers to the space of all vectors  $\mathbf{x} = (x_1, \dots, x_d)$ , with real-valued entries  $x_1, \dots, x_d \in \mathbb{R}$ , whose geometry is defined by the inner product  $\mathbf{x}^T \mathbf{x}' = \sum_{j=1}^d x_j x'_j$  between any two vectors  $\mathbf{x}, \mathbf{x}' \in \mathbb{R}^d$  [6]. 3, 8, 19

**feature** A feature of a data point is one of its properties that can be measured or computed in an automated fashion. For example, if a data point is a bitmap image, then we could use the red-green-blue intensities of its pixels as features. Some widely used synonyms for the term feature are “covariate”, “explanatory variable”, “independent variable”, “input (variable)”, “predictor (variable)” or “regressor” [53–55]. However, this book makes consequent use of the term features for low-level properties of data points that can be measured easily. 1–3, 5–17, 20–22

**feature map** A map that transforms the original features of a data point into new features. The so-obtained new features might be preferable over the original features for several reasons. For example, the shape of datasets might become simpler in the new feature space, allowing to use linear models in the new features. Another reason could be that the number of new features is much smaller which is preferable in terms of avoiding overfitting. The special case of feature maps that deliver two numeric features are particularly useful for data visualization. Indeed, we can then depict data points in a scatterplot by using these two features as the coordinates of a data point. 13

**feature matrix** Consider a dataset  $\mathcal{D}$  of  $m$  data points that are characterized by feature vectors  $\mathbf{x}^{(1)}, \dots, \mathbf{x}^{(m)}$ . It is convenient to collect these feature

vectors into a feature matrix  $\mathbf{X} := (\mathbf{x}^{(1)}, \dots, \mathbf{x}^{(m)})$ . 2, 8, 11

**feature space** The feature space of a given ML application or method is constituted by all potential values that the feature vector of a data point can take on. Within this book the most frequently used choice for the feature space is the Euclidean space  $\mathbb{R}^d$  with dimension  $d$  being the number of individual features of a data point. 10, 13

**federated learning (FL)** Federated learning is an umbrella term for ML methods that train models in a collaborative fashion using decentralized data and computation. 1–11, 17

**Finnish Meteorological Institute** The Finnish Meteorological Institute is a government agency responsible for gathering and reporting weather data in Finland. 2, 7, 12–14, 16

**General Data Protection Regulation** The General Data Protection Regulation (GDPR) is a law that has been passed by the European Union (EU) and put into effect on May 25, 2018 <https://gdpr.eu/tag/gdpr/>. The GDPR imposes obligations onto organizations anywhere, so long as they target, collect or in any other way process data related to people (i.e., personal data) in the EU. 5

**generalized total variation** Generalized total variation measures the changes of vector-valued node attributes of a graph. 7, 9

**gradient** For a real-valued function  $f : \mathbb{R}^d \rightarrow \mathbb{R} : \mathbf{w} \mapsto f(\mathbf{w})$ , a vector  $\mathbf{g}$  such that  $\lim_{\mathbf{w} \rightarrow \mathbf{w}'} \frac{f(\mathbf{w}) - (f(\mathbf{w}') + \mathbf{g}^T(\mathbf{w} - \mathbf{w}'))}{\|\mathbf{w} - \mathbf{w}'\|} = 0$  is referred to as the gradient of



$f$  at  $\mathbf{w}'$ . If such a vector exists it is denoted  $\nabla f(\mathbf{w}')$  or  $\nabla f(\mathbf{w})|_{\mathbf{w}'}$  [6].  
1–4, 9, 13, 21, 25

**gradient descent (GD)** Gradient descent is an iterative method for finding the minimum of a differentiable function  $f(\mathbf{w})$ . 1, 2, 4, 5, 7, 11–13, 18

**gradient step** Given a differentiable real-valued function  $f(\mathbf{w})$  and a vector  $\mathbf{w}'$ , the gradient step updates  $\mathbf{w}'$  by adding the scaled negative gradient  $\nabla f(\mathbf{w}')$ ,  $\mathbf{w}' \mapsto \mathbf{w}' - \alpha \nabla f(\mathbf{w}')$ . 1–12, 18

**gradient-based method** Gradient-based methods are iterative algorithms for finding the minimum (or maximum) of a differentiable objective function of the model parameters. These algorithms construct a sequence of approximations to an optimal choice for model parameters that results in a minimum objective function value. As their name indicates, gradient-based methods use the gradients of the objective function evaluated during previous iterations to construct new (hopefully) improved model parameters. 1–6, 8–11, 22

**graph** A graph  $\mathcal{G} = (\mathcal{V}, \mathcal{E})$  is a pair that consists of a node set  $\mathcal{V}$  and an edge set  $\mathcal{E}$ . In general, a graph is specified by a map that assigns to each edge  $e \in \mathcal{E}$  a pair of nodes [56]. One important family of graphs (simple undirected graphs) is obtained by identifying each edge  $e \in \mathcal{E}$  with two different nodes  $\{i, i'\}$ . Weighted graphs also specify numeric weights  $A_e$  for each edge  $e \in \mathcal{E}$ . 6, 7

**GTV minimization** GTV minimization is an instance of RERM using the GTV of local model parameters as a regularizer. 1, 2, 6–12

**hypothesis** A map (or function)  $h : \mathcal{X} \rightarrow \mathcal{Y}$  from the feature space  $\mathcal{X}$  to the label space  $\mathcal{Y}$ . Given a data point with features  $\mathbf{x}$  we use a hypothesis map  $h$  to estimate (or approximate) the label  $y$  using the predicted label  $\hat{y} = h(\mathbf{x})$ . ML is about learning (or finding) a hypothesis map  $h$  such that  $y \approx h(\mathbf{x})$  for any data point. 1–7, 9–17, 20–24

