## Contents

**Part 1. Preliminaries**

Chapter 1. Introduction
- 1. A simple example: coin tossing 2
- 2. From estimation to prediction 3
- 3. Goals of learning 7

Chapter 2. Concentration inequalities
- 1. The basic tools 11
- 2. The Chernoff bounding trick and Hoeffding’s inequality 13
- 3. From bounded variables to bounded differences: McDiarmid’s inequality 16
- 4. McDiarmid’s inequality in action 18

**Part 2. Basic Theory**

Chapter 3. Formulation of the learning problem
- 1. The realizable case 24
- 2. Example: learning axis-parallel rectangles 28
- 3. Agnostic (or model-free) learning 32
- 4. Empirical risk minimization 35

Chapter 4. Empirical Risk Minimization: Abstract risk bounds and Rademacher averages
- 1. An abstract framework for ERM 40
- 2. Bounding the uniform deviation: Rademacher averages 42
- 3. Structural results for Rademacher averages 46

Chapter 5. Vapnik–Chervonenkis classes
- 1. Vapnik–Chervonenkis dimension: definition 50
- 2. Examples of Vapnik–Chervonenkis classes 52

Chapter 6. Binary classification
- 1. Learning linear discriminant rules 61
- 2. Risk bounds for combined classifiers via surrogate loss functions 63
- 3. Weighted linear combination of classifiers 66
- 4. Kernel machines 68
- 5. Convex risk minimization 77

Chapter 7. Regression with quadratic loss 80
1. ERM over a ball in RKHS  
2. Regularized least squares in an RKHS  

**Part 3. Some Applications**  

Chapter 8. Empirical vector quantization  
1. A brief introduction to source coding  
2. Fixed-rate vector quantization  
3. Learning an optimal quantizer  
4. Finite sample bound for empirically optimal quantizers  

Chapter 9. Dimensionality reduction in Hilbert spaces  
1. Examples  
2. Proof of Theorem 9.1  
3. Linear operators between Hilbert spaces  

Chapter 10. Stochastic simulation via Rademacher bootstrap  
1. Empirical Risk Minimization: a quick review  
2. Empirical Rademacher averages  
3. Sequential learning algorithms  
4. A sequential algorithm for stochastic simulation  
5. Technical lemma  

**Part 4. Advanced Topics**  

Chapter 11. Stability of learning algorithms  
1. An in-depth view of learning algorithms  
2. A primer on convex functions  
3. Learnability without uniform convergence  
4. Learnability and stability  
5. Stability of stochastic gradient descent  
6. Differentially private algorithms and generalization  
7. Technical lemmas  

Chapter 12. Minimax lower bounds  
1. Preparation: minimax lower bounds for statistical estimation  
2. Proof of Theorem 12.1  
3. Proof of Theorem 12.2  

Appendix A. Probability and random variables  

Bibliography
Part 1

Preliminaries
Introduction

1. A simple example: coin tossing

Let us start things off with a simple illustrative example. Suppose someone hands you a coin that has an unknown probability $\theta$ of coming up heads. You wish to determine this probability (coin bias) as accurately as possible by means of experimentation. Experimentation in this case amounts to repeatedly tossing the coin (this assumes, of course, that the bias of the coin on subsequent tosses does not change, but let’s say you have no reason to believe otherwise). Let us denote the two possible outcomes of a single toss by 1 (for heads) and 0 (for tails). Thus, if you toss the coin $n$ times, then you can record the outcomes as $X_1, \ldots, X_n$, where each $X_i \in \{0, 1\}$ and $P(X_i = 1) = \theta$ independently of all other $X_j$’s. More succinctly, we can write our sequence of outcomes as $X^n \in \{0, 1\}^n$, which is a random binary n-tuple. This is our sample.

What would be a reasonable estimate of $\theta$? Well, by the Law of Large Numbers we know that, in a long sequence of independent coin tosses, the relative frequency of heads will eventually approach the true coin bias with high probability. So, without further ado you go ahead and estimate $\theta$ by

$$\hat{\theta}_n(X^n) = \frac{1}{n} \sum_{i=1}^{n} X_i$$

(recall that each $X_i \in \{0, 1\}$, so the sum in the above expression simply counts the number of times the coin came up heads). The notation $\hat{\theta}_n(X^n)$ indicates the fact that the above estimate depends on the sample size $n$ and on the entire sample $X^n$.

How accurate can this estimator be? To answer this question, let us fix an accuracy parameter $\varepsilon \in [0, 1]$. Given $\theta$ and $n$, we can partition the entire set $\{0, 1\}^n$ into two disjoint sets:

$$G_{n,\varepsilon} := \left\{ x^n \in \{0, 1\}^n : |\hat{\theta}_n(x^n) - \theta| \leq \varepsilon \right\}$$

$$B_{n,\varepsilon} := \left\{ x^n \in \{0, 1\}^n : |\hat{\theta}_n(x^n) - \theta| > \varepsilon \right\} .$$

As the notation suggests, the $n$-tuples in $G_{n,\varepsilon}$ are the “good ones:” if our random sequence of tosses $X^n$ happens to land in $G_{n,\varepsilon}$, then our estimate $\hat{\theta}_n$ will differ from the true bias $\theta$ by at most $\varepsilon$ in either direction. On the other hand, if $X^n$ lands in $B_{n,\varepsilon}$, then we will have no such luck. Of course, since we do not know $\theta$, we have no way of telling whether $X^n$ is in $G_{n,\varepsilon}$ or in $B_{n,\varepsilon}$. The best we can do is to compute the probability of a “bad sample” for each possible value of $\theta$. This can be done using the so-called Chernoff bound [HR90]

$$P_\theta(B_{n,\varepsilon}) \equiv P_\theta \left( |\hat{\theta}_n(X^n) - \theta| > \varepsilon \right) \leq 2e^{-2n\varepsilon^2}$$

(1.1)
(soon you will see where this comes from). Here, \( P^\theta \) denotes the distribution of the random sample \( X^n \) when the probability of heads on each toss is \( \theta \). Now, Eq. (1.1) says two things: (1) For any desired accuracy \( \varepsilon \), probability of getting a bad sample decreases exponentially with sample size \( n \). (2) In order to guarantee that the probability of a bad sample is at most \( \delta \), you will need

\[
    n \geq \frac{1}{2\varepsilon^2} \log \left( \frac{2}{\delta} \right)
\]

coin tosses\(^1\). Thus, if you toss the coin at least this many times, then, no matter what \( \theta \) is, you can assert with confidence at least \( 1 - \delta \) that \( \theta \) is somewhere between \( \hat{\theta}_n - \varepsilon \) and \( \hat{\theta}_n + \varepsilon \). This leads to the following

**Observation 1.1.** For any true value \( \theta \) of the coin bias,

\[
    n(\varepsilon, \delta) := \left\lceil \frac{1}{2\varepsilon^2} \log \left( \frac{2}{\delta} \right) \right\rceil
\]

tosses suffice to guarantee with confidence \( 1 - \delta \) that the estimate \( \hat{\theta}_n \) has accuracy \( \varepsilon \).

In view of this observation, we can call the function \( (\varepsilon, \delta) \mapsto n(\varepsilon, \delta) \) the *sample complexity* of coin tossing.

This simple example illustrates the essence of statistical learning theory: We wish to learn something about a phenomenon of interest, and we do so by observing random samples of some quantity pertaining to the phenomenon. There are two basic questions we can ask:

1. How large of a sample do we need to achieve a given accuracy with a given confidence?
2. How efficient can our learning algorithm be?

Statistical learning theory [Vap98, Vid03] primarily concerns itself with the first of these questions, while the second question is within the purview of computational learning theory [Val84, KV94]. However, there are some overlaps between these two fields. In particular, we can immediately classify learning problems into “easy” and “hard” ones by looking at how their sample complexity grows as a function of \( 1/\varepsilon \) and \( 1/\delta \). In general, an easy problem is one whose sample complexity is polynomial in \( 1/\varepsilon \) and *polylogarithmic* in \( 1/\delta \) (“polylogarithmic” means polynomial in \( \log(1/\delta) \)). Of course, there are other factors that affect the sample complexity, and we will pay close attention to those as well.

### 2. From estimation to prediction

The coin tossing example of Section 1 was concerned with estimation. In fact, estimation was the focus of classical statistics, with early works dating back to Gauss, Laplace and the numerous members of the Bernoulli clan (the book by Stigler [Sti86] is an excellent survey of the history of statistics, full of amusing anecdotes and trivia, and much historical and scientific detail besides). By contrast, much of statistical learning theory (and much of modern statistics too) focuses on prediction (see the book by Clarke, Fokoué and Zhang [CFZ09] for a comprehensive exposition of the predictive view of statistical machine learning and data mining). In a typical prediction problem, we have two jointly distributed random

\(^1\)Unless stated otherwise, \( \log \) will always denote natural logarithms (base \( e \)).
variables\(^2\) \(X\) and \(Y\), where only \(X\) is available for observation, and we wish to devise a means of predicting \(Y\) on the basis of this observation. Thus, a predictor is any well-behaved\(^3\) function from \(X\) (the domain of \(X\)) into \(Y\) (the domain of \(Y\)). For example, in medical diagnosis, \(X\) might record the outcomes of a series of medical tests and other data for a single patient, while \(Y \in \{0, 1\}\) would correspond to the patient either having or not having a particular health issue.

The basic premise of statistical learning theory is that the details of the joint distribution \(P\) of \(X\) and \(Y\) are vague (or even completely unknown), and the only information we have to go on is a sequence of \(n\) independent observations \((X_1, Y_1), \ldots, (X_n, Y_n)\) drawn from \(P\). Assuming we have a quantitative criterion by which to judge a predictor’s accuracy, the same basic question presents itself: How large does the sample \(\{(X_i, Y_i)\}_{i=1}^n\) have to be in order for us to be able to construct a predictor achieving a given level of accuracy and confidence?

Of course, not all learning problems involve prediction. For example, problems like clustering, density estimation, feature (or representation) learning do not. We will see later that the mathematical formalism of statistical learning theory is flexible enough to cover such problems as well. For now, though, let us focus on prediction to keep things concrete. To get a handle on the learning problem, let us first examine the ideal situation, in which the distribution \(P\) is known.

### 2.1. Binary classification

The simplest prediction problem is that of binary classification (also known as pattern classification or pattern recognition) [DGL96]. In a typical scenario, \(X\) is a subset of \(\mathbb{R}^p\), the \(p\)-dimensional Euclidean space, and \(Y = \{0, 1\}\). A predictor (or a classifier) is any mapping \(f : X \to \{0, 1\}\). A standard way of evaluating the quality of binary classifiers is by looking at their probability of classification error. Thus, for a classifier \(f\) we define the classification loss (or risk)

\[
L_P(f) := \mathbb{P}(f(X) \neq Y) \equiv \int_{X \times \{0, 1\}} 1\{f(x) \neq y\} P(dx, dy),
\]

where \(1\{\cdot\}\) is the indicator function taking the value 1 if the statement in the braces is true, and 0 otherwise. What is the best classifier for a given \(P\)? The answer is given by the following

**Proposition 1.1.** Given the joint distribution \(P\) on \(X \times \{0, 1\}\), let \(\eta(x) := \mathbb{E}[Y|X = x] \equiv \mathbb{P}(Y = 1|X = x)\). Then the classifier

\[
f_P^*(x) := \begin{cases} 1, & \text{if } \eta(x) \geq 1/2 \\ 0, & \text{otherwise} \end{cases}
\]  

(1.2)

minimizes the probability of classification error over all \(f : X \to \{0, 1\}\), i.e.,

\[
L_P(f_P^*) = \min_{f : X \to \{0, 1\}} L_P(f).
\]

---

\(^2\)Please consult Appendix A for basic definitions and notation pertaining to probability distributions and random variables.

\(^3\)In fancy language, “well-behaved” will typically mean “measurable” with respect to appropriate \(\sigma\)-fields defined on \(X\) and \(Y\). We will ignore measurability issues in this course.
Remark 1.1. Some terminology: The function $\eta$ defined above is called the \textit{regression function}, the classifier in (1.2) is called the \textit{Bayes classifier}, and its risk
\[ L^*_P := L_P(f^*_P) \]
is called the \textit{Bayes rate}.

Proof. Consider an arbitrary classifier $f : X \to \{0,1\}$. Then
\[
L_P(f) = \int_{X \times \{0,1\}} 1_{\{f(x)\neq y\}} P(dx,dy) \\
= \int_X P_X(dx) \left\{ P_{Y|X}(1|x)1_{\{f(x)\neq 1\}} + P_{Y|X}(0|x)1_{\{f(x)\neq 0\}} \right\} \\
= \int_X P_X(dx) \left\{ \eta(x)1_{\{f(x)\neq 1\}} + (1-\eta(x))1_{\{f(x)\neq 0\}} \right\},
\]
where we have used Eq. (2.1), the factorization $P = P_X \times P_{Y|X}$, and the definition of $\eta$. From the above, it is easy to see that, in order to minimize $L_P(f)$, it suffices to minimize the term $\ell(f,x)$ in (1.3) separately for each value of $x \in X$. If we let $f(x) = 1$, then $\ell(f,x) = 1 - \eta(x)$, while for $f(x) = 0$ we will have $\ell(f,x) = \eta(x)$. Clearly, we should set $f(x)$ to 1 or 0, depending on whether $1 - \eta(x) \leq \eta(x)$ or not. This yields the rule in (1.2). \hfill \square

2.2. Minimum mean squared error prediction. Another prototypical example of a prediction problem is \textit{minimum mean squared error (MMSE) prediction} [CZ07], where $X \subseteq \mathbb{R}^p$, $Y \subseteq \mathbb{R}$, and the admissible predictors are functions $f : X \to \mathbb{R}$. The quality of such a predictor $f$ is measured by the \textit{MMSE}
\[
L_P(f) := \mathbb{E}(f(X) - Y)^2 \equiv \int_{X \times Y} (f(x) - y)^2 P(dx,dy).
\]
The MMSE predictor is characterized by the following

Proposition 1.2. Given the joint distribution $P$ on $X \times Y$ with $X \subseteq \mathbb{R}^p$ and $Y \subseteq \mathbb{R}$, the \textit{regression function} $f_P^*(x) := \mathbb{E}[Y|X = x]$ is the MMSE predictor. Moreover, for any other predictor $f$ we have
\[
L_P(f) = \|f - f_P^*\|^2_{L^2(P_X)} + L_P^*,
\]
where for any function $g : X \to \mathbb{R}$
\[
\|g\|^2_{L^2(P_X)} := \int_X |g(x)|^2 P_X(dx) \equiv \mathbb{E}|g(X)|^2
\]
is the squared $L^2$ norm with respect to the marginal distribution $P_X$, and $L_P^* := L_P(f_P^*)$.

Proof. Consider an arbitrary predictor $f : X \to \mathbb{R}$. Then
\[
L_P(f) = \mathbb{E}(f(X) - Y)^2 \\
= \mathbb{E}(f(X) - f_P^*(X) + f_P^*(X) - Y)^2 \\
= \mathbb{E}(f(X) - f_P^*(X))^2 + 2\mathbb{E}[(f(X) - f_P^*(X))(f_P^*(X) - Y)] + \mathbb{E}(f_P^*(X) - Y)^2 \\
= \|f - f_P^*\|^2_{L^2(P_X)} + 2\mathbb{E}[(f(X) - f_P^*(X))(f_P^*(X) - Y)] + L_P^*.
\]
Let us analyze the second (cross) term. Using the law of iterated expectation, we have
\[
\mathbb{E}[(f(X) - f_P^*(X))(f_P^*(X) - Y)] = \mathbb{E}[\mathbb{E}[(f(X) - f_P^*(X))(f_P^*(X) - Y)|X]]
\]
\[
= \mathbb{E}[(f(X) - f_P^*(X))\mathbb{E}[(f_P^*(X) - Y)|X]]
\]
\[
= \mathbb{E}[(f(X) - f_P^*(X))(f_P^*(X) - \mathbb{E}[Y|X])]
\]
\[
= 0,
\]
where in the last step we used the definition \(f_P^*(x) := \mathbb{E}[Y|X = x]\). Thus,
\[
L_P(f) = \|f - f_P^*\|_{L^2(P_X)}^2 + L_P^* \geq L_P^*,
\]
where equality holds if and only if \(f = f_P^*\) (with \(P_X\)-probability one).

### 2.3. A general prediction problem.
In the general case, \(X\) and \(Y\) are arbitrary sets, admissible predictors are functions \(f : X \to Y\) (or, more generally, \(f : X \to U\) for some suitable prediction space \(U\)), and the quality of a predictor \(f\) on a pair \((x, y) \in X \times Y\) is judged in terms of some fixed loss function \(\ell : U \times Y \to \mathbb{R}\) by \(\ell(f(x), y)\), the loss incurred in predicting the true \(y\) by \(\hat{u} = f(x)\). The expected risk of \(f\) is then
\[
L_P(f) := \mathbb{E}[\ell(f(X), Y)] \equiv \int_{X \times Y} \ell(f(x), y) P(dx, dy).
\]

This set-up covers the two previous examples:

1. If \(X \subseteq \mathbb{R}^p\), \(Y = U = \{0, 1\}\), and \(\ell(u, y) := 1_{\{u \neq y\}}\), then we recover the binary classification problem.
2. If \(X \subseteq \mathbb{R}^p\), \(Y \subseteq \mathbb{R} = U\), and \(\ell(u, y) := (u - y)^2\), then we recover the MMSE prediction problem.

Given \(P\) and \(\ell\), we define the minimum risk
\[
(1.4) \quad L_P^* := \inf_{f:X \to U} \mathbb{E}[\ell(f(X), Y)],
\]
where we use inf instead of min since there may not be a minimizing \(f\) (when that happens, one typically picks some small \(\varepsilon > 0\) and seeks \(\varepsilon\)-minimizers, i.e., \(f_{\varepsilon}^* : X \to U\), such that
\[
(1.5) \quad L_P(f_{\varepsilon}^*) \leq L_P(f) + \varepsilon
\]
for all \(f : X \to U\)). We will just assume that a minimizer exists, but continue to use inf to keep things general.

Thus, an abstract prediction problem is characterized by three objects: a probability distribution \(P\) of \((X, Y) \in X \times Y\), a class of admissible predictors \(f : X \to U\), and a loss function \(\ell : U \times Y \to \mathbb{R}\). The solution to the prediction problem is any \(f_P^*\) that attains the infimum in (1.4) (or comes \(\varepsilon\)-close as in (1.5)). Once such a \(f_P^*\) is computed, we can use it to predict the output \(Y \in Y\) for any given input \(X \in X\) by \(\hat{Y} = f_P^*(X)\), where the interpretation is that the random couple \((X, Y) \sim P\) pertains to the phenomenon of interest, \(X\) corresponds to its observable aspects, and \(Y\) corresponds to some unobservable characteristic that we may want to ascertain.
3. Goals of learning

We will close our introduction to statistical learning theory by a rough sketch of the “goals of learning” in a random environment. Please keep in mind that this is not meant to be a definitive treatment, which will come later in the course.

So far we have discussed the “ideal” case when the distribution \( P \) of \((X, Y)\) is known. Statistical learning theory deals with the setting where our knowledge of \( P \) is only partial (or nonexistent), but we have access to a training sample \((X_1, Y_1), \ldots, (X_n, Y_n)\) of independent draws from \( P \). Formally, we say that the pairs \((X_i, Y_i), 1 \leq i \leq n\), are independent and identically distributed (i.i.d.) according to \( P \), and we often write this as

\[
(X_i, Y_i) \overset{\text{i.i.d.}}{\sim} P, \quad i = 1, \ldots, n.
\]

To keep the notation simple, let us denote by \( Z \) the product space \( X \times Y \) and let \( Z_i = (X_i, Y_i) \) for each \( i \). Our training sample is then \( Z^n = (Z_1, \ldots, Z_n) \in Z^n \). Roughly speaking, the goal of learning is to take \( Z^n \) as an input and to produce a candidate predictor \( \hat{f}_n : X \rightarrow \mathbb{U} \) as an output. Note that since \( Z^n \) is a random variable, so is \( \hat{f}_n \). A learning algorithm (or a learner) is a procedure that can do this for any sample size \( n \). Thus, a learning algorithm is a box for converting training samples into predictors.

Let’s suppose that we have some learning algorithm to play with. Given a sample \( Z^n \) of size \( n \), it outputs a candidate predictor \( \hat{f}_n \). How good is this predictor? Well, let’s suppose that someone (say, Nature) hands us a fresh independent sample \( Z = (X, Y) \) from the same distribution \( P \) that has generated the training sample \( Z^n \). Then we can test \( \hat{f}_n \) by applying it to \( X \) and seeing how close \( \hat{U} = \hat{f}_n(X) \) is to \( Y \) by computing the instantaneous loss \( \ell(\hat{U}, Y) \equiv \ell(\hat{f}_n(X), Y) \). The expectation of the instantaneous loss w.r.t. the (unknown) distribution \( P \),

\[
L_P(\hat{f}_n) \equiv \int_{X \times Y} \ell(\hat{f}_n(x), y) P(dx, dy),
\]

is called the generalization error of the learner at sample size \( n \). It is crucial to note that \( L_P(\hat{f}_n) \) is a random variable, since \( \hat{f}_n \) is a function of the random sample \( Z^n \). In fact, to be more precise, we should write the generalization error as the conditional expectation \( \mathbb{E}[\ell(\hat{f}_n(X), Y)|Z^n] \), but since \( Z = (X, Y) \) is assumed to be independent from \( Z^n \), we get

(1.6)

Now, we will say that our learner has done a good job when its generalization error is suitably small. But how small can it be? To answer this question (or at least to point towards a possible answer), we must first agree that learning without any initial assumptions is a futile task. For example, consider fitting a curve to a training sample \((X_1, Y_1), \ldots, (X_n, Y_n)\), where both the \( X_i \)’s and the \( Y_i \)’s are real numbers. A simple-minded approach would be to pick any curve that precisely agreed with the entire sample – in other words, to select some \( \hat{f}_n \), such that \( \hat{f}_n(X_i) = Y_i \) for all \( i = 1, \ldots, n \). But there is an uncountable infinity of such functions! Which one should we choose? The answer is, of course, there is no way to know, if only because we have no clue about \( P \)! We could pick a very smooth function, but it could very well happen that the optimal \( f^*_P \) tends to be smooth for some values of the input and rough for some others. Alternatively, we could choose a very wiggly and complicated curve, but then it might just be the case that \( f^*_P \) is really simple.
A way out of this dilemma is to introduce what is known in the artificial intelligence community as an *inductive bias*. We go about it by restricting the space of candidate predictors our learner is allowed to search over to some suitable family $\mathcal{H}$, which is typically called the *hypothesis space*. Thus, we stipulate that $\hat{f}_n \in \mathcal{H}$ for any sample $Z^n$. Given $P$, let us define the minimum risk over $\mathcal{H}$:

$$L^*_P(\mathcal{H}) := \inf_{f \in \mathcal{H}} L_P(f).$$

(1.7)

Clearly, $L^*_P(\mathcal{H}) \geq L^*_P$, since the latter involves minimization over a larger set. However, now, provided the hypothesis space $\mathcal{H}$ is “manageable,” we may actually hope to construct a learner that would guarantee that

$$L_P(\hat{f}_n) \approx L^*_P(\mathcal{H}) \text{ with high probability.}$$

(1.8)

Then, if we happen to be so lucky that $f^*_P$ is actually in $\mathcal{H}$, we will have attained the Holy Grail, but even if we are not so lucky, we may still be doing pretty well. To get a rough idea of what is involved, let us look at the *excess risk* of $\hat{f}_n$ relative to the best predictor $f^*_P$:

$$E_P(\hat{f}_n) := L_P(\hat{f}_n) - L^*_P = L_P(\hat{f}_n) - L^*_P(\mathcal{H}) + L^*_P(\mathcal{H}) - L^*_P.$$

(1.9)

If the learner is good in the sense of (1.8), then we will have

$$E_P(\hat{f}_n) \approx L^*_P(\mathcal{H}) - L^*_P \text{ with high probability,}$$

which, in some sense, is the next best thing to the Holy Grail, especially if we can choose $\mathcal{H}$ so well that we can guarantee that the difference $L^*_P(\mathcal{H}) - L^*_P$ is small for any possible choice of $P$.

Note the decomposition of the excess risk into two terms, denoted in (1.9) by $E_{\text{est}}$ and $E_{\text{approx}}$. The first term, $E_{\text{est}}$, depends on the learned predictor $\hat{f}_n$, as well as on the hypothesis class $\mathcal{H}$, and is referred to as the *estimation error* of the learner. The second term, $E_{\text{approx}}$, depends only on $\mathcal{H}$ and on $P$, and is referred to as the *approximation error* of the hypothesis space. Most of the effort in statistical learning theory goes into analyzing and bounding the estimation error for various choices of $\mathcal{H}$. Analysis of $E_{\text{approx}}$ is the natural domain of approximation theory. The overall performance of a given learning algorithm depends on the interplay between these two sources of error. The text by Cucker and Zhou [CZ07] does a wonderful job of treating both the estimation and the approximation aspects of learning algorithms.

### 3.1. Beyond prediction

As we had briefly pointed out earlier, not all learning problems involve prediction. Luckily, the mathematical formalism we have just introduced can be easily adapted to a more general view of learning. Consider a random object $Z$ taking values in some space $Z$ according to an unknown distribution $P$. Suppose that there is a very large class $\mathcal{F}$ of functions $f : Z \to \mathbb{R}$, and for each $f \in \mathcal{F}$ we can define its expected loss (or risk)

$$L_P(f) := \mathbb{E}[f(Z)] = \int_Z f(z)P(\text{dz}).$$

(1.10)
Suppose also that $F$ has the property that there exists at least one $f^*_P \in F$ that achieves
\[ L_P(f^*_P) = \inf_{f \in F} L_P(f). \]
\[ L \]
The class $F$ may even depend on $P$. Let’s see how we can describe some unsupervised learning problems in this way:

- **Density estimation.** Suppose that $Z \subseteq \mathbb{R}^d$ for some $d$, and that $P$ has a probability density function (pdf) $p$. We can construct a suitable class $F$ as follows: pick a nonnegative function $\ell : \mathbb{R} \times \mathbb{R} \to \mathbb{R}^+$, and let $F = \mathcal{F}_{P,\ell}$ consist of all functions of the form
\[ f_q(z) = \ell(p(z), q(z)), \]
as $q$ ranges over a suitable class of pdf’s $q$ on $\mathbb{R}^d$. Then
\[ L_P(f_q) = E_P[\ell(p(Z), q(Z))] = \int_{\mathbb{R}^d} p(z) \ell(p(z), q(z)) dz. \]

This is fairly general. For example, if we assume that $p > 0$ on $Z$, then we can let $\ell(u, u') = |\frac{u'}{u} - 1|^2$, in which case we recover the well-known $L^2$ criterion:
\[ L_P(f_q) = \int_{\mathbb{R}^d} p(z) \left| \frac{q(z)}{p(z)} - 1 \right|^2 dz = \|p - q\|_2^2. \]

Or we can let $\ell(u, u') = \log(u/u')$, which gives us the relative entropy (also known as the Kullback–Leibler divergence):
\[ L_P(f_q) = \int_{\mathbb{R}^d} p(z) \log \frac{p(z)}{q(z)} dz = D(p\|q). \]

- **Clustering.** In a basic form of the clustering problem, we seek a partition of the domain $Z$ of interest into a fixed number, say $k$, of disjoint clusters $C_1, \ldots, C_k$, such that all points $z$ that belong to the same cluster are somehow “similar.” For example, we may define a distance function $d : Z \times Z \to \mathbb{R}^+$ and represent each cluster $C_j$, $1 \leq j \leq k$, by a single “representative” $v_j \in Z$. A clustering $C$ is then described by $k$ pairs $\{(C_j, v_j)\}_{j=1}^k$, where $Z = \bigcup_{j=1}^k C_j$. Consider the class $F = \mathcal{F}_k$ of all functions of the form
\[ f_C(z) = \sum_{j=1}^k 1_{\{z \in C_j\}} d(z, v_j) \]
as $C$ runs over all clusterings $\{(C_j, v_j)\}_{j=1}^k$. We can then evaluate the quality of our clustering $C$ by looking at the expectation
\[ L_P(f_C) = E_P \left[ \sum_{j=1}^k 1_{\{Z \in C_j\}} d(Z, v_j) \right] \]

- **Feature learning.** Broadly speaking, feature learning refers to constructing a representation of the original input $Z$ that could be fed to a supervised learning algorithm further down the line. There could be multiple reasons for wanting to do this, ranging from computational considerations to a desire to capture “salient” characteristics of the data that could be relevant for prediction, while “factoring
out” the irrelevant parts. Mathematically, a feature is a mapping \( \varphi : Z \to \tilde{Z} \) into some other representation space \( \tilde{Z} \), so that each point \( z \in Z \) is represented \( \tilde{z} = \varphi(z) \), and it is this representation that will be used by another learning algorithm down the line. (Ideally, good feature representations should be agnostic with respect to the nature of the learning problem where they will be used.) One way to score the quality of a feature is to consider a loss function of the form \( \ell : Z \times \tilde{Z} \to \mathbb{R}^+ \), so that \( \ell(z, \tilde{z}) \) is small if \( z \) is well-represented by \( \tilde{z} \). Then, for a fixed collection \( \Phi \) of candidate feature maps, we could consider a class \( F = F_{\Phi, \ell} \) of functions of the form \( f_{\varphi}(z) = \ell(z, \varphi(z)), \quad \varphi \in \Phi \).

This is a very wide umbrella that can cover a wide variety of unsupervised learning tasks (e.g., clustering).

These examples show that unsupervised learning problems can also be formulated in terms of minimizing an appropriately defined expected loss. The only difference is that the loss function may sometimes depend on the underlying distribution, which is unknown. However, under suitable assumptions on the problem components, it is often possible to find an alternative hypothesis space \( \mathcal{H} \) which (unlike \( \mathcal{F} \)) does not depend on \( P \), such that the minimum expected loss \( L_P^*(\mathcal{F}) \) can be related to the minimum expected loss \( L_P^*(\mathcal{H}) \). Just as before, a learning algorithm is a rule for mapping an i.i.d. sample \( Z^n = (Z_1, \ldots, Z_n) \) from \( P \) to an element \( \hat{f}_n \in \mathcal{H} \). The objective is also the same as before: ensure that

\[
L_P(\hat{f}_n) \approx L_P^*(\mathcal{H}) \quad \text{with high probability.}
\]

Thus, we can treat supervised learning and unsupervised learning on the same footing.
In the previous chapter, the following result was stated without proof. If \(X_1, \ldots, X_n\) are independent Bernoulli(\(\theta\)) random variables representing the outcomes of a sequence of \(n\) tosses of a coin with bias (probability of heads) \(\theta\), then for any \(\varepsilon \in (0, 1)\)

\[
P \left( \left| \hat{\theta}_n - \theta \right| \geq \varepsilon \right) \leq 2e^{-2n\varepsilon^2} \tag{2.1}
\]

where

\[
\hat{\theta}_n = \frac{1}{n} \sum_{i=1}^{n} X_i
\]

is the fraction of heads in \(X^n = (X_1, \ldots, X_n)\). Since \(\theta = E\hat{\theta}_n\), (2.1) says that the sample (or empirical) average of the \(X_i\)'s concentrates sharply around the statistical average \(\theta = E X_1\). Bounds like these are fundamental in statistical learning theory. In this chapter, we will learn the techniques needed to derive such bounds for settings much more complicated than coin tossing. This is not meant to be a complete picture; a detailed treatment can be found in the excellent recent book by Boucheron, Lugosi, and Massart [BLM13].

1. The basic tools

We start with Markov’s inequality: Let \(X \in \mathbb{R}\) be a nonnegative random variable. Then for any \(t > 0\) we have

\[
P(X \geq t) \leq \frac{E X}{t}. \tag{2.2}
\]

The proof is simple:

\[
P(X \geq t) = E[1\{X \geq t\}]
\leq \frac{E[X 1\{X \geq t\}]}{t}
\leq \frac{E X}{t}, \tag{2.3, 2.4}
\]

where:

- (2.3) uses the fact that the probability of an event can be expressed as the expectation of its indicator function:
  \[P(X \in A) = \int_A P_X(dx) = \int_A 1\{x \in A\} P_X(dx) = E[1\{X \in A\}]\]

- (2.4) uses the fact that
  \[X \geq t > 0 \implies \frac{X}{t} \geq 1\]
(2.5) uses the fact that
\[ X \geq 0 \implies X \mathbf{1}_{\{X \geq t\}} \leq X, \]
so consequently \( \mathbb{E}[X \mathbf{1}_{\{X \geq t\}}] \leq \mathbb{E}X. \)

Markov’s inequality leads to our first bound on the probability that a random variable deviates from its expectation by more than a given amount: Chebyshev’s inequality. Let \( X \) be an arbitrary real random variable. Then for any \( t > 0 \)
\[ P(|X - \mathbb{E}X| \geq t) \leq \frac{\text{Var}[X]}{t^2}, \]
where \( \text{Var} X := \mathbb{E}[(X - \mathbb{E}X)^2] = \mathbb{E}X^2 - (\mathbb{E}X)^2 \) is the variance of \( X \). To prove (2.6), we apply Markov’s inequality (2.2) to the nonnegative random variable \( |X - \mathbb{E}X|^2 \):
\[ P(|X - \mathbb{E}X| \geq t) = P(|X - \mathbb{E}X|^2 \geq t^2) \leq \frac{\mathbb{E}|X - \mathbb{E}X|^2}{t^2}, \]
where the first step uses the fact that the function \( \phi(x) = x^2 \) is monotonically increasing on \([0, \infty)\), so that \( a \geq b \geq 0 \) if and only if \( a^2 \geq b^2 \).