**hypothesis space** Every practical ML method uses a specific hypothesis space (or model)  $\mathcal{H}$ . The hypothesis space of a ML method is a subset of all possible maps from the feature space to label space. The design choice of the hypothesis space should take into account available computational resources and statistical aspects. If the computational infrastructure allows for efficient matrix operations, and there is a (approximately) linear relation between features and label, a useful choice for the hypothesis space might be the linear model. 1, 4, 5, 11–16, 20, 23, 24

**i.i.d.** It can be useful to interpret data points  $\mathbf{z}^{(1)}, \dots, \mathbf{z}^{(m)}$  as realizations of independent and identically distributed RVs with a common probability distribution. If these RVs are continuous, their joint probability density function (pdf) is  $p(\mathbf{z}^{(1)}, \dots, \mathbf{z}^{(m)}) = \prod_{r=1}^m p(\mathbf{z}^{(r)})$  with  $p(\mathbf{z})$  being the common marginal pdf of the underlying RVs. 3, 6, 10–12, 14, 21

**i.i.d. assumption** The i.i.d. assumption interprets data points of a dataset as the realizations of i.i.d. RVs. 6, 13, 21

**interpretability** A ML method is interpretable for a specific user if she can well anticipate the predictions delivered by the method. The notion of

interpretability can be made precise using quantitative measures of the uncertainty about the predictions [57]. 13

**label** A higher level fact or quantity of interest associated with a data point. If a data point is an image, its label might be the fact that it shows a cat (or not). Some widely used synonyms for the term label are "response variable", "output variable" or "target" [53–55]. 1–3, 5–14, 16, 17, 20, 22, 23

**label space** Consider a ML application that involves data points characterized by features and labels. The label space is constituted by all potential values that the label of a data point can take on. Regression methods, aiming at predicting numeric labels, often use the label space  $\mathcal{Y} = \mathbb{R}$ . Binary classification methods use a label space that consists of two different elements, e.g.,  $\mathcal{Y} = \{-1, 1\}$ ,  $\mathcal{Y} = \{0, 1\}$  or  $\mathcal{Y} = \{\text{"cat image"}, \text{"no cat image"}\}$  10

**Laplacian matrix** The geometry or structure of a graph  $\mathcal{G}$  can be analyzed using the properties of special matrices that are associated with  $\mathcal{G}$ . One such matrix is the graph Laplacian matrix  $\mathbf{L}$  which is defined for an undirected and weighted graph (e.g., the empirical graph of networked data) [58, 59]. 1, 3–5, 14

**law of large numbers** The law of large numbers refers to the convergence of the average of an increasing (large) number of i.i.d. RVs to the mean (or expectation) of their common probability distribution. Different instances of the law of large numbers are obtained using different notions of convergence. 12

**learning rate** Consider an iterative method for finding or learning a good choice for a hypothesis. Such an iterative method repeats similar computational (update) steps that adjust or modify the current choice for the hypothesis to obtain an improved hypothesis. A prime example for such an iterative learning method is GD and its variants. We refer by learning rate to any parameter of an iterative learning method that controls the extent by which the current hypothesis might be modified or improved in each iteration. A prime example for such a parameter is the step size used in GD. Some authors use the term learning rate mostly as a synonym for the step size of (a variant of) GD 1–9, 11, 13, 22

**learning task** A learning tasks consists of a specific choice for a collection of data points (e.g., all images stored in a particular database), their features and labels. 3, 12

**least absolute shrinkage and selection operator (Lasso)** The least absolute shrinkage and selection operator (Lasso) is an instance of structural risk minimization (SRM) for learning the weights  $\mathbf{w}$  of a linear map  $h(\mathbf{x}) = \mathbf{w}^T \mathbf{x}$ . The Lasso minimizes the sum consisting of an average squared error loss (as in linear regression) and the scaled  $\ell_1$  norm of the weight vector  $\mathbf{w}$ . 20

**linear model** We use the term linear model in a very specific sense. In particular, a linear model is a hypothesis space which consists of all linear maps,

$$\mathcal{H}^{(d)} := \{h(\mathbf{x}) = \mathbf{w}^T \mathbf{x} : \mathbf{w} \in \mathbb{R}^d\}. \quad (10.1)$$

Note that (10.1) defines an entire family of hypothesis spaces, which is parametrized by the number  $d$  of features that are linearly combined to form the prediction  $h(\mathbf{x})$ . The design choice of  $d$  is guided by computational aspects (smaller  $d$  means less computation), statistical aspects (increasing  $d$  might reduce prediction error) and interpretability (a linear model using few carefully chosen features might be considered interpretable). 1–3, 6–13, 16, 17

**linear regression** Linear regression aims at learning a linear hypothesis map to predict a numeric label based on numeric features of a data point. The quality of a linear hypothesis map is measured using the average squared error loss incurred on a set of labeled data points (which we refer to as training set). 1–4, 7–9, 12, 14, 15

**local dataset** The concept of a local dataset is in-between the concept of a data point and a dataset. A local dataset consists of several individual data points which are characterized by features and labels. In contrast to a single dataset used in basic ML methods, a local dataset is also related to other local datasets via different notions of similarities. These similarities might arise from probabilistic models or communication infrastructure and are encoded in the edges of an empirical graph. 1–3, 5–8, 11–14, 17