Now let’s apply these tools to the problem of bounding the probability that, for a coin with bias \( \theta \), the fraction of heads in \( n \) trials differs from \( \theta \) by more than some \( \varepsilon > 0 \). To that end, let us represent the outcomes of the \( n \) tosses by \( n \) independent Bernoulli(\( \theta \)) random variables \( X_1, \ldots, X_n \in \{0, 1\} \), where \( P(X_i = 1) = \theta \) for all \( i \). Let
\[ \hat{\theta}_n = \frac{1}{n} \sum_{i=1}^{n} X_i. \]

Then
\[ \mathbb{E}\hat{\theta}_n = \mathbb{E} \left[ \frac{1}{n} \sum_{i=1}^{n} X_i \right] = \frac{1}{n} \sum_{i=1}^{n} \mathbb{E}X_i = \mathbb{E}X = \theta, \]
and
\[ \text{Var}[\hat{\theta}_n] = \text{Var} \left[ \frac{1}{n} \sum_{i=1}^{n} X_i \right] = \frac{1}{n^2} \sum_{i=1}^{n} \text{Var}[X_i] = \frac{\theta (1 - \theta)}{n}, \]
where we have used the fact that the \( X_i \)’s are i.i.d., so \( \text{Var}[X_1 + \ldots + X_n] = \sum_{i=1}^{n} \text{Var}[X_i] = n \text{Var} X_1 \). Now we are in a position to apply Chebyshev’s inequality:
\[ P \left( |\hat{\theta}_n - \theta| \geq \varepsilon \right) \leq \frac{\text{Var}[\hat{\theta}_n]}{\varepsilon^2} = \frac{\theta (1 - \theta)}{n \varepsilon^2}. \]

At the very least, (2.9) shows that the probability of getting a bad sample decreases with sample size. Unfortunately, it does not decrease fast enough. To see why, we can appeal to the Central Limit Theorem, which (roughly) states that
\[ P \left( \sqrt{\frac{n}{\theta (1 - \theta)}} (\hat{\theta}_n - \theta) \geq t \right) \xrightarrow{n \to \infty} 1 - \Phi(t) \leq \frac{1}{\sqrt{2\pi}} \frac{e^{-t^2/2}}{t}, \]
where \( \Phi(t) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{t} e^{-x^2/2} dx \) is the standard Gaussian CDF. This would suggest something like
\[
P(\hat{\theta}_n - \theta \geq \varepsilon) \approx \exp \left( -\frac{n\varepsilon^2}{2\theta(1-\theta)} \right),
\]
which decays with \( n \) much faster than the right-hand side of (2.9),

2. The Chernoff bounding trick and Hoeffding’s inequality

To fix (2.9), we will use a very powerful technique, known as the Chernoff bounding trick \([Che52]\). Let \( X \) be real-valued random variable. Suppose we are interested in bounding the probability \( P(X \geq \mathbb{E}X + t) \) for some particular \( t > 0 \). Observe that for any \( s > 0 \) we have
\[
P(X \geq \mathbb{E}X + t) = P\left( e^{s(X-\mathbb{E}X)} \geq e^{st} \right) \leq e^{-st} \mathbb{E}\left[ e^{s(X-\mathbb{E}X)} \right],
\]
where the first step is by monotonicity of the function \( \phi(x) = e^{sx} \) and the second step is by Markov’s inequality (2.2). The Chernoff trick is to choose an \( s > 0 \) that would make the right-hand side of (2.10) suitably small. In fact, since (2.10) holds simultaneously for all \( s > 0 \), the optimal thing to do is to take
\[
P(X \geq \mathbb{E}X + t) \leq \inf_{s>0} e^{-st} \mathbb{E}\left[ e^{s(X-\mathbb{E}X)} \right].
\]
However, often a good upper bound on the moment-generating function \( \mathbb{E}\left[ e^{s(X-\mathbb{E}X)} \right] \) is enough. One such bound was developed by Hoeffding \([Hoe63]\) for the case when \( X \) is bounded with probability one:

**Lemma 2.1 (Hoeffding).** Let \( X \) be a random variable, such that \( P(a \leq X \leq b) = 1 \) for some \( -\infty < a \leq b < \infty \). Then for all \( s > 0 \)
\[
\mathbb{E}\left[ e^{s(X-\mathbb{E}X)} \right] \leq e^{s^2(b-a)^2/8}.
\]

To prove the lemma, we first start with a useful bound on the variance of a bounded random variable:

**Lemma 2.2.** If \( U \) is a random variable such that \( P(a \leq U \leq b) \), then
\[
\text{Var}[U] \leq \frac{(b-a)^2}{4}.
\]

**Proof.** We use the fact that, for any real-valued random variable \( U \),
\[
\text{Var}[U] \leq \mathbb{E}[(U - c)^2], \quad \forall c \in \mathbb{R}.
\]
(In particular \( c = \mathbb{E}U \) achieves equality in the above bound.) Now let \( c = \frac{a+b}{2} \), the midpoint of the interval \([a, b]\). Then, since \( a \leq U \leq b \) almost surely, we know that
\[
|U - c| \leq \frac{b-a}{2}.
\]
Using this \( c \) in (2.13), we obtain \( \text{Var}[U] \leq \mathbb{E}[(U - c)^2] \leq \frac{(b-a)^2}{4} \), as claimed. \( \square \)
Remark 2.1. The bound of Lemma 2.2 is actually sharp: consider

\[
U = \begin{cases} 
  a, & \text{with prob. } \frac{1}{2} \\
  b, & \text{with prob. } \frac{1}{2}.
\end{cases}
\]

Then

\[
\text{Var}[U] = E[U^2] - (EU)^2 = \frac{a^2 + b^2}{2} - \left( \frac{a + b}{2} \right)^2 = \frac{(b - a)^2}{4}.
\]

Now we can prove Hoeffding’s lemma:

Proof (of Lemma 2.1). Without loss of generality, we may assume that \( EX = 0 \). Thus, we are interested in bounding \( E[e^{sX}] \). Let’s consider instead the logarithmic moment-generating function

\[
\psi(s) := \log E[e^{sX}].
\]

Then

\[
\psi'(s) = \frac{E[Xe^{sX}]}{E[e^{sX}]}, \quad \psi''(s) = \frac{E[X^2e^{sX}]}{E[e^{sX}]} - \left( \frac{E[Xe^{sX}]}{E[e^{sX}]} \right)^2.
\]

(2.14)

(we are being a bit loose here, assuming that we can interchange the order of differentiation and expectation, but in this case everything can be confirmed rigorously). Now consider another random variable \( U \) whose distribution is related to \( X \) by

\[
E[f(U)] = E[f(X)e^{sX}]
\]

(2.15)

for any real-valued function \( f : \mathbb{R} \to \mathbb{R} \). To convince ourselves that this is a legitimate construction, let’s plug in an indicator function of any event \( A \):

\[
P[U \in A] = E[1_{\{U \in A\}}] = \frac{E[1_{\{X \in A\}}e^{sX}]}{E[e^{sX}]}.
\]

(2.16)

It is then not hard to show that this is indeed a valid probability measure. This construction is known as the twisting (or tilting) technique or as exponential change of measure.

We note two things:

1. Using (2.16) with \( A = [a, b] \), we get

\[
P[a \leq U \leq b] = \frac{E[1_{\{a \leq X \leq b\}}e^{sX}]}{E[e^{sX}]} = 1,
\]

(2.17)

since \( a \leq X \leq b \). Moreover, if \( A \) is any event in the complement of \([a, b]\), then \( P[U \in A] = 0 \), since \( E[1_{\{X \in A\}}e^{sX}] = 0 \). That is, \( U \) is bounded between \( a \) and \( b \) with probability one, just like \( X \).  

2. Using (2.15) first with \( f(U) = U \) and then with \( f(U) = U^2 \), we get

\[
E[U] = \frac{E[Xe^{sX}]}{E[e^{sX}]}, \quad E[U^2] = \frac{E[X^2e^{sX}]}{E[e^{sX}]}.
\]

(2.18)
Comparing the expressions in (2.18) with (2.14), we observe that \( \psi''(s) = \text{Var}[U] \). Now, since \( a \leq U \leq B \), it follows from Lemma 2.2 that \( \psi''(s) \leq \frac{(b-a)^2}{4} \). Therefore,

\[
\psi(s) = \int_0^s \int_0^t \psi''(v) dv dt \leq \frac{s^2(b-a)^2}{8},
\]

where we have used the fact that \( \psi'(0) = \psi(0) = 0 \). Exponentiating both sides, we are done. \( \square \)

We will now use the Chernoff method and the above lemma to prove the following

**Theorem 2.1 (Hoeffding’s inequality)**. Let \( X_1, \ldots, X_n \) be independent random variables, such that \( X_i \in [a_i, b_i] \) with probability one. Let \( S_n := \sum_{i=1}^{n} X_i \). Then for any \( t > 0 \)

\[
\Pr(S_n - \mathbb{E}S_n \geq t) \leq \exp \left( -\frac{2t^2}{\sum_{i=1}^{n}(b_i - a_i)^2} \right) ; \tag{2.19}
\]

\[
\Pr(S_n - \mathbb{E}S_n \leq -t) \leq \exp \left( -\frac{2t^2}{\sum_{i=1}^{n}(b_i - a_i)^2} \right) . \tag{2.20}
\]

Consequently,

\[
\Pr(\left| S_n - \mathbb{E}S_n \right| \geq t) \leq 2 \exp \left( -\frac{2t^2}{\sum_{i=1}^{n}(b_i - a_i)^2} \right) . \tag{2.21}
\]

**Proof.** By replacing each \( X_i \) with \( X_i - \mathbb{E}X_i \), we may as well assume that \( \mathbb{E}X_i = 0 \). Then \( S_n = \sum_{i=1}^{n} X_i \). Using Chernoff’s trick, we write

\[
\Pr(S_n \geq t) = \Pr(e^{sS_n} \geq e^{st}) \leq e^{-st} \mathbb{E}[e^{sS_n}] . \tag{2.22}
\]

Since the \( X_i \)'s are independent,

\[
\mathbb{E}[e^{sS_n}] = \mathbb{E}[e^{s(X_1+\ldots+X_n)}] = \mathbb{E}\left[ \prod_{i=1}^{n} e^{sX_i} \right] = \prod_{i=1}^{n} \mathbb{E}[e^{sX_i}] . \tag{2.23}
\]

Since \( X_i \in [a_i, b_i] \), we can apply Lemma 2.1 to write \( \mathbb{E}[e^{sX_i}] \leq e^{s^2(b_i-a_i)^2/8} \). Substituting this into (2.23) and (2.22), we obtain

\[
\Pr(S_n \geq t) \leq e^{-st} \prod_{i=1}^{n} e^{s^2(b_i-a_i)^2/8}
\]

\[
= \exp \left( -st + \frac{s^2}{8} \sum_{i=1}^{n}(b_i - a_i)^2 \right)
\]

If we choose \( s = \frac{4t}{\sum_{i=1}^{n}(b_i-a_i)^2} \), then we obtain (2.19). The proof of (2.20) is similar. \( \square \)

Now we will apply Hoeffding’s inequality to improve our crude concentration bound (2.9) for the sum of \( n \) independent Bernoulli(\( \theta \)) random variables, \( X_1, \ldots, X_n \). Since each \( X_i \in \{0, 1\} \), we can apply Theorem 2.1 to get, for any \( t > 0 \),

\[
\Pr \left( \left| \sum_{i=1}^{n} X_i - n\theta \right| \geq t \right) \leq 2e^{-2t^2/n}.
\]
Therefore,

\[
P \left( \left| \hat{\theta}_n - \theta \right| \geq \varepsilon \right) = P \left( \left| \sum_{i=1}^{n} X_i - n\theta \right| \geq n \varepsilon \right) \leq 2e^{-2n\varepsilon^2},
\]

which gives us the claimed bound (2.1).

3. From bounded variables to bounded differences: McDiarmid’s inequality

Hoeffding’s inequality applies to sums of independent random variables. We will now develop its generalization, due to McDiarmid [McD89], to arbitrary real-valued functions of independent random variables that satisfy a certain condition.

Let \( X \) be some set, and consider a function \( g : X^n \rightarrow \mathbb{R} \). We say that \( g \) has bounded differences if there exist nonnegative numbers \( c_1, \ldots, c_n \), such that

\[
\sup_{x \in X} g(x_1, \ldots, x_{i-1}, x, x_{i+1}, \ldots, x_n) - \inf_{x \in X} g(x_1, \ldots, x_{i-1}, x, x_{i+1}, \ldots, x_n) \leq c_i
\]

for all \( i = 1, \ldots, n \) and all \( x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n \in X \). In words, if we change the \( i \)th variable while keeping all the others fixed, the value of \( g \) will not change by more than \( c_i \).

**Theorem 2.2** (McDiarmid’s inequality [McD89]). Let \( X^n = (X_1, \ldots, X_n) \in X^n \) be an \( n \)-tuple of independent \( X \)-valued random variables. If a function \( g : X^n \rightarrow \mathbb{R} \) has bounded differences, as in (2.24), then, for all \( t > 0 \),

\[
P \left( g(X^n) - E g(X^n) \geq t \right) \leq \exp \left( -\frac{2t^2}{\sum_{i=1}^{n} c_i^2} \right);
\]

\[
P \left( E g(X^n) - g(X^n) \geq t \right) \leq \exp \left( -\frac{2t^2}{\sum_{i=1}^{n} c_i^2} \right).
\]

**Proof.** Let us first sketch the general idea behind the proof. Let \( Z = g(X^n) \) and \( V = Z - E Z \). The first step will be to write \( V \) as a sum \( \sum_{i=1}^{n} V_i \), where the terms \( V_i \) are constructed so that:

1. \( V_i \) is a function only of \( X^i = (X_1, \ldots, X_i) \), and \( E[V_i | X^{i-1}] = 0 \).
2. There exist functions \( A_i, B_i : X^{i-1} \rightarrow \mathbb{R} \) such that, conditionally on \( X^{i-1} \),

\[
A_i(X^{i-1}) \leq V_i \leq B_i(X^{i-1}),
\]

and, moreover, \( B_i(X^{i-1}) - A_i(X^{i-1}) \leq c_i \).

Provided we can arrange things in this way, we can apply Lemma 2.1 to \( V_i \) conditionally on \( X^{i-1} \):

\[
E[e^{V_i} | X^{i-1}] \leq e^{c_i^2/8}.
\]
Then, using Chernoff’s method, we have

\[
P(Z - EZ \geq t) = P(V \geq t)
\]

\[
\leq e^{-st} E[e^{sV}]
\]

\[
= e^{-st} E[e^{s\sum_{i=1}^{n} V_i}]
\]

\[
= e^{-st} E[e^{s\sum_{i=1}^{n-1} V_i} e^{sV_n}]
\]

\[
= e^{-st} E[e^{s\sum_{i=1}^{n-1} V_i} E[e^{sV_n} | X^{n-1}]]
\]

\[
\leq e^{-st} e^{s^2 c_2^2 / 8} E[e^{s\sum_{i=1}^{n-1} V_i}],
\]

where in the next-to-last step we used the fact that \(V_1, \ldots, V_{n-1}\) depend only on \(X^{n-1}\), and in the last step we used (2.27) with \(i = n\). If we continue peeling off the terms involving \(V_{n-1}, V_{n-2}, \ldots, V_1\), we will get

\[
P(Z - EZ \geq t) \leq \exp \left(-st + \frac{s^2}{8} \sum_{i=1}^{n} c_i^2\right).
\]

Taking \(s = 4t / \sum_{i=1}^{n} c_i^2\), we end up with (2.25).

It remains to construct the \(V_i\)’s with the desired properties. To that end, let

\[
V_i = E[Z|X^i] - E[Z|X^{i-1}],
\]

where \(E[Z|X^0] = EZ\), and, by telescoping,

\[
\sum_{i=1}^{n} V_i = \sum_{i=1}^{n} \{E[Z|X^i] - E[Z|X^{i-1}]\} = E[Z|X^n] - EZ = Z - EZ = V.
\]

Note that \(V_i\) depends only on \(X^i\) by construction, and that

\[
E[V_i | X^{i-1}] = E[E[Z|X^i] - E[Z|X^{i-1}] | X^{i-1}]
\]

\[
= E[E[Z|X^{i-1}, X_i] | X^{i-1}] - E[Z|X^{i-1}]
\]

\[
= E[Z|X^{i-1}] - E[Z|X^{i-1}]
\]

\[
= 0,
\]

where we have used the law of iterated expectation in the conditional form \(E[E[U|V,W]|V] = E[U|V]\). Moreover, let

\[
A_i(X^{i-1}) = \inf_{x \in X} E[g(X^{i-1}, x, X^n) - g(X^n)|X^{i-1}]
\]

\[
B_i(X^{i-1}) = \sup_{x \in X} E[g(X^{i-1}, x, X^n) - g(X^n)|X^{i-1}],
\]

17
where we have used the fact that the $X_i$'s are independent, and where $X_{i+1}^n := (X_{i+1}, \ldots, X_n)$. Then evidently $A_i(X^{-1}) \leq V_i \leq B_i(X^{-1})$, and
\[
B_i(X^{-1}) - A_i(X^{-1}) = \sup_{x \in X} \sup_{x' \in X} \mathbb{E}[g(X^{-1}, x, X_{i+1}^n) - g(X^{-1}, x', X_{i+1}^n)|X^{-1}]
\]
\[
= \sup_{x \in X} \sup_{x' \in X} \left( \int [g(X^{-1}, x, x_{i+1}^n) - g(X^{-1}, x', x_{i+1}^n)] \, P(dx_{i+1}^n) \right)
\]
\[
\leq \int \sup_{x \in X} \sup_{x' \in X} [g(X^{-1}, x, x_{i+1}^n) - g(X^{-1}, x', x_{i+1}^n)] \, P(dx_{i+1}^n)
\]
\[
\leq c_i,
\]
where the last step follows from the bounded difference property of $g$. \qed

4. McDiarmid’s inequality in action

McDiarmid’s inequality is an extremely powerful and often used tool in statistical learning theory. We will now discuss several examples of its use. To that end, we will first introduce some notation and definitions.

Let $X$ be some (measurable) space. If $Q$ is a probability distribution of an $X$-valued random variable $X$, then we can compute the expectation of any (measurable) function $f : X \to \mathbb{R}$ w.r.t. $Q$. So far, we have denoted this expectation by $\mathbb{E}f(X)$ or by $\mathbb{E}_Q f(X)$. We will often find it convenient to use an alternative notation, $Q(f)$.

Let $X^n = (X_1, \ldots, X_n)$ be $n$ independent identically distributed (i.i.d.) $X$-valued random variables with common distribution $P$. The main object of interest to us is the empirical distribution induced by $X^n$, which we will denote by $P_{X^n}$. The empirical distribution assigns the probability $1/n$ to each $X_i$, i.e.,
\[
P_{X^n} = \frac{1}{n} \sum_{i=1}^{n} \delta_{X_i}.
\]

Here, $\delta_x$ denotes a unit mass concentrated at a point $x \in X$, i.e., the probability distribution on $X$ that assigns each event $A$ the probability
\[
\delta_x(A) = 1_{\{x \in A\}}, \quad \forall \text{ measurable } A \subseteq X.
\]

We note the following important facts about $P_{X^n}$:

1. Being a function of the sample $X^n$, $P_{X^n}$ is a random variable taking values in the space of probability distributions over $X$.
2. The probability of a set $A \subseteq X$ under $P_{X^n}$,
\[
P_{X^n}(A) = \frac{1}{n} \sum_{i=1}^{n} 1_{\{X_i \in A\}},
\]

is the empirical frequency of the set $A$ on the sample $X^n$. The expectation of $P_{X^n}(A)$ is equal to $P(A)$, the $P$-probability of $A$. Indeed,
\[
\mathbb{E}P_{X^n}(A) = \mathbb{E} \left[ \frac{1}{n} \sum_{i=1}^{n} 1_{\{X_i \in A\}} \right] = \frac{1}{n} \sum_{i=1}^{n} \mathbb{E}[1_{\{X_i \in A\}}] = \frac{1}{n} \sum_{i=1}^{n} P(X_i \in A) = P(A).
\]
(Think back to our coin-tossing example – this is a generalization of that idea, where we approximate actual probabilities of events by their relative frequencies in a series of independent trials.)

(3) Given a function $f : X \to \mathbb{R}$, we can compute its expectation w.r.t. $P_{X^n}$:

$$P_{X^n}(f) = \frac{1}{n} \sum_{i=1}^{n} f(X_i),$$

which is just the sample mean of $f$ on $X^n$. It is also referred to as the empirical expectation of $f$ on $X^n$. We have

$$E P_{X^n}(f) = E \left[ \frac{1}{n} \sum_{i=1}^{n} f(X_i) \right] = \frac{1}{n} \sum_{i=1}^{n} E f(X_i) = E f(X) = P(f).$$

We can now proceed to our examples.

4.1. Sums of bounded random variables. In the special case when $X = \mathbb{R}$, $P$ is a probability distribution supported on a finite interval, and $g(X^n)$ is the sum

$$g(X^n) = \sum_{i=1}^{n} X_i,$$

McDiarmid’s inequality simply reduces to Hoeffding’s. Indeed, for any $x^n \in [a, b]^n$ and $x'_i \in [a, b]$ we have

$$g(x^{i-1}, x_i, x^n_{i+1}) - g(x^{i-1}, x'_i, x^n_{i+1}) = x_i - x'_i \leq b - a.$$

Interchanging the roles of $x'_i$ and $x_i$, we get

$$g(x^{i-1}, x'_i, x^n_{i+1}) - g(x^{i-1}, x_i, x^n_{i+1}) = x'_i - x_i \leq b - a.$$

Hence, we may apply Theorem 2.2 with $c_i = b - a$ for all $i$ to get

$$P \left( |g(X^n) - E g(X^n)| \geq t \right) \leq 2 \exp \left( -\frac{2t^2}{n(b-a)^2} \right).$$

4.2. Uniform deviations. Let $X_1, \ldots, X_n$ be $n$ i.i.d. $X$-valued random variables with common distribution $P$. By the Law of Large Numbers, for any $A \subseteq X$ and any $\varepsilon > 0$

$$\lim_{n \to \infty} P \left( |P_{X^n}(A) - P(A)| \geq \varepsilon \right) = 0.$$

In fact, we can use Hoeffding’s inequality to show that

$$P \left( |P_{X^n}(A) - P(A)| \geq \varepsilon \right) \leq 2e^{-2n\varepsilon^2}.$$

This probability bound holds for each $A$ separately. However, in learning theory we are often interested in the deviation of empirical frequencies from true probabilities simultaneously over some collection of subsets of $X$. To that end, let $\mathcal{A}$ be such a collection and consider the function

$$g(X^n) := \sup_{A \in \mathcal{A}} |P_{X^n}(A) - P(A)|.$$

Later in the course we will see that, for certain choices of $\mathcal{A}$, $E g(X^n) = O(1/\sqrt{n})$. However, regardless of what $\mathcal{A}$ is, it is easy to see that, by changing only one $X_i$, the value of $g(X^n)$
can change at most by $1/n$. Let $x^n = (x_1, \ldots, x_n)$, choose some other $x'_i \in X$, and let $x^n_{(i)}$ denote $x^n$ with $x_i$ replaced by $x'_i$:

$$x^n = (x^{i-1}, x_i, x_{i+1}^n), \quad x^n_{(i)} = (x^{i-1}, x'_i, x_{i+1}^n).$$

Then

$$g(x^n) - g(x^n_{(i)}) = \sup_{A \in A} \left| P_{x^n}(A) - P(A) \right| - \sup_{A' \in A} \left| P_{x^n_{(i)}}(A') - P(A') \right|$$

$$\leq \sup_{A \in A} \inf_{A' \in A} \left\{ \left| P_{x^n}(A) - P(A) \right| - \left| P_{x^n_{(i)}}(A) - P(A) \right| \right\}$$

$$\leq \frac{1}{n} \sup_{A \in A} |1_{\{x_i \in A\}} - 1_{\{x'_i \in A\}}|$$

$$\leq \frac{1}{n}. $$

Interchanging the roles of $x^n$ and $x^n_{(i)}$, we obtain

$$g(x^n_{(i)}) - g(x^n) \leq \frac{1}{n}.$$

Thus,

$$|g(x^n) - g(x^n_{(i)})| \leq \frac{1}{n}.$$

Note that this bound holds for all $i$ and all choices of $x^n$ and $x^n_{(i)}$. This means that the function $g$ defined in (2.28) has bounded differences with $c_1 = \ldots = c_n = 1/n$. Consequently, we can use Theorem 2.2 to get

$$\mathbb{P} \left( |g(X^n) - \mathbb{E}g(X^n)| \geq \varepsilon \right) \leq 2e^{-2n\varepsilon^2}.$$

This shows that the *uniform deviation* $g(X^n)$ concentrates sharply around its mean $\mathbb{E}g(X^n)$.

### 4.3. Uniform deviations continued.

The same idea applies to arbitrary real-valued functions over $X$. Let $X^n = (X_1, \ldots, X_n)$ be as in the previous example. Given any function $f : X \rightarrow [0, 1]$, Hoeffding’s inequality tells us that

$$\mathbb{P} \left( |P_{X^n}(f) - \mathbb{E}f(X)| \geq \varepsilon \right) \leq 2e^{-2n\varepsilon^2}.$$

However, just as in the previous example, in learning theory we are primarily interested in controlling the deviations of empirical means from true means simultaneously over whole classes of functions. To that end, let $\mathcal{F}$ be such a class consisting of functions $f : X \rightarrow [0, 1]$ and consider the *uniform deviation*

$$g(X^n) := \sup_{f \in \mathcal{F}} |P_{X^n}(f) - P(f)|.$$
An argument entirely similar to the one in the previous example\(^1\) shows that this \(g\) has bounded differences with \(c_1 = \ldots = c_n = 1/n\). Therefore, applying McDiarmid’s inequality, we obtain

\[
P(\left| g(X^n) - \mathbb{E}g(X^n) \right| \geq \varepsilon) \leq 2e^{-2n\varepsilon^2}.
\]

We will see later that, for certain function classes \(\mathcal{F}\), we will have \(\mathbb{E}g(X^n) = O(1/\sqrt{n})\).

### 4.4. Kernel density estimation.

For our final example, let \(X^n = (X_1, \ldots, X_n)\) be an \(n\)-tuple of i.i.d. real-valued random variables whose common distribution \(P\) has a probability density function (pdf) \(f\), i.e.,

\[
P(A) = \int_A f(x) \, dx
\]

for any measurable set \(A \subseteq \mathbb{R}\). We wish to estimate \(f\) from the sample \(X^n\). A popular method is to use a kernel estimate (the book by Devroye and Lugosi [DL01] has plenty of material on density estimation, including kernel methods, from the viewpoint of statistical learning theory). To that end, we pick a nonnegative function \(K : \mathbb{R} \rightarrow \mathbb{R}\) that integrates to one, \(\int K(x) \, dx = 1\) (such a function is called a kernel), as well as a positive bandwidth (or smoothing constant) \(h > 0\) and form the estimate

\[
\hat{f}_n(x) = \frac{1}{nh} \sum_{i=1}^n K \left( \frac{x - X_i}{h} \right).
\]

It is not hard to verify\(^2\) that \(\hat{f}_n\) is a valid pdf, i.e., that it is nonnegative and integrates to one. A common way of quantifying the performance of a density estimator is to use the \(L^1\) distance to the true density \(f\):

\[
\| \hat{f}_n - f \|_{L^1} = \int_{\mathbb{R}} \left| \hat{f}_n(x) - f(x) \right| \, dx.
\]

Note that \(\| \hat{f}_n - f \|_{L^1}\) is a random variable since it depends on the random sample \(X^n\). Thus, we can write it as a function \(g(X^n)\) of the sample \(X^n\). Leaving aside the problem of actually bounding \(\mathbb{E}g(X^n)\), we can easily establish a concentration bound for it using McDiarmid’s inequality. To do that, we need to check that \(g\) has bounded differences. Choosing \(x^n\) and

\(^1\)Exercise: verify this!

\(^2\)Another exercise!
as before, we have
\[ g(x^n) - g(x^n_{(i)}) \]
\[ = \int_{\mathbb{R}} \left| \frac{1}{nh} \sum_{j=1}^{i-1} K \left( \frac{x - x_j}{h} \right) + \frac{1}{nh} K \left( \frac{x - x_i}{h} \right) + \frac{1}{nh} \sum_{j=i+1}^{n} K \left( \frac{x - x_j}{h} \right) - f(x) \right| dx \]
\[ - \int_{\mathbb{R}} \left| \frac{1}{nh} \sum_{j=1}^{i-1} K \left( \frac{x - x_j}{h} \right) + \frac{1}{nh} K \left( \frac{x - x_i'}{h} \right) + \frac{1}{nh} \sum_{j=i+1}^{n} K \left( \frac{x - x_j}{h} \right) - f(x) \right| dx \]
\[ \leq \frac{1}{nh} \int_{\mathbb{R}} \left| K \left( \frac{x - x_i}{h} \right) - K \left( \frac{x - x_i'}{h} \right) \right| dx \]
\[ \leq \frac{2}{nh} \int_{\mathbb{R}} K \left( \frac{x}{h} \right) dx \]
\[ = \frac{2}{n}. \]
Thus, we see that \( g(X^n) \) has the bounded differences property with \( c_1 = \ldots = c_n = \frac{2}{n} \), so that
\[ \mathbb{P} \left( |g(X^n) - \mathbb{E}g(X^n)| \geq \varepsilon \right) \leq 2e^{-n\varepsilon^2/2}. \]
Part 2

Basic Theory
CHAPTER 3

Formulation of the learning problem

Now that we have seen an informal statement of the learning problem, as well as acquired some technical tools in the form of concentration inequalities, we can proceed to define the learning problem formally. Recall that the basic goal is to be able to predict some random variable $Y$ of interest from a correlated random observation $X$, where the predictor is to be constructed on the basis of $n$ i.i.d. training samples $(X_1, Y_1), \ldots, (X_n, Y_n)$ from the joint distribution of $(X, Y)$. We will start by looking at an idealized scenario (often called the realizable case in the literature), in which $Y$ is a deterministic function of $X$, and we happen to know the function class to which it belongs. This simple set-up will let us pose, in a clean form, the basic requirements a learning algorithm should satisfy. Once we are done with the realizable case, we can move on to the general setting, in which the relationship between $X$ and $Y$ is probabilistic and not known precisely. This is often referred to as the model-free or agnostic case.

This order of presentation is, essentially, historical. The first statement of the learning problem is hard to trace precisely, but the “modern” algorithmic formalization seems to originate with the 1984 work of Valiant [Val84] on learning Boolean formulae. Valiant has focused on computationally efficient learning algorithms. The agnostic (or model-free) formulation was first proposed and studied by Haussler [Hau92] in 1992.

The material in this chapter closely follows the excellent exposition of Vidyasagar [Vid03, Ch. 3].

1. The realizable case

We start with an idealized scenario, now often referred to in the literature as the realizable case. The basic set-up is as follows. We have a set $X$ (often called the feature space or input space) and a family $\mathcal{P}$ of probability distributions on $X$. We obtain an i.i.d. sample $X^n = (X_1, \ldots, X_n)$ drawn according to some $P \in \mathcal{P}$, which we do not know (although it may very well be the case that $\mathcal{P}$ is a singleton, $|\mathcal{P}| = 1$, in which case we, of course, do know $P$). We will look at two basic problems:

1. Concept learning: There is a class $C$ of subsets of $X$, called the concept class, and an unknown target concept $C^* \in C$ is picked by Nature. For each feature $X_i$ in our sample $X^n$, we receive a binary label $Y_i = 1_{\{X_i \in C^*\}}$. The $n$ feature-label pairs form the training set

$$ (X_1, Y_1) = (X_1, 1_{\{X_1 \in C^*\}}), \ldots, (X_n, Y_n) = (X_n, 1_{\{X_n \in C^*\}}). $$

The objective is to approximate the target concept $C^*$ as accurately as possible.

2. Function learning: There is a class $\mathcal{F}$ of functions $f : X \rightarrow [0, 1]$, and an unknown target function $f^* \in \mathcal{F}$ is picked by nature. For each input point $X_i$ in the sample
$X^n$, we receive a real-valued output $Y_i = f^*(X_i)$. The $n$ input-output pairs

\[(3.2) \quad (X_1, Y_1) = (X_1, f^*(X_1)), \ldots, (X_n, f^*(X_n)).\]

The objective is to approximate the target function $f^*$ as accurately as possible. (Note: the requirement that $f$ map $X$ into $[0, 1]$ is imposed primarily for technical convenience; using appropriate moment and/or tail behavior assumptions on $P$, it is possible to remove this requirement, but the resulting proofs will be somewhat laborious.)

We will now consider these two problems separately.

1.1. Concept learning. As we already stated, the goal of concept learning is to approximate the target concept $C^*$ as accurately as possible on the basis of the training data (3.1). This is done by means of a learning algorithm. An algorithm of this sort should be capable of producing an approximation to $C^*$ given the training set of the form (3.1) of any size $n$. More precisely:

Definition 3.1. A concept learning problem is specified by a triple $(X, \mathcal{P}, \mathcal{C})$, where $X$ is the feature space, $\mathcal{P}$ is a family of probability distributions on $X$, and $\mathcal{C}$ is a concept class. A learning algorithm for $(X, \mathcal{P}, \mathcal{C})$ is a sequence $A = \{A_n\}_{n=1}^\infty$ of mappings

$$A_n : (X \times \{0, 1\})^n \rightarrow \mathcal{C}.$$ 

If $\mathcal{P}$ consists of only one distribution $P$, then the mappings $A_n$ may depend on $P$; otherwise, they may only depend on $P$ as a whole. The idea behind the above definition is that for each training set size $n$ we have a definite procedure for forming an approximation to the unknown target concept $C^*$ on the basis of the training set of that size.

For brevity, let us denote by $Z_i$ the $i$th training pair $(X_i, Y_i) = (X_i, 1_{\{X_i \in C^*\}})$, and let us denote by $Z$ the set $X \times \{0, 1\}$. Given a training set $Z^n = (Z_1, \ldots, Z_n) \in \mathcal{Z}^n$ and a learning algorithm $A$, the approximation to $C^*$ is

$$\hat{C}_n = A_n(Z^n) = A_n(Z_1, \ldots, Z_n) = A_n((X_1, 1_{\{X_1 \in C^*\}}, \ldots, (X_n, 1_{\{X_n \in C^*\}})).$$

Note that $\hat{C}_n$ is an element of the concept class $\mathcal{C}$ (by definition), and that it is a random variable since it depends on the random sample $Z^n$. It is often referred to as a hypothesis output by the learning algorithm $A$.

How shall we measure the goodness of this approximation $\hat{C}_n$? A natural thing to do is the following. Suppose now we draw a fresh feature $X$ from the same distribution $P \in \mathcal{P}$ as the one that has generated the training feature set $X^n$ and venture a hypothesis that $X$ belongs to the target concept $C^*$ if $X \in \hat{C}_n$, i.e., if $1_{\{X \in \hat{C}_n\}} = 1$. When would we make a mistake, i.e., misclassify $X$? There are two mutually exclusive cases:

1. $X$ is in $C^*$, but not in $\hat{C}_n$, i.e., $X \in C^* \cap \hat{C}_n^c$, where $\hat{C}_n^c = X \setminus \hat{C}_n$ is the complement of $\hat{C}_n$ in $X$.

2. $X$ is not in $C^*$, but it is in $\hat{C}_n$, i.e., $X \in (C^*)^c \cap \hat{C}_n$.

Thus, we will misclassify $X$ precisely when it happens to lie in the symmetric difference $C^* \triangle \hat{C}_n := (C^* \cap \hat{C}_n^c) \cup ((C^*)^c \cap \hat{C}_n)$. This will happen with probability $P(C^* \triangle \hat{C}_n)$ — note, by the way, that this is a random number since $\hat{C}_n$ depends on the training data $Z^n$. At any rate, we take the $P$-probability of
the symmetric difference \( C^* \triangle \hat{C}_n \) as our measure of performance of \( \mathcal{A} \). In order to streamline the notation, let us define the risk (or loss) of any \( C \in \mathcal{C} \) w.r.t. \( C^* \) and \( P \) as
\[
L_P(C, C^*) := P(C \triangle C^*) = P(X \in C \triangle C^*).
\]

**Exercise 3.1.** Prove that
\[
L_P(C, C^*) = \int_X \| \mathbf{1}_{\{x \in C\}} - \mathbf{1}_{\{x \in C^*\}} \|^2 P(dx).
\]

In other words, \( L_P(C, C^*) \) is the squared \( L^2(P) \) norm of the difference of the indicator functions \( I_C(\cdot) = \mathbf{1}_{\{x \in C\}} \) and \( I_{C^*}(\cdot) = \mathbf{1}_{\{x \in C^*\}} \), \( L_P(C, C^*) = \|I_C - I_{C^*}\|_{L^2(P)}^2 \).