**local model** Consider a collections of local datasets that are assigned to the nodes of an empirical graph. A local model  $\mathcal{H}^{(i)}$  is a hypothesis space that is assigned to a node  $i \in \mathcal{V}$ . Different nodes might be assigned different hypothesis spaces, i.e., in general  $\mathcal{H}^{(i)} \neq \mathcal{H}^{(i')}$  for different

nodes  $i, i' \in \mathcal{V}$ . 1–7, 10–14, 23

**loss** With a slight abuse of language, we use the term loss either for the loss function itself or for its value for a specific pair of a data point and a hypothesis. 1, 3, 6, 7, 9, 10, 12, 14–16, 20–24

**loss function** A loss function is a map

$$L : \mathcal{X} \times \mathcal{Y} \times \mathcal{H} \rightarrow \mathbb{R}_+ : ((\mathbf{x}, y), h) \mapsto L((\mathbf{x}, y), h)$$

which assigns a pair consisting of a data point, with features  $\mathbf{x}$  and label  $y$ , and a hypothesis  $h \in \mathcal{H}$  the non-negative real number  $L((\mathbf{x}, y), h)$ . The loss value  $L((\mathbf{x}, y), h)$  quantifies the discrepancy between the true label  $y$  and the predicted label  $h(\mathbf{x})$ . Smaller (closer to zero) values  $L((\mathbf{x}, y), h)$  mean a smaller discrepancy between predicted label and true label of a data point. Figure 10.1 depicts a loss function for a given data point, with features  $\mathbf{x}$  and label  $y$ , as a function of the hypothesis  $h \in \mathcal{H}$ . 1–3, 5, 7, 9, 13, 14, 21

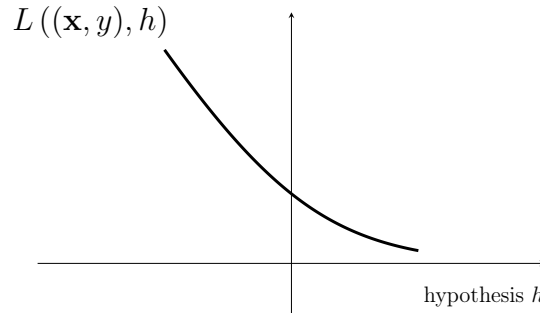


Figure 10.1: Some loss function  $L((\mathbf{x}, y), h)$  for a fixed data point, with feature vector  $\mathbf{x}$  and label  $y$ , and varying hypothesis  $h$ . ML methods try to find (learn) a hypothesis that incurs minimum loss.

**model** We use the term model as a synonym for hypothesis space 1, 3–7, 9–13, 16

**model parameters** Model parameters are numbers that select a hypothesis map out of a hypothesis space. 1, 2, 7, 9, 12–14, 18

**multivariate normal distribution** The multivariate normal distribution  $\mathcal{N}(\mathbf{m}, \mathbf{C})$  is an important family of probability distributions for a continuous RV  $\mathbf{x} \in \mathbb{R}^d$  [4, 60, 61]. This family is parametrized by the mean  $\mathbf{m}$  and covariance matrix  $\mathbf{C}$  of  $\mathbf{x}$ . If the covariance matrix is invertible, the probability distribution of  $\mathbf{x}$  is

$$p(\mathbf{x}) \propto \exp \left( - (1/2) (\mathbf{x} - \mathbf{m})^T \mathbf{C}^{-1} (\mathbf{x} - \mathbf{m}) \right).$$

9

**mutual information** The mutual information  $I(\mathbf{x}; y)$  between two RVs  $\mathbf{x}$ ,  $y$  defined on the same probability space is given by

$$I(\mathbf{x}; y) := \mathbb{E} \left\{ \log \frac{p(\mathbf{x}, y)}{p(\mathbf{x})p(y)} \right\}.$$

It is a measure for how well we can estimate  $y$  based solely from  $\mathbf{x}$ . A large value of  $I(\mathbf{x}; y)$  means that  $y$  can be well predicted solely from  $\mathbf{x}$ . The prediction could be obtained by a hypothesis learnt by a ML method. 17

**objective function** An objective function is a map that assigns each possible value of an optimization variable, such as the parameters  $\mathbf{w}$  of a hypothesis  $h^{(\mathbf{w})}$ , to an objective value  $f(\mathbf{w})$ . The objective value  $f(\mathbf{w})$

could be the risk or the empirical risk of a hypothesis  $h^{(\mathbf{w})}$ . 1, 2, 4–8, 10, 12–14, 24

**overfitting** Consider a ML method that uses ERM to learn a hypothesis with minimum empirical risk on a given training set. Such a method is “overfitting” the training set if it learns hypothesis with small empirical risk on the training set but unacceptably large loss outside the training set. 7, 11

**parameters** The parameters of a ML model are tunable (learnable or adjustable) quantities that allow to choose between different hypothesis maps. For example, the linear model  $\mathcal{H} := \{h : h(x) = w_1x + w_2\}$  consists of all hypothesis maps  $h(x) = w_1x + w_2$  with a particular choice for the parameters  $w_1, w_2$ . Another example of parameters are the weights assigned to the connections of an ANN. 1–7, 10–15, 23

**polynomial regression** Polynomial regression aims at learning a polynomial hypothesis map to predict a numeric label based on numeric features of a data point. For data points characterized by a single numeric features, polynomial regression uses the hypothesis space  $\mathcal{H}_d^{(\text{poly})} := \{h(x) = \sum_{j=0}^{d-1} x^j w_j\}$ . The quality of a polynomial hypothesis map is measured using the average squared error loss incurred on a set of labeled data points (which we refer to as training set). 12