Roughly speaking, we will say that \( \mathcal{A} \) is a good algorithm if
\[
(3.3) \quad L_P(\hat{C}_n, C^*) \to 0 \quad \text{as } n \to \infty
\]
for any \( P \in \mathcal{P} \) and any \( C^* \in \mathcal{C} \). Since \( \hat{C}_n \) is a random element of \( \mathcal{C} \), the convergence in (3.3) can only be in some probabilistic sense. In order to make things precise, for any \( C \in \mathcal{C} \) let \( \mathcal{P}_C \) the joint distribution of a pair \( Z = (X, Y) \), where \( X \sim P \) and \( Y = \mathbf{1}_{\{x \in C\}} \). Then we define the following two quantities:
\[
r_A(n, \varepsilon, P) := \sup_{C \in \mathcal{C}} P^n_C \left( Z^n \in Z^n : L_P(A_n(Z^n), C) \geq \varepsilon \right)
\]
\[
\bar{r}_A(n, \varepsilon, \mathcal{P}) := \sup_{P \in \mathcal{P}} r_A(n, \varepsilon, P)
\]
where \( P^n_C \) denotes the \( n \)-fold product of \( P \). For a fixed \( P \) (which amounts to assuming that the features \( X^n \) were drawn i.i.d. from \( P \)), \( r_A(n, \varepsilon, P) \) quantifies the worst-case “size” of the set of “bad” samples, where we say that a sample \( X^n \) is bad if it causes the learning algorithm \( \mathcal{A} \) to output a hypothesis \( \hat{C}_n = A_n(Z^n) \) whose risk is larger than \( \varepsilon \). The worst case is over the entire concept class \( \mathcal{C} \), since we do not know the target concept \( C^* \). The quantity \( \bar{r}_A(n, \varepsilon, \mathcal{P}) \) accounts for the fact that we do not know which \( P \in \mathcal{P} \) has generated the training feature points.

With all these things defined, we can now state the following:

**Definition 3.2.** A learning algorithm \( \mathcal{A} = \{A_n\} \) is probably approximately correct (or PAC) to accuracy \( \varepsilon \) if
\[
(3.4) \quad \lim_{n \to \infty} \bar{r}_A(n, \varepsilon, \mathcal{P}) = 0.
\]
We say that \( \mathcal{A} \) is PAC if it is PAC to accuracy \( \varepsilon \) for every \( \varepsilon > 0 \). The concept class \( \mathcal{C} \) is called PAC learnable to accuracy \( \varepsilon \) w.r.t. \( \mathcal{P} \) if there exists an algorithm that is PAC to accuracy \( \varepsilon \). Finally, we say that \( \mathcal{C} \) is PAC learnable if there exists an algorithm that is PAC.

The term “probably approximately correct,” which seems to have first been introduced by Angluin [Ang88], is motivated by the following observations. First, the hypothesis \( \hat{C}_n \) output by \( \mathcal{A} \) for some \( n \) is only an approximation to the target concept \( C^* \). Thus, \( L_P(\hat{C}_n, C^*) \) will be, in general, nonzero. But if it is small, then we are justified in claiming that \( \hat{C}_n \) is approximately correct. Secondly, we may always encounter a bad sample, so \( L_P(\hat{C}_n, C^*) \) can be made small only with high probability. Thus, informally speaking, a PAC algorithm is one that “works reasonably well most of the time.”
An equivalent way of phrasing the statement that a learning algorithm is PAC is as follows: For any \( \varepsilon > 0 \) and \( \delta > 0 \), there exists some \( n(\varepsilon, \delta) \in \mathbb{N} \), such that

\[
P_C^n(\mathbb{Z}^n \in \mathbb{Z}^n : L_P(A_n(\mathbb{Z}^n), C) > \varepsilon) \leq \delta, \quad \forall n \geq n(\varepsilon, \delta), \forall C \in \mathcal{C}, \forall P \in \mathcal{P}.
\]

In this context, \( \varepsilon \) is called the accuracy parameter, while \( \delta \) is called the confidence parameter. The meaning of this alternative characterization is as follows. If the sample size \( n \) is at least \( n(\varepsilon, \delta) \), then we can state with confidence at least \( 1 - \delta \) that the hypothesis \( \hat{C}_n \) will correctly classify a fresh random point \( X \in \mathcal{X} \) with probability at least \( 1 - \varepsilon \).

The two problems of interest to us are:

1. Determine conditions under which a given concept class \( \mathcal{C} \) is PAC learnable.
2. Obtain upper and lower bounds on \( n(\varepsilon, \delta) \) as a function of \( \varepsilon, \delta \). The following terminology is often used: the smallest number \( n(\varepsilon, \delta) \) such that (3.5) holds is called the sample complexity.

### 1.2. Function learning

The goal of function learning is to construct an accurate approximation to an unknown target function \( f^* \in \mathcal{F} \) on the basis of training data of the form (3.2). Analogously to the concept learning scenario, we have:

**Definition 3.3.** A function learning problem is specified by a triple \((\mathcal{X}, \mathcal{P}, \mathcal{F})\), where \( \mathcal{X} \) is the input space, \( \mathcal{P} \) is a family of probability distributions on \( \mathcal{X} \), and \( \mathcal{F} \) is a class of functions \( f : \mathcal{X} \to [0,1] \). A learning algorithm for \((\mathcal{X}, \mathcal{P}, \mathcal{F})\) is a sequence \( \mathcal{A} = \{A_n\}_{n=1}^{\infty} \) of mappings

\[ A_n : (\mathcal{X} \times [0,1])^n \to \mathcal{F}. \]

As before, let us denote by \( Z_i \) the input-output pair \((X_i, Y_i) = (X_i, f^*(X_i))\) and by \( Z \) the product set \( \mathcal{X} \times [0,1] \). Given a training set \( \mathbb{Z}^n = (Z_1, \ldots, Z_n) \in \mathbb{Z}^n \) and a learning algorithm \( \mathcal{A} \), the approximation to \( f^* \) is

\[ \hat{f}_n = A_n(\mathbb{Z}^n) = A_n((X_1, f^*(X_1)), \ldots, (X_n, f^*(X_n))). \]

As in the concept learning setting, \( \hat{f}_n \) is a random element of the function class \( \mathcal{F} \).

In order to measure the performance of \( \mathcal{A} \), we again imagine drawing a fresh input point \( X \in \mathcal{X} \) from the same distribution \( P \in \mathcal{P} \) that has generated the training inputs \( \mathbb{X}^n \). A natural error metric is the squared loss \( |\hat{f}_n(X) - f^*(X)|^2 \). As before, we can define the risk (or loss) of any \( f \in \mathcal{F} \) w.r.t. \( f^* \) and \( P \) as

\[
L_P(f, f^*) := E_P|f(X) - f^*(X)|^2 = \|f - f^*\|_{L^2(P)}^2 = \int_X |f(x) - f^*(x)|^2 P(dx).
\]

Thus, the quantity of interest is the risk of \( \hat{f}_n \):

\[
L_P(\hat{f}_n, f^*) = \int_X |\hat{f}_n(x) - f^*(x)|^2 P(dx).
\]

Keep in mind that \( L_P(\hat{f}_n, f^*) \) is a random variable, as it depends on \( \hat{f}_n \), which in turn depends on the random sample \( \mathbb{Z}^n \in \mathbb{Z}^n \).
The concept learning problem is, in fact, a special case of the function learning problem. Indeed, fix a concept class $C$ and consider the function class $F$ consisting of the indicator functions of the sets in $C$:

$$F = \{ I_C : C \in \mathcal{C} \}.$$ 

Then for any $f = I_C$ and $f^* = I_{C^*}$ we will have

$$L_P(f, f^*) = \| I_C - I_{C^*} \|_2^2 = P(C \triangle C^*),$$

which is the error metric we have defined for concept learning.

If for each $f \in F$ we denote by $P_f$ the joint distribution of a pair $Z = (X, Y)$, where $X \sim P$ and $Y = f(X)$, then for a given learning problem $(X, P, F)$ and a given algorithm $A$ we can define

$$r_A(n, \varepsilon, P) := \sup_{f \in F} P^n_f (Z^n : L_P(A_n(Z^n), f) \geq \varepsilon)$$

$$\bar{r}_A(n, \varepsilon, P) := \sup_{P \in \mathcal{P}} r_A(n, \varepsilon, P)$$

for every $n \in \mathbb{N}$ and $\varepsilon > 0$. The meaning of these quantities is exactly parallel to the corresponding quantities in concept learning, and leads to the following definition:

**Definition 3.4.** A learning algorithm $A = \{ A_n \}$ is PAC to accuracy $\varepsilon$ if

$$\lim_{n \to \infty} \bar{r}_A(n, \varepsilon, P) = 0,$$

and PAC if it is PAC to accuracy $\varepsilon$ for all $\varepsilon > 0$. A function class $F = \{ f : X \to [0, 1] \}$ is PAC-learnable (to accuracy $\varepsilon$) w.r.t. $P$ if there exists an algorithm $A$ that is PAC for $(X, P, F)$ (to accuracy $\varepsilon$).

An equivalent way of stating that $A$ is PAC is that, for any $\varepsilon, \delta > 0$ there exists some $n(\varepsilon, \delta) \in \mathbb{N}$ such that

$$P^n_f (Z^n : L_P(A_n(Z^n), f) \geq \varepsilon) \leq \delta, \quad \forall n \geq n(\varepsilon, \delta), \forall f \in F, \forall P \in \mathcal{P}.$$ 

The smallest $n(\varepsilon, \delta) \in \mathbb{N}$ for which the above inequality holds is termed the sample complexity.

2. Example: learning axis-parallel rectangles

To make these ideas concrete, let us consider an example of a PAC-learnable concept class. Given what we know at this point, the only way to show that a given concept class is PAC-learnable is to exhibit an algorithm which is PAC. Later on, we will develop generic tools that will allow us to determine PAC-learnability without having to construct an algorithm for each separate case.

We take $X = [0, 1]^2$, the unit square in the plane, let $\mathcal{P}$ be the class of all probability distributions on $X$ (w.r.t. the usual Borel $\sigma$-algebra), and let $\mathcal{C}$ be the collection of all axis-parallel rectangles: that is, a set $C$ is in $\mathcal{C}$ if and only if it is of the form

$$C = [a_1, b_1] \times [a_2, b_2] = \{ (x_1, x_2) \in [0, 1]^2 : a_1 \leq x_1 \leq b_1, a_2 \leq x_2 \leq b_2 \}$$

for some $0 \leq a_1 \leq b_1 \leq 1$ and $0 \leq a_2 \leq b_2 \leq 1$ (see Figure 1).
Figure 1. An axis-parallel rectangle.

We now describe our learning algorithm. Given a training set \( Z^n = (Z_1, \ldots, Z_n) = ((X_1, Y_1), \ldots, (X_n, Y_n)) \), we say that the \( i \)th training pair \( Z_i = (X_i, 1_{(X_i \in C^*)}) \) is a positive example if \( Y_i = 1 \) (i.e., if \( X_i \) belongs to the target concept \( C^* \)), and is a negative example otherwise. Our algorithm \( A = \{A_n\}_{n=1}^{\infty} \) is the following intuitive rule: for each \( n \), we take

\[
\hat{C}_n = A_n(Z^n) = \text{smallest rectangle } C \in \mathcal{C} \text{ that contains all positive examples in } Z^n.
\]

Figure 1 shows a particular instance of this algorithm. We will now prove the following result, originally due to Blumer et al. [BEHW89]:

\[
\text{Theorem 3.1. The algorithm } A \text{ defined in (3.7), i.e., the one that returns the smallest axis-parallel rectangle that encloses all positive examples in } Z^n, \text{ satisfies}
\]

\[
\bar{r}_A(n, \varepsilon, \mathcal{P}) \leq 4(1 - \varepsilon/4)^n.
\]

Therefore, this algorithm is PAC, and the class \( \mathcal{C} \) is PAC-learnable.

**Proof.** Since no positive example can lie outside \( C^* \), the hypothesis \( \hat{C}_n \) produced by the algorithm (3.7) must lie inside \( C^* \): \( \hat{C}_n \subseteq C^* \). Therefore,

\[
\hat{C}_n \triangle C^* = C^* \cap (\hat{C}_n)^c \equiv C^* \setminus \hat{C}_n.
\]
If \( P(C^*) < \varepsilon \), then from (3.9) it follows that \( L_P(\hat{C}_n, C^*) = P(C^* \setminus \hat{C}_n) \leq P(C^*) < \varepsilon \). Thus, we will assume that \( P(C^*) \geq \varepsilon \). Suppose that \( C^* = [a_1, b_1] \times [a_2, b_2] \) and \( \hat{C}_n = [\hat{a}_1, \hat{b}_1] \times [\hat{a}_2, \hat{b}_2] \), and consider the following four rectangles:

- \( V_1 = [a_1, \hat{a}_1] \times [a_2, b_2] \),
- \( V_2 = (\hat{b}_1, b_1] \times [a_2, b_2] \),
- \( H_1 = [a_1, \hat{b}_1] \times [a_2, \hat{a}_2] \),
- \( H_2 = [a_1, \hat{b}_1] \times (\hat{b}_2, b_2] \)

(see Figure 3). From (3.9), we see that the symmetric difference \( \hat{C}_n \Delta C^* \) is exactly equal to the union of these four rectangles, which we will denote by \( E \):

\[
\hat{C}_n \Delta C^* = E := V_1 \cup V_2 \cup H_1 \cup H_2.
\]

(Note, by the way, that \( V_1, V_2, H_1, H_2, E \) are all random rectangles, since they depend on the hypothesis \( \hat{C}_n \) and thus on the random training set \( Z^n \).) Our goal is show that \( P(E) \leq \varepsilon \) with high probability.

We claim that, with probability at least \( 1 - 4(1 - \varepsilon/4)^n \), each of the rectangles \( V_1, V_2, H_1, H_2 \) has \( P \)-probability of no more than \( \varepsilon/4 \). Assuming this is the case, then \( P(E) = P(V_1 \cup V_2 \cup H_1 \cup H_2) \leq \varepsilon \) with probability at least \( 1 - 4(1 - \varepsilon/4)^n \). From this, we conclude that, for any \( C^* \),

\[
(3.10) \quad P_{C^*}^n (Z^n \in Z^n : L_P(A_n(Z^n), C^*) \geq \varepsilon) \leq P_{C^*}^n \left( Z^n \in Z^n : P(E) \geq \varepsilon \right) \leq 4(1 - \varepsilon/4)^n.
\]

Since this bound holds for all \( C^* \) and for all \( P \in \mathcal{P} \), we get (3.8).
It now remains to prove the claim. To that end, let $A_1$ be the smallest rectangle of the form $[a_1, a] \times [a_2, b_2]$, such that $P(A_1) \geq \varepsilon/4$, and choose $A_2, B_1, B_2$ in an analogous fashion. Consider the event

$$\bigcup_{i=1}^{n} \{ X_i \in A_1 \},$$

(3.11)
i.e., that $A_1$ is hit by at least one training example. If this event occurs, then any such training example must be a positive example (recall that there are no negative examples in $C^*$), and consequently we must have $P(V_1) \leq \varepsilon/4$. To see this, suppose that the event in (3.11) occurs, but $P(V_1) > \varepsilon/4$. Then there must be some $a'$, such that the closed rectangle $R = [a_1, a'] \times [a_2, b_2] \subset V_1$ with $P(R) > \varepsilon/4$. But then, since $A_1$ is the smallest rectangle of the form $[a_1, a] \times [a_2, b_2]$ whose $P$-probability is at least $\varepsilon/4$, we must have $A_1 \subseteq R \subset V_1$, which is impossible if the event (3.11) occurs. Thus, we obtain the following inclusion:

$$\bigcup_{i=1}^{n} \{ X_i \in A_1 \} \subseteq \{ P(V_1) \leq \varepsilon/4 \}.$$

or, taking the contrapositive,

$$\{ P(V_1) > \varepsilon/4 \} \subseteq \bigcap_{i=1}^{n} \{ X_i \notin A_1 \}.$$

The probability of the event that there are no training examples in $A_1$ can be computed as

$$P \left( \bigcap_{i=1}^{n} \{ X_i \notin A_1 \} \right) = \prod_{i=1}^{n} P( X_i \notin A_1 )$$

(3.12)

$$= [ P( X \notin A_1 ) ]^{n}$$

(3.13)

$$\leq (1 - \varepsilon/4)^n,$$

(3.14)

where (3.12) is by independence of the $X_i$’s, (3.13) follows from the fact that the $X_i$’s are identically distributed, and (3.14) follows from the fact that $P_A(A_1) \geq \varepsilon/4$ by construction. Therefore,

$$P \left[ P(V_1) > \varepsilon/4 \right] \leq P \left[ X_i \notin A_1, \forall i \right] \leq (1 - \varepsilon/4)^n.$$

Similar reasoning applies to $A_2, B_1, B_2$. Thus, with probability at least $1 - 4(1 - \varepsilon/4)^n$,

$$P(V_1) \leq \varepsilon/4, \quad P(V_2) \leq \varepsilon/4, \quad P(H_1) \leq \varepsilon/4, \quad P(H_2) \leq \varepsilon/4,$$

and the claim is proved.

**Corollary 3.1.** The sample complexity of learning axis-parallel rectangles satisfies

$$n(\varepsilon, \delta) \geq \frac{4 \log(4/\delta)}{\varepsilon}.$$

**Proof.** From (3.8), $\bar{r}_A(n, \varepsilon, \mathcal{P}) \leq \delta$ for all $n$ such that $4(1 - \varepsilon/4)^n \leq \delta$ or, equivalently, for all $n$, such that

$$n \log(1 - \varepsilon/4) \leq \log(\delta/4).$$

(3.16)
Using the inequality $\log x \leq x - 1$, we see that if $n$ satisfies (3.15), then it will satisfy (3.16). (Of course, (3.16) is tighter, but all we wanted to see that the number of training examples sufficient to learn an unknown concept $C^* \in \mathcal{C}$ with accuracy $\varepsilon$ and confidence $1 - \delta$ is polynomial in $1/\varepsilon$ and polylogarithmic in $1/\delta$.)

\[ \square \]

3. Agnostic (or model-free) learning

The realizable setting we have focused on in Section 1 rests on certain assumptions, which are not always warranted:

- The assumption that the target concept $C^*$ belongs to $\mathcal{C}$ (or that the target function $f^*$ belongs to $\mathcal{F}$) means that we are trying to fit a hypothesis to data, which are a priori known to have been generated by some member of the model class defined by $\mathcal{C}$ (or by $\mathcal{F}$). However, in general we may not want to (or be able to) assume much about the data generation process, and instead would like to find the best fit to the data at hand using an element of some model class of our choice.
- The assumption that the training features (or inputs) are labelled noiselessly by $1_{\{x \in C^*\}}$ (or by $f(x)$) rules out the possibility of noisy measurements or observations.
- Finally, even if the above assumption were true, we would not necessarily have a priori knowledge of the concept class $\mathcal{C}$ (or the function class $\mathcal{F}$) containing the target concept (or function). In that case, the best we could hope for is to pick our own model class and seek the best approximation to the unknown target concept (or function) among the elements of that class.

The model-free learning problem (also referred to as the agnostic case), introduced by Haussler [Hau92], takes a more general decision-theoretic approach and removes the above restrictions. It has the following ingredients:

- Sets $X$, $Y$, and $U$
- A class $\mathcal{P}$ of probability distributions on $Z := X \times Y$
- A class $\mathcal{F}$ of functions $f : X \to U$ (the hypothesis space)
- A loss function $\ell : Y \times U \to [0, 1]$

The learning process takes place as follows. We obtain an i.i.d. sample $Z^n = (Z_1, \ldots, Z_n)$, where each $Z_i = (X_i, Y_i)$ is drawn from the same fixed but unknown $P \in \mathcal{P}$. A learning algorithm is a sequence $A = \{A_n\}_{n=1}^{\infty}$ of mappings

$$A_n : Z^n \to \mathcal{F}.$$ 

As before, let

$$\widehat{f}_n = A_n(Z^n) = A_n(Z_1, \ldots, Z_n) = A_n((X_1, Y_1), \ldots, (X_n, Y_n)).$$

This is the hypothesis emitted by the learning algorithm based on the training data $Z^n$. Note that, by definition, $\widehat{f}_n$ is a random element of the hypothesis space $\mathcal{F}$, and that it maps each point $x \in X$ to a point $u = \widehat{f}_n(x) \in U$. Following the same steps as in the realizable case, we evaluate the goodness of $\widehat{f}_n$ by its expected loss

$$L_P(\widehat{f}_n) := E_P[\ell(Y, \widehat{f}_n(X))|Z^n] = \int_{X \times Y} \ell(y, \widehat{f}_n(x))P(dx, dy),$$

32
where the expectation is w.r.t. a random couple \((X, Y) \in Z\) drawn according to the same \(P\) but independently of \(Z^n\). Note that \(L_P(f_n)\) is a random variable since so is \(f_n\). In general, we can define the expected risk w.r.t. \(P\) for every \(f\) in our hypothesis space by

\[
L_P(f) := E_P[\ell(Y, f(X))] = \int_{X \times Y} \ell(y, f(x))P(dx, dy)
\]

as well as the minimum risk

\[
L_\star_P(\mathcal{F}) := \inf_{f \in \mathcal{F}} L_P(f).
\]

Conceptually, \(L_\star_P(\mathcal{F})\) is the best possible performance of any hypothesis in \(\mathcal{F}\) when the samples are drawn from \(P\); similarly, \(L_P(\hat{f}_n)\) is the actual performance of the algorithm with access to a training sample of size \(n\). It is clear from definitions that

\[
0 \leq L_P(\mathcal{F}) \leq L_P(\hat{f}_n) \leq 1.
\]

The goal of learning is to guarantee that \(L_P(\hat{f}_n)\) is as close as possible to \(L_\star_P(\mathcal{F})\), whatever the true \(P \in \mathcal{P}\) happens to be. In order to speak about this quantitatively, we need to assess the probability of getting a “bad” sample. To that end, we define, similarly to what we have done earlier, the quantity

\[
r_\Delta(n, \varepsilon) := \sup_{P \in \mathcal{P}} \left( P^n( Z^n \in Z^n : L_P(\hat{f}_n) \geq L_\star_P(\mathcal{F}) + \varepsilon) \right)
\]

for every \(\varepsilon > 0\). Thus, a sample \(Z^n \sim P^n\) is declared to be “bad” if it leads to a hypothesis whose expected risk on an independent test point \((X, Y) \sim P\) is greater than the smallest possible loss \(L_\star_P(\mathcal{F})\) by at least \(\varepsilon\). We have the following:

**Definition 3.5.** We say that a learning algorithm for a problem \((X, Y, U, \mathcal{P}, \mathcal{F}, \ell)\) is PAC to accuracy \(\varepsilon\) if

\[
\lim_{n \to \infty} r_\Delta(n, \varepsilon) = 0.
\]

An algorithm that is PAC to accuracy \(\varepsilon\) for every \(\varepsilon > 0\) is said to be PAC. A learning problem specified by a tuple \((X, Y, U, \mathcal{P}, \mathcal{F}, \ell)\) is model-free (or agnostically) learnable (to accuracy \(\varepsilon\)) if there exists an algorithm for it which is PAC (to accuracy \(\varepsilon\)).

Let us look at some examples.

### 3.1. Function learning in the realizable case.

First we show that the model-free framework contains the realizable set-up as a special case. To see this, let \(X\) be an arbitrary space and let \(Y = U = [0, 1]\). Let \(\mathcal{F}\) be a class of functions \(f : X \to [0, 1]\). Let \(\mathcal{P}_X\) be a family of probability distributions \(P_X\) on \(X\). To each \(P_X\) and each \(f \in \mathcal{F}\) associate a probability distribution \(P_{X,f}\) on \(X \times Y\) as follows: let \(X \sim P_X\), and let the conditional distribution of \(Y\) given \(X = x\) be given by

\[
P_{Y|X,f}(B|X = x) = 1_{\{f(x) \in B\}}
\]

for all (measurable) sets \(B \subseteq Y\). The resulting joint distribution \(P_{X,f}\) is then uniquely defined by its action on the “rectangles” \(A \times B\), \(A \subseteq X\) and \(B \subseteq Y\):

\[
P_{X,f}(A \times B) := \int_A P_{Y|X,f}(B|x)P_X(dx) = \int_A 1_{\{f(x) \in B\}}P_X(dx)
\]

Finally, let \(\mathcal{P} = \{P_{X,f} : f \in \mathcal{F}, P_X \in \mathcal{P}_X\}\). Finally, let \(\ell(y, u) := |y - u|^2\).
Now, fixing a probability distribution \( P \in \mathcal{P} \) is equivalent to fixing some \( P_X \in \mathcal{P}_X \) and some \( f \in \mathcal{F} \). A random element of \( Z = X \times Y \) drawn according to such a \( P \) has the form \((X, f(X))\), where \( X \sim P_X \). An i.i.d. sequence \((X_1, Y_1), \ldots, (X_n, Y_n)\) drawn according to \( P \) therefore has the form

\[(X_1, f(X_1)), \ldots, (X_n, f(X_n)),\]

which is precisely what we had in our discussion of function learning in the realizable case. Next, for any \( P = P_{X,f} \in \mathcal{P} \) and any other \( g \in \mathcal{F} \), we have

\[
L_{P_{X,f}}(g) = \int_{X \times Y} |y - g(x)|^2 P_{X,f}(dx, dy)
\]

\[
= \int_{X \times Y} 1_{\{y=f(x)\}} |y - g(x)|^2 P_X(dx)
\]

\[
= \int_X |f(x) - g(x)|^2 P_X(dx)
\]

\[
= \|f - g\|_{L^2(P_X)}^2,
\]

which is precisely the risk \( L_{P_X}(g,f) \) that we have considered in our function learning formulation earlier. Moreover,

\[
L^*_{P_X} = \inf_{g \in \mathcal{F}} L_{P_{X,f}}(g) = \inf_{g \in \mathcal{F}} \|f - g\|_{L^2(P_X)}^2 \equiv 0.
\]

Therefore,

\[
r_A(n, \varepsilon) = \sup_{P_{X,f} \in \mathcal{P}} P^n_{X,f} \left( Z^n \in \mathcal{Z}^n : L_{P_{X,f}}(\hat{f}_n) \geq L^*_{P_{X,f}} + \varepsilon \right)
\]

\[
= \sup_{P_X \in \mathcal{P}_X} \sup_{f \in \mathcal{F}} P^n_X \left( X^n \in \mathcal{X}^n : L_{P}(\hat{f}_n, f) \geq \varepsilon \right)
\]

\[
\equiv \bar{r}_A(n, \varepsilon, \mathcal{P}_X).
\]

Thus, the function learning problem in the realizable case can be covered under the model-free framework as well.

### 3.2. Learning to classify with noisy labels.

Consider the concept learning problem in the realizable case, except that now the labels \( Y_i \), which in the original problem had the form \( 1_{\{X_i \in C^*\}} \) for some target concept \( C^* \), are noisy. That is, if \( X_i \) is a training feature point, then the label \( Y_i \) may be “flipped” due to chance, independently of all other \( X_j \)'s, \( j \neq i \).

The precise formulation of this problem is as follows. Let \( X \) be a given feature space, let \( C \) be a concept class on it, and let \( \mathcal{P}_X \) be a class of probability distributions on \( X \). Suppose that Nature picks some distribution \( P_X \in \mathcal{P}_X \) of the features and some target concept \( C^* \in \mathcal{C} \). The training data are generated as follows. First, an i.i.d. sample \( X^n = (X_1, \ldots, X_n) \) is drawn according to some \( P_X \in \mathcal{P}_X \). Then the corresponding labels \( Y_1, \ldots, Y_n \in \{0, 1\} \) are generated as follows:

\[
Y_i = \begin{cases} 
1_{\{X_i \in C^*\}}, & \text{with probability } 1 - \eta \\
1 - 1_{\{X_i \in C^*\}}, & \text{with probability } \eta
\end{cases}
\]

independently of \( X^n \), \( \{Y_j\}_{j \neq i} \)

where \( \eta < 1/2 \) is the classification noise rate.
In other words, the best achievable performance when learning a concept to accuracy $\varepsilon$ are faced with the learning problem specified by $X$. PAC-learnability in the model-free setting). Of how to construct PAC learning algorithms (and the related question of when a hypothesis concept to accuracy $\eta$ on noisy labels with noise rate $\{Z \in C\}$ only if there was an error. In other words, $\times Y = X \times \{0, 1\}$ as follows. Let $X \sim P_X$, and for a given $C \in C$ consider the conditional probability of $Y = 1$ given $X = x$. If $x \in C$, then $Y = 1$ if and only if there was no error in the label; on the other hand, if $x \not\in C$, then $Y = 1$ if and only if there was an error. In other words, $P_{X,C}(1|x) = (1 - \eta)1_{\{x \in C\}} + \eta 1_{\{x \not\in C\}}.
\text{and} 
\begin{equation}
P_{X,C}(0|x) = (1 - \eta)1_{\{x \not\in C\}} + \eta 1_{\{x \in C\}}.
\end{equation}
Now, given a hypothesis $f = 1_{\{C'\}} \in \mathcal{F}$, we have $L_{P_{X,C}}(I_{C'}) = \int_{X \times Y} |y - I_{C'}(x)|^2 P_{X,C}(dx, dy)$. Computing this integral is straightforward: using Eqs. (3.18) and (3.19), we can write $\int_{X \times Y} |y - 1_{\{x \in C'\}}|^2 P_{X,C}(dx, dy) = (1 - \eta) \int_X |1_{\{x \in C\}} - 1_{\{x \in C'\}}|^2 P_X(dx) + \eta \int_X |1_{\{x \not\in C\}} - 1_{\{x \in C'\}}|^2 P_X(dx) = (1 - \eta) P_X(C \triangle C') + \eta P_X((C \triangle C')^c) = (1 - \eta) P_X(C \triangle C') + \eta (1 - P_X(C \triangle C')) = \eta + (1 - 2\eta) P_X(C \triangle C').$
From this, we have $L_{P_{X,C}}^*(\mathcal{F}) = \inf_{C' \in \mathcal{C}} L_{P_{X,C}}(I_{C'}) = \eta + (1 - 2\eta) \inf_{C' \in \mathcal{C}} P_X(C \triangle C') = \eta,$ where the infimum is achieved by letting $C' = C$. From this it follows that $L_{P_{X,C}}^*(C') \geq L_{P_{X,C}}^* + \varepsilon \quad \iff \quad P_{X,C}(C \triangle C') \geq \frac{\varepsilon}{1 - 2\eta}$
In other words, the best achievable performance when learning a concept to accuracy $\varepsilon$ from noisy labels with noise rate $\eta$ is equal to the best achievable performance when learning a concept to accuracy $\frac{\varepsilon}{1 - 2\eta}$ from noise-free labels.

4. Empirical risk minimization

Having formulated the model-free learning problem, we must now turn to the question of how to construct PAC learning algorithms (and the related question of when a hypothesis class is PAC-learnable in the model-free setting).

We will first start with a heuristic argument and then make it rigorous. Suppose we are faced with the learning problem specified by $(X, Y, U, \mathcal{P}, \mathcal{F}, \ell)$. Given a training set $Z^n = (Z_1, \ldots, Z_n)$, where each $Z_i = (X_i, Y_i)$ is independently drawn according to some
unknown $P \in \mathcal{P}$, what should we do? The first thing to note is that, for any hypothesis $f \in \mathcal{F}$, we can approximate its risk $L_P(f)$ by the empirical risk

$$
\frac{1}{n} \sum_{i=1}^{n} \ell(Y_i, f(X_i)),
$$

whose expectation w.r.t. the distribution of $Z^n$ is clearly equal to $L_P(f)$. In fact, since $\ell$ is bounded between 0 and 1, Hoeffding’s inequality tells us that

$$
\left| \frac{1}{n} \sum_{i=1}^{n} \ell(Y_i, f(X_i)) - L_P(f) \right| < \varepsilon \quad \text{with probability at least } 1 - 2e^{-2n\varepsilon^2}.
$$

We can express these statements more succinctly if we define, for each $f \in \mathcal{F}$, the function $\ell_f : Z \to [0, 1]$ by

$$
\ell_f(z) \equiv \ell_f(x, y) := \ell(y, f(x)).
$$

Then the empirical risk (3.20) is just the expectation of $\ell_f$ w.r.t. the empirical distribution $P_{Z^n}$:

$$
P_{Z^n}(\ell_f) = \frac{1}{n} \sum_{i=1}^{n} \ell(Y_i, f(X_i)),
$$

and, since $L_P(f) = \mathbb{E}_P[\ell(Y, f(X))] = P(\ell_f)$, we will have

$$
|P_{Z^n}(\ell_f) - P(\ell_f)| < \varepsilon \quad \text{with probability at least } 1 - 2e^{-2n\varepsilon^2}.
$$

Now, given the data $Z^n$ we can compute the empirical risks $P_{Z^n}(\ell_f)$ for every $f$ in our hypothesis class $\mathcal{F}$. Since (3.22) holds for each $f \in \mathcal{F}$ individually, we may intuitively claim that the empirical risk for each $f$ is a sufficiently accurate estimator of the corresponding true risk $L_P(f) \equiv P(\ell_f)$. Thus, a reasonable learning strategy would be to find any $\hat{f}_n \in \mathcal{F}$ that would minimize the empirical risk, i.e., take

$$
\hat{f}_n = \arg \min_{f \in \mathcal{F}} P_{Z^n}(\ell_f) = \arg \min_{f \in \mathcal{F}} \frac{1}{n} \sum_{i=1}^{n} \ell(Y_i, f(X_i)).
$$

The reason why we would expect something like (3.23) to work is as follows: if a given $f^*$ is a minimizer of $L_P(f) = P(\ell_f)$ over $\mathcal{F}$,

$$
f^* = \arg \min_{f \in \mathcal{F}} P(\ell_f),
$$

then its empirical risk, $P_{Z^n}(f^*)$, will be close to $L_P(f^*) = P(\ell_{f^*}) = L_P^*(\mathcal{F})$ with high probability. Moreover, it makes sense to expect that, in some sense, $\hat{f}_n$ defined in (3.23) would be “close” to $f^*$, resulting in something like

$$
P(\hat{f}_n) \approx P_{Z^n}(\hat{f}_n) \approx P_{Z^n}(f^*) \approx P(f^*)
$$

with high probability.

Unfortunately, this is not true in general. However, as we will now see, it is true under certain regularity conditions on the objects $\mathcal{P}$, $\mathcal{F}$, and $\ell$. In order to state these regularity conditions precisely, let us define the induced loss function class

$$
\mathcal{L}_\mathcal{F} := \{ \ell_f : f \in \mathcal{F} \}. $$
Each \( \ell_f \in \mathcal{L}_F \) corresponds to the hypothesis \( f \in \mathcal{F} \) via (3.21). Now, for any \( n \in \mathbb{N} \) and any \( \varepsilon > 0 \) let us define
\[
q(n, \varepsilon) := \sup_{P \in \mathcal{P}} P^n \left( Z^n \in Z^n : \sup_{f \in \mathcal{F}} |P^n(\ell_f) - P(\ell_f)| \geq \varepsilon \right).
\]
For a fixed \( P \in \mathcal{P} \), quantity \( \sup_{f \in \mathcal{F}} |P^n(\ell_f) - P(\ell_f)| \) is the worst-case deviation between the empirical means \( P^n(\ell_f) \) and their expectations \( P(\ell_f) \) over the entire hypothesis class \( \mathcal{F} \). Given \( P \), we say that an i.i.d. sample \( Z^n \in Z^n \) is “bad” if there exists at least one \( f \in \mathcal{F} \), for which
\[
|P^n(\ell_f) - P(\ell_f)| \geq \varepsilon.
\]
Equivalently, a sample is bad if
\[
\sup_{f \in \mathcal{F}} |P^n(\ell_f) - P(\ell_f)| \geq \varepsilon.
\]
The quantity \( q(n, \varepsilon) \) then compensates for the fact that \( P \) is unknown by considering the worst case over the entire class \( \mathcal{P} \). With this in mind, we make the following definition:

**Definition 3.6.** We say that the induced class \( \mathcal{L}_F \) has the uniform convergence of empirical means (UCEM) property w.r.t. \( \mathcal{P} \) if
\[
\lim_{n \to \infty} q(n, \varepsilon) = 0
\]
for every \( \varepsilon > 0 \).