**positive semi-definite** A symmetric matrix  $\mathbf{Q} = \mathbf{Q}^T \in \mathbb{R}^{d \times d}$  is referred to as positive semi-definite if  $\mathbf{x}^T \mathbf{Q} \mathbf{x} \geq 0$  for every vector  $\mathbf{x} \in \mathbb{R}^d$ . 2, 4, 6, 8, 13



**prediction** A prediction is an estimate or approximation for some quantity of interest. ML revolves around learning or finding a hypothesis map  $h$  that reads in the features  $\mathbf{x}$  of a data point and delivers a prediction  $\hat{y} := h(\mathbf{x})$  for its label  $y$ . 5, 6, 12, 13, 15, 21

**privacy leakage** Consider a (ML or FL) system that processes a local dataset  $\mathcal{D}^{(i)}$  and shares data, such as the predictions obtained for new data points, with other parties. Privacy leakage arises if the shared data carries information about a private (sensitive) feature of a data point (which might be a human) of  $\mathcal{D}^{(i)}$ . The amount of privacy leakage can be measured via mutual information using a probabilistic model for the local dataset. 17

**privacy protection** Privacy protection aims at avoiding (or minimizing) the privacy leakage occurring within data processing systems (such as ML or FL methods). 1

**probabilistic model** A probabilistic model interprets data points as realizations of RVs with a joint probability distribution. This joint probability distribution typically involves parameters which have to be manually chosen (=design choice) or learnt via statistical inference methods [30]. 1, 6–8, 10, 11, 13, 15, 17, 22

**probability density function (pdf)** The probability density function (pdf)  $p(x)$  of a real-valued RV  $x \in \mathbb{R}$  is a particular representation of its probability distribution. If the pdf exists, it can be used to compute the probability that  $x$  takes on a value from a (measurable) set  $\mathcal{B} \subseteq \mathbb{R}$  via  $p(x \in \mathcal{B}) = \int_{\mathcal{B}} p(x') dx'$  [4, Ch. 3]. The pdf of a vector-valued RV

$\mathbf{x} \in \mathbb{R}^d$  (if it exists) allows to compute the probability that  $\mathbf{x}$  falls into a (measurable) region  $\mathcal{R}$  via  $p(\mathbf{x} \in \mathcal{R}) = \int_{\mathcal{R}} p(\mathbf{x}') dx'_1 \dots dx'_d$  [4, Ch. 3]. 10

**probability distribution** The data generated in some ML applications can be reasonably well modelled as realizations of a RV. The overall statistical properties (or intrinsic structure) of such data are then governed by the probability distribution of this RV. We use the term probability distribution in a highly informal manner and mean the collection of probabilities assigned to different values or value ranges of a RV. The probability distribution of a binary RV  $y \in \{0, 1\}$  is fully specified by the probabilities  $p(y = 0)$  and  $p(y = 1) (= 1 - p(y = 0))$ . The probability distribution of a real-valued RV  $x \in \mathbb{R}$  might be specified by a probability density function  $p(x)$  such that  $p(x \in [a, b]) \approx p(a)|b - a|$ . In the most general case, a probability distribution is defined by a probability measure [60, 62]. 1, 2, 6, 9–12, 15, 17, 21, 22

**projected GD** Projected GD extends basic GD for unconstrained optimization to handle constraints on the optimization variable (model parameters). A single iteration of projected GD consists of first taking a gradient step and then projecting the result back into a constrain set. 1, 11, 12

**proximable** A Convex function for which the proximity operator can be computed efficiently are sometimes referred to as “proximable” or “simple” [34]. 9

**proximity operator** Given a convex function and a vector  $\mathbf{x}$ , we define its

proximity operator as

$$\mathbf{prox}_{L_i(\cdot), 2\lambda}(\mathbf{w}'') := \underset{\mathbf{w} \in \mathbb{R}^d}{\operatorname{argmin}} f(\mathbf{w}) + (\rho/2) \|\mathbf{w} - \mathbf{w}'\|_2^2 \text{ with } \rho > 0.$$

Convex functions for which the proximity operator can be computed efficiently are sometimes referred to as “proximable” or “simple” [34]. 9,

18

**quadratic function** A quadratic function  $f(\mathbf{w})$ , reading in a vector  $\mathbf{w} \in \mathbb{R}^d$  as its argument, is such that

$$f(\mathbf{w}) = \mathbf{w}^T \mathbf{Q} \mathbf{w} + \mathbf{q}^T \mathbf{w} + a,$$

with some matrix  $\mathbf{Q} \in \mathbb{R}^{d \times d}$ , vector  $\mathbf{q} \in \mathbb{R}^d$  and scalar  $a \in \mathbb{R}$ . 2, 4, 7–9,

15

**random variable (RV)** A random variable is a mapping from a probability space  $\mathcal{P}$  to a value space [62]. The probability space, whose elements are elementary events, is equipped with a probability measure that assigns a probability to subsets of  $\mathcal{P}$ . A binary random variable maps elementary events to a set containing two different values, e.g.,  $\{-1, 1\}$  or  $\{\text{cat}, \text{no cat}\}$ . A real-valued random variable maps elementary events to real numbers  $\mathbb{R}$ . A vector-valued random variable maps elementary events to the Euclidean space  $\mathbb{R}^d$ . Probability theory uses the concept of measurable spaces to rigorously define and study the properties of (large) collections of random variables [60, 62]. 1–3, 6, 9–12, 15, 17, 18, 20, 21, 24