**Theorem 3.2.** If the induced class \( \mathcal{L}_F \) has the UCEM property, then the empirical risk minimization (ERM) algorithm of (3.23) is PAC.

**Proof.** Fix \( \varepsilon, \delta > 0 \). We will now show that we can find a sufficiently large \( n(\varepsilon, \delta) \), such that \( r_{\mathcal{A}}(n, \varepsilon) < \delta \) for all \( n \geq n(\varepsilon, \delta) \), where \( r_{\mathcal{A}}(n, \varepsilon) \) is defined in (3.17).

Let \( f^* \in \mathcal{F} \) minimize the true risk w.r.t. \( P \), i.e., \( P(f^*) = L^*_P(\mathcal{F}) \). For any \( n \), we have
\[
L_P(\hat{f}_n) - L^*_P = P(\ell_{\hat{f}_n}) - P(f^*)
\]
\[
= \underbrace{P(\ell_{\hat{f}_n}) - P^n(\ell_{\hat{f}_n})}_T_1 + \underbrace{P^n(\ell_{\hat{f}_n}) - P^n(\ell_{f^*})}_T_2 + \underbrace{P^n(\ell_{f^*}) - P(\ell_{f^*})}_T_3,
\]
where in the second line we have added and subtracted \( P^n(\ell_{\hat{f}_n}) \) and \( P^n(\ell_{f^*}) \). We will now analyze the behavior of the three terms, \( T_1 \), \( T_2 \), and \( T_3 \). Since \( \hat{f}_n \) minimizes the empirical risk \( P^n(\ell_f) \) over all \( f \in \mathcal{F} \), we will have
\[
T_2 = P^n(\ell_{\hat{f}_n}) - P^n(\ell_{f^*}) \leq 0.
\]
Next,
\[
T_1 = P(\ell_{\hat{f}_n}) - P^n(\ell_{\hat{f}_n}) \leq \sup_{f \in \mathcal{F}} |P^n(\ell_f) - P(\ell_f)| \leq \sup_{f \in \mathcal{F}} |P^n(\ell_f) - P(\ell_f)|,
\]
and the same upper bound holds for \( T_3 \). Hence,
\[
L_P(\hat{f}_n) - L^*_P(\mathcal{F}) \leq 2 \sup_{f \in \mathcal{F}} |P^n(\ell_f) - P(\ell_f)|.
\]

37
Now, since $\mathcal{L}_F$ has the UCEM property, we can find some sufficiently large $n_0(\varepsilon, \delta)$, such that

$$q(n, \varepsilon/2) = \sup_{P \in \mathcal{P}} P^n\left(Z^n \in Z^n : \sup_{f \in F} |P_{Z^n}(\ell_f) - P(\ell_f)| \geq \varepsilon/2\right) < \delta, \quad \forall n \geq n_0(\varepsilon, \delta).$$

From this it follows that, for all $n \geq n_0(\varepsilon, \delta)$, we will have

$$P^n\left(Z^n : \sup_{f \in \mathcal{F}} |P_{Z^n}(\ell_f) - P(\ell_f)| \geq \varepsilon/2\right) < \delta, \quad \forall P \in \mathcal{P}.$$ 

From (3.25), we see that

$$L_P(\hat{f}_n) \geq L^*_P(\mathcal{F}) + \varepsilon \quad \implies \quad \sup_{f \in \mathcal{F}} |P_{Z^n}(\ell_f) - P(\ell_f)| \geq \varepsilon/2$$

for all $n$. However, for all $n \geq n_0(\varepsilon, \delta)$ the latter event will occur with probability at most $\delta$, no matter which $P$ is in effect. Therefore, for all $n \geq n_0(\varepsilon, \delta)$ we will have

$$r_A(n, \varepsilon) = \sup_{P \in \mathcal{P}} P^n \left(Z^n : L_P(\hat{f}_n) \geq L^*_P(\mathcal{F}) + \varepsilon\right)$$

$$\leq \sup_{P \in \mathcal{P}} P^n \left(Z^n : \sup_{f \in \mathcal{F}} |P_{Z^n}(\ell_f) - P(\ell_f)| \geq \varepsilon/2\right)$$

$$\equiv q(n, \varepsilon/2)$$

$$< \delta,$$

which is precisely what we wanted to show. Thus, $r_A(n, \varepsilon) \to 0$ as $n \to \infty$ for every $\varepsilon > 0$, which means that the ERM algorithm is PAC. \hfill \Box

This theorem shows that the UCEM property of the induced class $\mathcal{L}_F$ is a sufficient condition for the ERM algorithm to be PAC. Now the whole affair rests on us being able to establish the UCEM property for various “interesting” and “useful” problem specifications. This will be our concern in the chapters ahead. However, let me give you a hint of what to expect. In many cases, we will be able to show that the induced class $\mathcal{L}_F$ is so well-behaved that the bound

$$\mathbb{E}_P^n \left[ \sup_{f \in \mathcal{F}} |P_{Z^n}(\ell_f) - P(\ell_f)| \right] \leq \frac{C_{\mathcal{F}, \ell}}{\sqrt{n}}$$

holds for every $P$, where $C_{\mathcal{F}, \ell} > 0$ is some constant that depends only on the characteristics of the hypothesis class $\mathcal{F}$ and the loss function $\ell$. Since $\ell_f$ is bounded between 0 and 1, the function

$$g(Z^n) := \sup_{f \in \mathcal{F}} |P_{Z^n}(\ell_f) - P(\ell_f)|$$

has bounded differences with constants $c_1 = \ldots = c_n = 1/n$. McDiarmid’s inequality then tells us that, for any $t > 0$,

$$P^n \left( g(Z^n) - \mathbb{E}g(Z^n) \geq t \right) \leq e^{-2nt^2}.$$ 

Let

$$n_0(\varepsilon, \delta) := \max \left\{ \frac{4C_{\mathcal{F}, \ell}^2}{\varepsilon^2}, \frac{2}{\varepsilon^2} \log \left( \frac{1}{\delta} \right) \right\} + 1.$$
Then for any \( n \geq n_0(\varepsilon, \delta) \)

\[
P^n\left(g(Z^n) \geq \varepsilon\right) = P^n\left(g(Z^n) - \mathbb{E}g(Z^n) \geq \varepsilon - \mathbb{E}g(Z^n)\right)
\leq P^n\left(g(Z^n) - \mathbb{E}g(Z^n) \geq \varepsilon - \frac{C_{\mathcal{F},\ell}}{\sqrt{n}}\right)
\leq P^n\left(g(Z^n) - \mathbb{E}g(Z^n) \geq \frac{\varepsilon}{2}\right)
\leq e^{-n\varepsilon^2/2}
< \delta
\]

because of (3.26)

\[\leq e^{-n\varepsilon^2/2}\]

because \( n > \frac{4C_{\mathcal{F},\ell}^2}{\varepsilon^2} \)

using (3.27) with \( t = \varepsilon/2 \)

because \( n > \frac{2}{\varepsilon^2} \log \left(\frac{1}{\delta}\right) \)

for any probability distribution \( P \) over \( Z = X \times Y \). Thus, we have derived a very important fact: If the induced loss class \( \mathcal{L}_X \) satisfies (3.26), then (a) it has the UCEM property, and consequently is model-free learnable using the ERM algorithm, and (b) the sample complexity is polynomial in \( 1/\varepsilon \) and logarithmic in \( 1/\delta \). Our next order of business will be to derive sufficient conditions on \( \mathcal{F} \) and \( \ell \) for something like (3.26) to hold.
CHAPTER 4

Empirical Risk Minimization: Abstract risk bounds and Rademacher averages

In the last chapter, we have left off with a theorem that gave a sufficient condition for the Empirical Risk Minimization (ERM) algorithm

\[
\hat{f}_n = \arg \min_{f \in \mathcal{F}} P_{Z^n}(\ell_f)
\]

(4.1)

\[
= \arg \min_{f \in \mathcal{F}} \frac{1}{n} \sum_{i=1}^{n} \ell(Y_i, f(X_i))
\]

(4.2)

to be PAC for a given learning problem with hypothesis space \( \mathcal{F} \) and loss function \( \ell \). This condition pertained to the behavior of the uniform deviation of empirical means from true means over the induced class \( \mathcal{L}_\mathcal{F} = \{ \ell_f : f \in \mathcal{F} \} \). Specifically, we proved that ERM is a PAC algorithm if

\[
\lim_{n \to \infty} \sup_{P \in \mathcal{P}} P^n \left( \sup_{f \in \mathcal{F}} |P_{Z^n}(\ell_f) - P(\ell_f)| \geq \varepsilon \right) = 0, \quad \forall \varepsilon > 0,
\]

(4.3)

where \( \mathcal{P} \) is the class of probability distributions generating the training data.

1. An abstract framework for ERM

To study ERM in a general framework, we will adopt a simplified notation often used in the literature. We have a space \( Z \) and a class \( \mathcal{F} \) of functions \( f : Z \to [0, 1] \). Let \( \mathcal{P}(Z) \) denote the space of all probability distributions on \( Z \). For each sample size \( n \), the training data are in the form of an \( n \)-tuple \( Z^n = (Z_1, \ldots, Z_n) \) of \( Z \)-valued random variables drawn according to some unknown \( P \in \mathcal{P} \). For each \( P \), we can compute the expected risk of any \( f \in \mathcal{F} \) by

\[
P(f) = E_P f(Z) = \int_Z f(z) P(dz).
\]

(4.4)

The minimum risk over \( \mathcal{F} \) is

\[
L^*_P(\mathcal{F}) := \inf_{f \in \mathcal{F}} P(f).
\]

(4.5)

A learning algorithm is a sequence \( \mathcal{A} = \{ A_n \}_{n \geq 1} \) of mappings \( A_n : Z^n \to \mathcal{F} \), and the objective is to ensure that

\[
P(\hat{f}_n) \approx L^*_P(\mathcal{F}) \quad \text{eventually with high probability}.
\]

(4.6)
The ERM algorithm works by taking
\begin{equation}
\hat{f}_n = \arg\min_{f \in \mathcal{F}} P_{Z^n}(f)
\end{equation}
\begin{equation}
= \arg\min_{f \in \mathcal{F}} \frac{1}{n} \sum_{i=1}^{n} f(Z_i).
\end{equation}
This way of writing down our problem hides most of the ingredients that were specified in Haussler’s framework of model-free learning, so it is important to keep in mind that $Z$ is an input/output pair $(X,Y)$ and the functions $f \in \mathcal{F}$ are really the induced losses for some loss function $\ell$ and hypothesis class $\mathcal{G}$. However, recalling our discussion of unsupervised learning problems in Chapter 1, we do not insist on splitting $Z$ into input $X$ and output $Y$, nor do we need to imagine any particular structure for $f$.

We have already seen that the consistency of ERM hinges on the uniform deviation behavior of empirical means in $\mathcal{F}$. In order to have a clean way of keeping track of all the relevant quantities, let us introduce some additional notation. First of all, we need a way of comparing the behavior of any two probability distributions $P$ and $P'$ on the class $\mathcal{F}$. A convenient way of doing this is through the $\mathcal{F}$-seminorm
\begin{equation}
\|P - P'\|_{\mathcal{F}} := \sup_{f \in \mathcal{F}} |P(f) - P'(f)|
\end{equation}
\begin{equation}
= \sup_{f \in \mathcal{F}} |\mathbb{E}_P f - \mathbb{E}_{P'} f|
\end{equation}
\begin{equation}
= \sup_{f \in \mathcal{F}} \left| \int_{Z} f(z)P(dz) - \int_{Z} f(z)P'(dz) \right|.
\end{equation}
We say that $\| \cdot \|_{\mathcal{F}}$ is a seminorm because it has all the properties of a norm (in particular, it satisfies the triangle inequality), but it may happen that $\|P - P'\|_{\mathcal{F}} = 0$ for $P \neq P'$. Next, given a random sample $Z^n$ we define the uniform deviation
\begin{equation}
\Delta_n(Z^n) := \|P_{Z^n} - P\|_{\mathcal{F}} \equiv \sup_{f \in \mathcal{F}} |P_{Z^n}(f) - P(f)|.
\end{equation}
To keep things simple, we do not indicate the underlying distribution $P$ or the function class $\mathcal{F}$ explicitly. We will do this from now on, unless some confusion is possible, in which case we will use appropriate indices. Thus, we will write $L(f)$, $L^*(\mathcal{F})$, etc., and you should always keep in mind that all expectations are computed w.r.t. the (unknown) data-generating distribution $P \in \mathcal{P}(Z)$. In the same spirit, we will denote by $P_n(f)$ the empirical risk of $f$ on the sample $Z^n$:
\begin{equation}
P_n(f) = P_{Z^n}(f) = \frac{1}{n} \sum_{i=1}^{n} f(Z_i).
\end{equation}
The following result is key to understanding the role of the uniform deviations $\Delta_n(Z^n)$ in controlling the performance of the ERM algorithm.

**Proposition 4.1.** The ERM algorithm satisfies the following inequalities:
\begin{equation}
P(\hat{f}_n) \leq L^*(\mathcal{F}) + 2\Delta_n(Z^n)
\end{equation}
\begin{equation}
P(\hat{f}_n) \leq P_n(\hat{f}_n) + \Delta_n(Z^n).
\end{equation}
Proof. We have already proved the two inequalities of the proposition in the last lecture, except now they are written in our new abstract notation. Let us give the proof again in order to get comfortable with the notation. Let $f^*$ be any minimizer of $P(f)$ over $\mathcal{F}$. Then

\begin{align}
& P(\hat{f}_n) - L^*(\mathcal{F}) = P(\hat{f}_n) - P(f^*) \\
& = P(\hat{f}_n) - P_n(\hat{f}_n) + P_n(\hat{f}_n) - P_n(f^*) + P_n(f^*) - P(f^*),
\end{align}

where $P_n(\hat{f}_n) - P_n(f^*) \leq 0$ by definition of ERM,

\begin{align}
P(\hat{f}_n) - P_n(\hat{f}_n) \leq \sup_{f \in \mathcal{F}} [P_n(f) - P(f)] \leq \|P_n - P\|_F = \Delta_n(Z^n),
\end{align}

and the same holds for $P_n(f^*) - P(f^*)$. This proves both (4.14) and (4.15). \qed

The bound (4.14) says that, if the uniform deviation $\Delta_n(Z^n)$ is small, then the expected risk of the ERM hypothesis will be close to the minimum risk $L^*(\mathcal{F})$; in addition, the bound (4.15) says that the empirical estimate $P_n(\hat{f}_n)$ is an accurate estimate of the generalization performance of $\hat{f}_n$. Both bounds suggest that the success of ERM depends on how small the uniform deviation $\Delta_n(Z^n)$ can be. Thus, we need to develop tools for analyzing the behavior of $\Delta_n(Z^n)$.

2. Bounding the uniform deviation: Rademacher averages

It turns out that the behavior of the uniform deviation $\Delta_n(Z^n)$ is closely connected to how the values of the functions $f \in \mathcal{F}$ on randomly selected $n$-tuples $Z^n$ correlate with random signs. Intuitively, this can be motivated as follows. In order for ERM to succeed, the function class $\mathcal{F}$ has to be “discriminating;” we should be able to clearly separate all near-minimizers of the empirical risk from functions whose empirical risks (and hence expected risks) are high, but only if the sample is representative of the true data-generating distribution. If the class $\mathcal{F}$ is discriminating not only on the actual sample, but also on its random perturbations, then we cannot expect the empirical risks to truly reflect the generalization ability of the functions in $\mathcal{F}$. As we will soon see, the degree of correlation of the “projections” of $\mathcal{F}$ onto random samples with random signs is captured by the quantities known as the Rademacher averages.

First, we need some preparatory results. Let $Y$ be a real-valued random variable. We say that it is symmetric if $-Y$ has the same distribution as $Y$. This is equivalent to saying that

\begin{align}
P(Y \geq a) = P(Y \leq -a), \quad \forall a \in \mathbb{R}.
\end{align}

A random variable $\sigma$ taking values $-1$ or $+1$ with probability $1/2$ is called a Rademacher random variable.

Lemma 4.1. Let $U$ and $U'$ be two i.i.d. real-valued random variables. Then $Y = U - U'$ is symmetric.
Proof. Let $F(u) = P(U \geq u)$. Then
\begin{align*}
P(Y \geq a) &= P(U - U' \geq a) \\
&= E\left[E\left[1_{\{U - U' \geq a\}}|U'\right]\right] \\
&= EF(a + U') \\
&= EF(a + U),
\end{align*}
where the last line is because $U$ and $U'$ are i.i.d. An analogous calculation for $P(Y \leq -a)$ gives the same result. □

Lemma 4.2. Let $Y$ be a symmetric random variable, and let $\sigma$ be a Rademacher random variable independent of $Y$. Then $W = \sigma Y$ has the same distribution as $Y$.