**realization** Consider a RV  $x$  which maps each element (outcome, or elementary event)  $\omega \in \mathcal{P}$  of a probability space  $\mathcal{P}$  to an element  $a$  of a measurable space  $\mathcal{N}$  [6, 62, 63]. A realization of  $x$  is any element  $a' \in \mathcal{N}$  such that there is an element  $\omega' \in \mathcal{P}$  with  $x(\omega') = a'$ . 1, 6, 11, 12, 14, 17, 21

**regression** Regression problems revolve around the problem of predicting a numeric label solely from the features of a data point. 11

**regularization** Regularization techniques modify the ERM principle such that the learnt hypothesis performs well (generalizes) beyond the training set. One specific implementation of regularization is to add a penalty or regularization term to the objective function of ERM (which is the average loss on the training set). This regularization term can be interpreted as an estimate for the increase in the expected loss (risk) compared to the average loss on the training set. 1, 4, 7, 10, 11, 13, 14, 20, 21, 23

**regularized empirical risk minimization** Synonym for SRM. 7–9

**regularizer** A regularizer assigns each hypothesis  $h$  from a hypothesis space  $\mathcal{H}$  a quantitative measure  $\mathcal{R}\{h\}$  for how much its prediction error on a training set might differ from its prediction errors on data points outside the training set. Ridge regression uses the regularizer  $\mathcal{R}\{h\} := \|\mathbf{w}\|_2^2$  for linear hypothesis maps  $h^{(\mathbf{w})}(\mathbf{x}) := \mathbf{w}^T \mathbf{x}$  [5, Ch. 3]. The least absolute shrinkage and selection operator (Lasso) uses the regularizer  $\mathcal{R}\{h\} := \|\mathbf{w}\|_1$  for linear hypothesis maps  $h^{(\mathbf{w})}(\mathbf{x}) := \mathbf{w}^T \mathbf{x}$  [5, Ch. 3]. 7–9, 14

**ridge regression** Ridge regression learns the parameter (or weight) vector  $\mathbf{w}$  of a linear hypothesis map  $h^{(\mathbf{w})}(\mathbf{x}) = \mathbf{w}^T \mathbf{x}$ . The quality of a particular choice for the parameter vector  $\mathbf{w}$  is measured by the sum of two components. The first components is the average squared error loss incurred by  $h^{(\mathbf{w})}$  on a set of labeled data points (the training set). The second component is the scaled squared Euclidean norm  $\lambda \|\mathbf{w}\|_2^2$  with a regularization parameter  $\lambda > 0$ . It can be shown that the effect of adding to  $\lambda \|\mathbf{w}\|_2^2$  to the average squared error loss is equivalent to replacing the original data points by an ensemble of realizations of a RV centered around these data points. 2, 8, 12, 14–17, 20

**risk** Consider a hypothesis  $h$  that is used to predict the label  $y$  of a data point based on its features  $\mathbf{x}$ . We measure the quality of a particular prediction using a loss function  $L((\mathbf{x}, y), h)$ . If we interpret data points as the realizations of i.i.d. RVs, also the  $L((\mathbf{x}, y), h)$  becomes the realization of a RV. Using such an i.i.d. assumption allows to define the risk of a hypothesis as the expected loss  $\mathbb{E}\{L((\mathbf{x}, y), h)\}$ . Note that the risk of  $h$  depends on both, the specific choice for the loss function and the probability distribution of the data points. 1, 6, 10, 16, 20

**scatterplot** A visualization technique that depicts data points by markers in a two-dimensional plane. 7

**smooth** We refer to a real-valued function as smooth if it is differentiable and its gradient is continuous [44, 64]. In particular, a differentiable function  $f(\mathbf{w})$  is referred to as  $\beta$ -smooth if the gradient  $\nabla f(\mathbf{w})$  is Lipschitz

continuous with Lipschitz constant  $\beta$ , i.e.,

$$\|\nabla f(\mathbf{w}) - \nabla f(\mathbf{w}')\| \leq \beta \|\mathbf{w} - \mathbf{w}'\|.$$

1, 3, 5, 24

**squared error loss** The squared error loss measures the prediction error of a hypothesis  $h$  when predicting a numeric label  $y \in \mathbb{R}$  from the features  $\mathbf{x}$  of a data point. It is defined as

$$L((\mathbf{x}, y), h) := (y - \underbrace{h(\mathbf{x})}_{=\hat{y}})^2. \quad (10.2)$$

2, 3, 7, 13, 14, 16, 21

**statistical aspects** By statistical aspects of a ML method, we refer to (properties of) the probability distribution of its output given a probabilistic model for the data fed into the method. 1, 4, 7, 13, 15

**step size** Many ML methods use iterative optimization methods (such as gradient-based methods) to construct a sequence of increasingly accurate hypothesis maps  $h^{(1)}, h^{(2)}, \dots$ . The  $r$ th iteration of such an algorithm starts from the current hypothesis  $h^{(r)}$  and tries to modify it to obtain an improved hypothesis  $h^{(r+1)}$ . Iterative algorithms often use a step size (hyper-) parameter. The step size controls the amount by which a single iteration can change or modify the current hypothesis. Since the overall goal of such iteration ML methods is to learn a (approximately) optimal hypothesis we refer to a step size parameter also as a learning rate. 1

**stopping criterion** Many ML methods use iterative algorithms that construct a sequence of model parameters (such as the weights of a linear map or the weights of an ANN) that (hopefully) converge to an optimal choice for the model parameters. In practice, given finite computational resources, we need to stop iterating after a finite number of times. A stopping criterion is any well-defined condition required for stopping iterating. 1–3, 5, 6, 10, 11

**structural risk minimization** Structural risk minimization is the problem of finding the hypothesis that optimally balances the average loss (or empirical risk) on a training set with a regularization term. The regularization term penalizes a hypothesis that is not robust against (small) perturbations of the data points in the training set. 12, 20

**total variation** Consider some empirical graph whose nodes carry (personalized) local model parameters. The total variation measures the discrepancies between across edges  $\{i, i'\}$ . 1, 3, 5–7, 14

**training error** The average loss of a hypothesis when predicting the labels of data points in a training set. We sometimes refer by training error also the minimum average loss incurred on the training set by any hypothesis out of a hypothesis space. 1, 10–13, 16, 17, 23, 24

**training set** A set of data points that is used in ERM to learn a hypothesis  $\hat{h}$ . The average loss of  $\hat{h}$  on the training set is referred to as the training error. The comparison between training error and validation error of  $\hat{h}$  allows to diagnose ML methods and informs how to improve them (e.g.,

using a different hypothesis space or collecting more data points). 3–9, 11–16, 20, 21, 23, 24

**validation** Consider a hypothesis  $\hat{h}$  that has been learn via ERM on some training set  $\mathcal{D}$ . Validation refers to the practice of trying out a hypothesis  $\hat{h}$  on a validation set that consists of data points that are not contained in the training set  $\mathcal{D}$ . 1, 5, 6, 9

**validation error** Consider a hypothesis  $\hat{h}$  which is obtained by ERM on a training set. The average loss of  $\hat{h}$  on a validation set, which is different from the training set, is referred to as the validation error. 1, 10–13, 16, 17, 23, 24

**validation set** A set of data points that have not been used as training set in ERM to learn a hypothesis  $\hat{h}$ . The average loss of  $\hat{h}$  on the validation set is referred to as the validation error and used to diagnose the ML method (see [5, Sec. 6.6.]). The comparison between training error and validation error can inform directions for improvements of the ML method (such as using a different hypothesis space). 9, 12, 13, 16, 24

**variance** The variance of a real-valued RV  $x$  is defined as the expectation  $\mathbb{E}\{(x - \mathbb{E}\{x\})^2\}$  of the squared difference  $x$  and its expectation  $\mathbb{E}\{x\}$ . We extend this definition to vector-valued RVs  $\mathbf{x}$  as  $\mathbb{E}\{\|\mathbf{x} - \mathbb{E}\{\mathbf{x}\}\|_2^2\}$ . 12

**zero-gradient condition** Consider the unconstrained optimization problem  $\min_{\mathbf{w} \in \mathbb{R}^d} f(\mathbf{w})$  with a smooth and convex objective function  $f(\mathbf{w})$ . A



necessary and sufficient condition for a vector  $\hat{\mathbf{w}} \in \mathbb{R}^d$  to solve this problem is that the gradient  $\nabla f(\hat{\mathbf{w}})$  is the zero-vector,

$$\nabla f(\hat{\mathbf{w}}) = \mathbf{0} \Leftrightarrow f(\hat{\mathbf{w}}) = \min_{\mathbf{w} \in \mathbb{R}^d} f(\mathbf{w}).$$

10

## References

- [1] W. Rudin, *Real and Complex Analysis*, 3rd ed. New York: McGraw-Hill, 1987.
- [2] G. H. Golub and C. F. Van Loan, *Matrix Computations*, 3rd ed. Baltimore, MD: Johns Hopkins University Press, 1996.
- [3] G. Golub and C. van Loan, “An analysis of the total least squares problem,” *SIAM J. Numerical Analysis*, vol. 17, no. 6, pp. 883–893, Dec. 1980.
- [4] D. Bertsekas and J. Tsitsiklis, *Introduction to Probability*, 2nd ed. Athena Scientific, 2008.
- [5] A. Jung, *Machine Learning: The Basics*, 1st ed. Springer Singapore, Feb. 2022.
- [6] W. Rudin, *Principles of Mathematical Analysis*, 3rd ed. New York: McGraw-Hill, 1976.
- [7] M. Wollschlaeger, T. Sauter, and J. Jasperneite, “The future of industrial communication: Automation networks in the era of the internet of things and industry 4.0,” *IEEE Industrial Electronics Magazine*, vol. 11, no. 1, pp. 17–27, 2017.
- [8] M. Satyanarayanan, “The emergence of edge computing,” *Computer*, vol. 50, no. 1, pp. 30–39, Jan. 2017. [Online]. Available: <https://doi.org/10.1109/MC.2017.9>

- [9] H. Ates, A. Yetisen, F. Güder, and C. Dincer, “Wearable devices for the detection of covid-19,” *Nature Electronics*, vol. 4, no. 1, pp. 13–14, 2021. [Online]. Available: <https://doi.org/10.1038/s41928-020-00533-1>
- [10] H. Boyes, B. Hallaq, J. Cunningham, and T. Watson, “The industrial internet of things (iiot): An analysis framework,” *Computers in Industry*, vol. 101, pp. 1–12, 2018. [Online]. Available: <https://www.sciencedirect.com/science/article/pii/S0166361517307285>
- [11] S. Cui, A. Hero, Z.-Q. Luo, and J. Moura, Eds., *Big Data over Networks*. Cambridge Univ. Press, 2016.
- [12] A. Barabási, N. Gulbahce, and J. Loscalzo, “Network medicine: a network-based approach to human disease,” *Nature Reviews Genetics*, vol. 12, no. 56, 2011.
- [13] M. E. J. Newman, *Networks: An Introduction*. Oxford Univ. Press, 2010.
- [14] B. McMahan, E. Moore, D. Ramage, S. Hampson, and B. A. y Arcas, “Communication-efficient learning of deep networks from decentralized data,” in *Proceedings of the 20th International Conference on Artificial Intelligence and Statistics*, ser. Proceedings of Machine Learning Research, A. Singh and J. Zhu, Eds., vol. 54. Fort Lauderdale, FL, USA: PMLR, 20–22 Apr 2017, pp. 1273–1282. [Online]. Available: <http://proceedings.mlr.press/v54/mcmahan17a.html>

- [15] T. Li, A. K. Sahu, A. Talwalkar, and V. Smith, “Federated learning: Challenges, methods, and future directions,” *IEEE Signal Processing Magazine*, vol. 37, no. 3, pp. 50–60, May 2020.
- [16] Y. Cheng, Y. Liu, T. Chen, and Q. Yang, “Federated learning for privacy-preserving ai,” *Communications of the ACM*, vol. 63, no. 12, pp. 33–36, Dec. 2020.
- [17] N. Agarwal, A. Suresh, F. Yu, S. Kumar, and H. McMahan, “cpSGD: Communication-efficient and differentially-private distributed sgd,” in *Proc. Neural Inf. Proc. Syst. (NIPS)*, 2018.
- [18] V. Smith, C.-K. Chiang, M. Sanjabi, and A. Talwalkar, “Federated Multi-Task Learning,” in *Advances in Neural Information Processing Systems*, vol. 30, 2017. [Online]. Available: <https://proceedings.neurips.cc/paper/2017/file/6211080fa89981f66b1a0c9d55c61d0f-Paper.pdf>
- [19] J. You, J. Wu, X. Jin, and M. Chowdhury, “Ship compute or ship data? why not both?” in *18th USENIX Symposium on Networked Systems Design and Implementation (NSDI 21)*. USENIX Association, April 2021, pp. 633–651. [Online]. Available: <https://www.usenix.org/conference/nsdi21/presentation/you>
- [20] D. Tse and P. Viswanath, *Fundamentals of Wireless Communication*. Cambridge University Press, 2005.
- [21] T. Yang, G. Andrew, H. Eichner, H. Sun, W. Li, N. Kong, D. Ramage, and F. Beaufays, “Applied federated learning: Improving

- google keyboard query suggestions,” 2018. [Online]. Available: <https://arxiv.org/abs/1812.02903>
- [22] A. Ghosh, J. Chung, D. Yin, and K. Ramchandran, “An efficient framework for clustered federated learning,” in *34th Conference on Neural Information Processing Systems (NeurIPS 2020)*, Vancouver, Canada, 2020.
- [23] F. Sattler, K. Müller, and W. Samek, “Clustered federated learning: Model-agnostic distributed multitask optimization under privacy constraints,” *IEEE Transactions on Neural Networks and Learning Systems*, 2020.
- [24] G. Strang, *Computational Science and Engineering*. Wellesley-Cambridge Press, MA, 2007.
- [25] —, *Introduction to Linear Algebra*, 5th ed. Wellesley-Cambridge Press, MA, 2016.
- [26] H. H. Bauschke and P. L. Combettes, *Convex Analysis and Monotone Operator Theory in Hilbert Spaces*. New York: Springer, 2011.
- [27] F. Pedregosa, “Scikit-learn: Machine learning in python,” *Journal of Machine Learning Research*, vol. 12, no. 85, pp. 2825–2830, 2011. [Online]. Available: <http://jmlr.org/papers/v12/pedregosa11a.html>
- [28] J. Hirvonen and J. Suomela. (2023) Distributed algorithms 2020.
- [29] S. Boyd and L. Vandenberghe, *Convex Optimization*. Cambridge, UK: Cambridge Univ. Press, 2004.

- [30] E. L. Lehmann and G. Casella, *Theory of Point Estimation*, 2nd ed. New York: Springer, 1998.
- [31] A. Esteva, B. Kuprel, R. A. Novoa, J. Ko, S. M. Swetter, H. M. Blau, and S. Thrun, “Dermatologist-level classification of skin cancer with deep neural networks,” *Nature*, vol. 542, 2017.
- [32] H. Lütkepohl, *New Introduction to Multiple Time Series Analysis*. New York: Springer, 2005.
- [33] D. Spielman, “Spectral graph theory,” in *Combinatorial Scientific Computing*, U. Naumann and O. Schenk, Eds. Chapman and Hall/CRC, 2012.
- [34] L. Condat, “A primal–dual splitting method for convex optimization involving lipschitzian, proximable and linear composite terms,” *Journal of Opt. Th. and App.*, vol. 158, no. 2, pp. 460–479, Aug. 2013.
- [35] N. Parikh and S. Boyd, “Proximal algorithms,” *Foundations and Trends in Optimization*, vol. 1, no. 3, pp. 123–231, 2013.
- [36] R. Peng and D. A. Spielman, “An efficient parallel solver for SDD linear systems,” in *Proc. ACM Symposium on Theory of Computing*, New York, NY, 2014, pp. 333–342.
- [37] N. K. Vishnoi, “ $Lx = b$  — Laplacian solvers and their algorithmic applications,” *Foundations and Trends in Theoretical Computer Science*, vol. 8, no. 1–2, pp. 1–141, 2012. [Online]. Available: <http://dx.doi.org/10.1561/04000000054>

- [38] A. Jacot, F. Gabriel, and C. Hongler, “Neural tangent kernel: Convergence and generalization in neural networks,” in *Advances in Neural Information Processing Systems*, S. Bengio, H. Wallach, H. Larochelle, K. Grauman, N. Cesa-Bianchi, and R. Garnett, Eds., vol. 31. Curran Associates, Inc., 2018. [Online]. Available: [https://proceedings.neurips.cc/paper\\_files/paper/2018/file/5a4be1fa34e62bb8a6ec6b91d2462f5a-Paper.pdf](https://proceedings.neurips.cc/paper_files/paper/2018/file/5a4be1fa34e62bb8a6ec6b91d2462f5a-Paper.pdf)
- [39] S. S. Du, X. Zhai, B. Póczos, and A. Singh, “Gradient descent provably optimizes over-parameterized neural networks,” in *7th International Conference on Learning Representations, ICLR 2019, New Orleans, LA, USA, May 6-9, 2019*. OpenReview.net, 2019. [Online]. Available: <https://openreview.net/forum?id=S1eK3i09YQ>
- [40] W. E, C. Ma, and L. Wu, “A comparative analysis of optimization and generalization properties of two-layer neural network and random feature models under gradient descent dynamics,” *Science China Mathematics*, vol. 63, no. 7, pp. 1235–1258, 2020. [Online]. Available: <https://doi.org/10.1007/s11425-019-1628-5>
- [41] A. Paszke, S. Gross, F. Massa, A. Lerer, J. Bradbury, G. Chanan, T. Killeen, Z. Lin, N. Gimeshein, L. Antiga, A. Desmaison, A. Köpf, E. Yang, Z. DeVito, M. Raison, A. Tejani, S. Chilamkurthy, B. Steiner, L. Fang, J. Bai, and S. Chintala, *PyTorch: An Imperative Style, High-Performance Deep Learning Library*. Red Hook, NY, USA: Curran Associates Inc., 2019.

- [42] D. P. Bertsekas, *Convex Optimization Algorithms*. Athena Scientific, 2015.
- [43] Y. L. T. Schaul, X. Zhang, “No more pesky learning rates,” in *Proc. of the 30th International Conference on Machine Learning, PMLR 28(3)*, vol. 28, Atlanta, Georgia, June 2013, pp. 343–351.
- [44] Y. Nesterov, *Introductory lectures on convex optimization*, ser. Applied Optimization. Kluwer Academic Publishers, Boston, MA, 2004, vol. 87, a basic course. [Online]. Available: <http://dx.doi.org/10.1007/978-1-4419-8853-9>
- [45] S. Chepuri, S. Liu, G. Leus, and A. Hero, “Learning sparse graphs under smoothness prior,” in *Proc. of the IEEE Int. Conf. on Acoustics, Speech and Signal Processing*, 2017, pp. 6508–6512.
- [46] E. Bagdasaryan, A. Veit, Y. Hua, D. Estrin, and V. Shmatikov, “How to backdoor federated learning,” in *Proceedings of the Twenty Third International Conference on Artificial Intelligence and Statistics*, ser. Proceedings of Machine Learning Research, S. Chiappa and R. Calandra, Eds., vol. 108. PMLR, 26–28 Aug 2020, pp. 2938–2948. [Online]. Available: <https://proceedings.mlr.press/v108/bagdasaryan20a.html>
- [47] T. M. Cover and J. A. Thomas, *Elements of Information Theory*, 2nd ed. New Jersey: Wiley, 2006.
- [48] X. Liu, H. Li, G. Xu, Z. Chen, X. Huang, and R. Lu, “Privacy-enhanced federated learning against poisoning adversaries,” *IEEE Transactions on Information Forensics and Security*, vol. 16, pp. 4574–4588, 2021.



- [49] J. Zhang, B. Chen, X. Cheng, H. T. T. Binh, and S. Yu, “PoisonGAN: Generative poisoning attacks against federated learning in edge computing systems,” *IEEE Internet of Things Journal*, vol. 8, no. 5, pp. 3310–3322, 2021.
- [50] P. Halmos, *Naive set theory*. Springer-Verlag, 1974.
- [51] I. Goodfellow, Y. Bengio, and A. Courville, *Deep Learning*. MIT Press, 2016.
- [52] O. Chapelle, B. Schölkopf, and A. Zien, Eds., *Semi-Supervised Learning*. Cambridge, Massachusetts: The MIT Press, 2006.
- [53] D. Gujarati and D. Porter, *Basic Econometrics*. McGraw Hill, 2009.
- [54] Y. Dodge, *The Oxford Dictionary of Statistical Terms*. Oxford University Press, 2003.
- [55] B. Everitt, *Cambridge Dictionary of Statistics*. Cambridge University Press, 2002.
- [56] R. T. Rockafellar, *Network Flows and Monotropic Optimization*. Athena Scientific, Jul. 1998.
- [57] A. Jung and P. Nardelli, “An information-theoretic approach to personalized explainable machine learning,” *IEEE Sig. Proc. Lett.*, vol. 27, pp. 825–829, 2020.
- [58] U. von Luxburg, “A tutorial on spectral clustering,” *Statistics and Computing*, vol. 17, no. 4, pp. 395–416, Dec. 2007.

- [59] A. Y. Ng, M. I. Jordan, and Y. Weiss, “On spectral clustering: Analysis and an algorithm,” in *Adv. Neur. Inf. Proc. Syst.*, 2001.
- [60] R. Gray, *Probability, Random Processes, and Ergodic Properties*, 2nd ed. New York: Springer, 2009.
- [61] A. Lapidoth, *A Foundation in Digital Communication*. New York: Cambridge University Press, 2009.
- [62] P. Billingsley, *Probability and Measure*, 3rd ed. New York: Wiley, 1995.
- [63] P. R. Halmos, *Measure Theory*. New York: Springer, 1974.
- [64] S. Bubeck, “Convex optimization. algorithms and complexity.” in *Foundations and Trends in Machine Learning*. Now Publishers, 2015, vol. 8.