Proof. Direct calculation:
\begin{align*}
P(W \leq a) &= \frac{1}{2}P(Y \leq a) + \frac{1}{2}P(Y \geq -a) = P(Y \leq a),
\end{align*}
where the second step is due to the symmetry of $Y$. Since this holds for an arbitrary $a \in \mathbb{R}$, we conclude that $W$ has the same distribution as $Y$. □

Corollary 4.1. Let $Y_1, \ldots, Y_n$ be $n$ independent symmetric random variables, and let $\sigma_1, \ldots, \sigma_n$ be independent Rademacher random variables that are also independent of the $Y_i$'s. Then the sum $Y_1 + \ldots + Y_n$ has the same distribution as $\sigma_1 Y_1 + \ldots + \sigma_n Y_n$.

Now we are ready to define Rademacher averages.

Definition 4.1. The Rademacher average of a bounded set $A \subset \mathbb{R}^n$ is
\begin{align*}
R_n(A) := E\sup_{a \in A}\left|\frac{1}{n}\sum_{i=1}^{n}\sigma_i a_i\right|,
\end{align*}
where the expectation is over $n$ i.i.d. Rademacher random variables $\sigma_1, \ldots, \sigma_n$.

Now consider a class $\mathcal{F}$ of functions $f : Z \to [0, 1]$ from our formulation of the ERM problem. The key result, which we will now prove, is that the uniform deviations $\Delta_n(Z^n)$ are controlled by the Rademacher averages of the random sets
\begin{align*}
\mathcal{F}(Z^n) := \{(f(Z_1), \ldots, f(Z_n)) : f \in \mathcal{F}\}.
\end{align*}
A useful way to think about $\mathcal{F}(Z^n)$ is as a “projection” of $\mathcal{F}$ onto the random sample $Z^n$.

Theorem 4.1. Fix a space $Z$ and let $\mathcal{F}$ be a class of functions $f : Z \to [0, 1]$. Then for any $P \in \mathcal{P}(Z)$
\begin{align*}
E\Delta_n(Z^n) \leq 2ER_n(\mathcal{F}(Z^n)).
\end{align*}
Proof. The proof uses a clever technique known as “symmetrization,” which goes back to the seminal work of Vapnik and Chervonenkis [VC71], but in its modern form is due to Giné and Zinn [GZ84]. The main idea is as follows. Consider a random i.i.d. sample $Z^n$ from $P$ and introduce an independent “ghost” sample $\overline{Z^n} = (Z_1, \ldots, Z_n)$ from the same $P$. ...
We will denote expectations w.r.t. $Z^n$ by $\mathbb{E}$. Let $\overline{P}_n$ denote the empirical distribution of $Z^n$.

Then for any bounded function $g : Z \to \mathbb{R}$ we can write

\[(4.28)\quad P(g) = \mathbb{E} \left[ \frac{1}{n} \sum_{i=1}^{n} g(Z_i) \right] = \mathbb{E} \overline{P}_n(g).\]

With this, we have

\[(4.29)\quad \Delta_n(Z^n) = \|P_n - P\|_{\mathcal{F}} = \sup_{f \in \mathcal{F}} |P_n(f) - P(f)|\]
\[(4.30)\quad = \sup_{f \in \mathcal{F}} |P_n(f) - \mathbb{E} \overline{P}_n(f)|\]
\[(4.31)\quad \leq \sup_{f \in \mathcal{F}} \mathbb{E} |P_n(f) - \overline{P}_n(f)|\]
\[(4.32)\quad \leq \mathbb{E} \sup_{f \in \mathcal{F}} |P_n(f) - \overline{P}_n(f)|,\]

where the first inequality uses convexity of the absolute value function, while the second is because $\sup \mathbb{E}[: \leq \mathbb{E} \sup[:$. Now let us take expectations of both sides w.r.t. $Z^n$ to get

\[(4.34)\quad \mathbb{E}\Delta_n(Z^n) \leq \mathbb{E} \sup_{f \in \mathcal{F}} |P_n(f) - \overline{P}_n(f)|,\]

where now the expectation on the right is w.r.t. both $Z^n$ and $\overline{Z}^n$, which are independent of each other. Let us inspect the difference $P_n(f) - \overline{P}_n(f)$:

\[(4.35)\quad P_n(f) - \overline{P}_n(f) = \frac{1}{n} \sum_{i=1}^{n} [f(Z_i) - f(\overline{Z}_i)].\]

For each $i$ $Z_i$ and $\overline{Z}_i$ are i.i.d., so the differences $f(Z_i) - f(\overline{Z}_i)$ are symmetric by Lemma 4.1. Introducing $n$ i.i.d. Rademacher random variables $\sigma_1, \ldots, \sigma_n$ independent of $Z^n$ and $\overline{Z}^n$, from Corollary 4.1 we know that

\[(4.36)\quad \frac{1}{n} \sum_{i=1}^{n} [f(Z_i) - f(\overline{Z}_i)] \overset{d}{=} \frac{1}{n} \sum_{i=1}^{n} \sigma_i [f(Z_i) - f(\overline{Z}_i)],\]

where $\overset{d}{=} \text{means "equality in distribution."}$ The same holds if we take the supremum of both sides over $f \in \mathcal{F}$. Hence,

\[(4.37)\quad \mathbb{E} \sup_{f \in \mathcal{F}} |P_n(f) - \overline{P}_n(f)| = \mathbb{E} \sup_{f \in \mathcal{F}} \left| \frac{1}{n} \sum_{i=1}^{n} [f(Z_i) - f(\overline{Z}_i)] \right|
\[(4.38)\quad \overset{d}{=} \mathbb{E} \sup_{f \in \mathcal{F}} \left| \frac{1}{n} \sum_{i=1}^{n} \sigma_i [f(Z_i) - f(\overline{Z}_i)] \right|,\]

44
where in the last line the expectation is over $Z^n$, $\overline{Z}^n$, and $\sigma^n = (\sigma_1, \ldots, \sigma_n)$. Now note that
\[
E \sup_{f \in F} \left| \frac{1}{n} \sum_{i=1}^{n} \sigma_i [f(Z_i) - f(\overline{Z}_i)] \right| \leq E \sup_{f \in F} \left| \frac{1}{n} \sum_{i=1}^{n} \sigma_i f(Z_i) \right| + E \sup_{f \in F} \left| \frac{1}{n} \sum_{i=1}^{n} \sigma_i f(\overline{Z}_i) \right|
\]
(4.39)
\[
= 2E \sup_{f \in F} \left| \frac{1}{n} \sum_{i=1}^{n} \sigma_i f(Z_i) \right|,
\]
(4.40)
where the first line is by the triangle inequality and the second line uses the fact that $Z^n$ has the same distribution as $\overline{Z}^n$. Now, since $Z^n$ and $\sigma^n$ are independent,
\[
E \sup_{f \in F} \left| \frac{1}{n} \sum_{i=1}^{n} \sigma_i f(Z_i) \right| = E Z^n \, E_{\sigma^n} \sup_{f \in F} \left| \frac{1}{n} \sum_{i=1}^{n} \sigma_i f(Z_i) \right| = E R_n(F(Z^n)).
\]
(4.41)
This completes the proof.

The above theorem implies the following key result on ERM:

**Corollary 4.2.** For any $P \in \mathcal{P}(Z)$ and any $n$, the ERM hypothesis $\hat{f}_n$ satisfies the bound
\[
P(\hat{f}_n) \leq L^*(F) + 4E R_n(F(Z^n)) + \sqrt{\frac{2\log(1/\delta)}{n}}
\]
(4.42)
with probability at least $1 - \delta$.

**Proof.** From Theorem 4.1 it follows that, for any $t > 0$,
\[
P \left( \Delta_n(Z^n) \geq 2E R_n(F(Z^n)) + t \right) \leq P \left( \Delta_n(Z^n) \geq E \Delta_n(Z^n) + t \right).
\]
(4.43)
The uniform deviation $\Delta(Z^n)$ has the bounded differences property with $c_1 = \ldots = c_n = 1/n$. Hence, by McDiarmid’s inequality
\[
P \left( \Delta_n(Z^n) \geq E \Delta_n(Z^n) + t \right) \leq e^{-2nt^2}.
\]
Letting $t = \sqrt{\frac{\log(1/\delta)}{2n}}$, we see that
\[
\Delta_n(Z^n) \leq E \Delta_n(Z^n) + \sqrt{\frac{\log(1/\delta)}{2n}}
\]
with probability at least $1 - \delta$. Together with (4.43), this implies that
\[
\Delta_n(Z^n) \leq 2E R_n(F(Z^n)) + \sqrt{\frac{\log(1/\delta)}{2n}}
\]
(4.44)
with probability at least $1 - \delta$. Combining this with the first bound of Proposition 4.1, we conclude that
\[
P(\hat{f}_n) \leq L^*(F) + 4E R_n(F(Z^n)) + \sqrt{\frac{2\log(1/\delta)}{n}}
\]
(4.45)
with probability at least $1 - \delta$. □
3. Structural results for Rademacher averages

The results developed above highlight the fundamental role played by Rademacher averages in bounding the generalization error of the ERM algorithm. In order to use these bounds, we need to get a better handle on the behavior of Rademacher averages.

**Lemma 4.3 (Basic properties of Rademacher averages).** Let $A$ and $B$ be bounded subsets of $\mathbb{R}^n$, and let $c \in \mathbb{R}$ be a constant. Then

\begin{align}
R_n(A \cup B) &\leq R_n(A) + R_n(B) \\
R_n(cA) &\leq |c|R_n(A) \\
R_n(A + B) &\leq R_n(A) + R_n(B),
\end{align}

where $cA := \{ca : a \in A\}$ and $A + B := \{a + b : a \in A, b \in B\}$. Moreover, let

\begin{align}
\text{conv } A &:= \left\{ \sum_{m=1}^{N} c_m a_m : N \in \mathbb{N}; a_m \in A; c_m \geq 0, \forall m; \sum_{m=1}^{N} c_m = 1 \right\} \\
\text{absconv } A &:= \left\{ \sum_{m=1}^{N} c_m a_m : N \in \mathbb{N}; a_m \in A; \sum_{m=1}^{n} |c_m| \leq 1 \right\}
\end{align}

be the convex hull of $A$ and

be the absolute convex hull of $A$. Then

\begin{align}
R_n(A) = R_n(\text{conv } A) = R_n(\text{absconv } A).
\end{align}

**Proof.** The proof is by direct calculation. First of all, by double-counting,

\begin{align}
R_n(A \cup B) &= \mathbb{E} \sup_{v \in A \cup B} \left| \frac{1}{n} \sum_{i=1}^{n} \sigma_i v_i \right| \\
&\leq \mathbb{E} \sup_{a \in A} \left| \frac{1}{n} \sum_{i=1}^{n} \sigma_i a_i \right| + \mathbb{E} \sup_{b \in B} \left| \frac{1}{n} \sum_{i=1}^{n} \sigma_i b_i \right| \\
&= R_n(A) + R_n(B).
\end{align}

The case of $cA$ is obvious. For $A + B$,

\begin{align}
R_n(A + B) &= \mathbb{E} \sup_{v \in A + B} \left| \frac{1}{n} \sum_{i=1}^{n} \sigma_i v_i \right| \\
&= \mathbb{E} \sup_{a \in A, b \in B} \left| \frac{1}{n} \sum_{i=1}^{n} \sigma_i (a_i + b_i) \right| \\
&\leq \mathbb{E} \sup_{a \in A} \left| \frac{1}{n} \sum_{i=1}^{n} \sigma_i a_i \right| + \mathbb{E} \sup_{b \in B} \left| \frac{1}{n} \sum_{i=1}^{n} \sigma_i b_i \right| \\
&= R_n(A) + R_n(B),
\end{align}

where the third step uses the triangle inequality.
Finally, consider the absolute convex hull of $\mathcal{A}$. Since $\mathcal{A} \subset \text{absconv} \mathcal{A}$, $R_n(\mathcal{A}) \leq R_n(\text{absconv} \mathcal{A})$. On the other hand, fix some $N \in \mathbb{N}$ and $N$ real numbers $c_1, \ldots, c_N$ such that $\sum_{m=1}^{N} |c_m| = 1$, and consider the set

$$c_1 \mathcal{A} + \ldots + c_N \mathcal{A} \equiv \left\{ c_1 a_1 + \ldots + c_N a_N : a_1, \ldots, a_N \in \mathcal{A} \right\}.$$  

Then

$$R_n(c_1 \mathcal{A} + \ldots + c_N \mathcal{A}) \leq \sum_{i=1}^{N} |c_i| R_n(\mathcal{A}) \leq R_n(\mathcal{A}).$$

Since $\text{absconv} \mathcal{A}$ is the union of all sets of the form (4.59) for all choices of $N$ and $\{c_m\}_{m=1}^{N}$, we see that $R_n(\text{absconv} \mathcal{A}) \leq R_n(\mathcal{A})$. Therefore, $R_n(\mathcal{A}) = R_n(\text{absconv} \mathcal{A})$. Since $\mathcal{A} \subset \text{conv} \mathcal{A} \subset \text{absconv} \mathcal{A}$, the same equality holds for the convex hull of $\mathcal{A}$.

The properties listed in the lemma show what happens to Rademacher averages when we form combinations of sets. This will be useful to us later, when we talk about hypothesis classes made up of simpler classes by means of operations like set-theoretic unions, intersections, complements or differences, logical connectives, or convex and linear combinations.

The next result, often referred to as the Finite Class Lemma, is very important:

**Lemma 4.4** (Finite class lemma). If $\mathcal{A} = \{a^{(1)}, \ldots, a^{(N)}\} \subset \mathbb{R}^n$ is a finite set with $\|a^{(j)}\| \leq L$ for all $j = 1, \ldots, N$ and $N \geq 2$, then

$$R_n(\mathcal{A}) \leq \frac{2L\sqrt{\log N}}{n}.$$  

**Proof.** Let $\sigma^n$ be $n$ i.i.d. Rademacher variables, and for every $j \in 1, \ldots, N$ let

$$Y_j := \frac{1}{n} \sum_{i=1}^{n} \sigma_i a_i^{(j)}.$$

Then for any $s > 0$

$$\mathbf{E}e^{sY_j} = \mathbf{E} \exp \left( \frac{s}{n} \sum_{i=1}^{n} \sigma_i a_i^{(j)} \right) = \prod_{i=1}^{n} \mathbf{E} e^{s \sigma_i a_i^{(j)} / n},$$

where the second step uses the fact that $\sigma^n$ are i.i.d. For each $i$, the random variable $\sigma_i a_i^{(j)}$ has zero mean and is bounded between $-a_i^{(j)}$ and $a_i^{(j)}$, so by the Hoeffding bound we have

$$\mathbf{E} e^{s \sigma_i a_i^{(j)} / n} \leq \exp \left( \frac{s^2 \|a_i^{(j)}\|^2}{2n^2} \right).$$

Therefore,

$$\mathbf{E} e^{sY_j} \leq \prod_{i=1}^{n} \exp \left( \frac{s^2 \|a_i^{(j)}\|^2}{2n^2} \right) = \exp \left( \frac{s^2}{2n^2} \sum_{i=1}^{n} |a_i^{(j)}|^2 \right) = \exp \left( \frac{s^2 \|a^{(j)}\|^2}{2n^2} \right) \leq \exp \left( \frac{s^2 L^2}{2n^2} \right).$$

Repeating the same argument for each $-Y_j$, we see that

$$\mathbf{E} e^{-sY_j} \leq \exp \left( \frac{s^2 L^2}{2n^2} \right).$$
Now we recall the following statement, which was given as a homework problem in Spring 2011 at Duke University\textsuperscript{1}: Let $U_1, \ldots, U_K$ be $K$ random variables (not necessarily independent) that are subgaussian with parameter $v > 0$, i.e.,

\begin{equation}
\mathbb{E}[e^{s U_k}] \leq e^{s^2 v^2 / 2}, \quad \forall s > 0.
\end{equation}

Then

\begin{equation}
\mathbb{E} \left[ \max_{1 \leq k \leq K} U_k \right] \leq v \sqrt{2 \log K}.
\end{equation}

Consider now the $2N$ random variables $Y_1, -Y_1, \ldots, Y_N, -Y_N$. According to (4.65) and (4.66), they are subgaussian with parameter $v = L/n$. Hence,

\begin{equation}
\mathbb{E} \left[ \max_{1 \leq j \leq N} |Y_j| \right] = \mathbb{E} \left[ \max (Y_1, -Y_1, \ldots, Y_N, -Y_N) \right] \leq \frac{L \sqrt{2 \log(2N)}}{n} \leq \frac{2L \sqrt{\log N}}{n},
\end{equation}

where the last step uses the fact that, since $N \geq 2$, $2N \leq N^2$. Finally,

\begin{equation}
R_n(A) = \mathbb{E} \left[ \max_{1 \leq j \leq N} \left| \frac{1}{n} \sum_{i=1}^{n} \sigma_i a_i(j) \right| \right] = \mathbb{E} \left[ \max_{1 \leq j \leq N} |Y_j| \right] \leq \frac{2L \sqrt{\log N}}{n},
\end{equation}

which is what we wanted to prove. \hfill \square

We will start exploring the implications of the Finite Class Lemma more fully in the next lecture, but we can give a brief preview here. Consider a learning problem of the type described in Section 1 in the special case when $\mathcal{F}$ consists of binary-valued functions on $\mathbb{Z}$, i.e., $\mathcal{F} = \{f : \mathbb{Z} \to \{0, 1\}\}$. From Theorem 4.1, we know that

\begin{equation}
\mathbb{E} \Delta_n(Z^n) \leq 2\mathbb{E} R_n(\mathcal{F}(Z^n)),
\end{equation}

where

\begin{equation}
\mathcal{F}(Z^n) := \{(f(Z_1), \ldots, f(Z_n)) : f \in \mathcal{F}\}.
\end{equation}

Note that because each $f$ can take values 0 or 1, $\mathcal{F}(Z^n) \subseteq \{0, 1\}^n$. Moreover, since for any $Z^n \in \mathbb{Z}^n$ and any $f \in \mathcal{F}$ we have

\begin{equation}
\sqrt{n} \sum_{i=1}^{n} |f(Z_i)|^2 \leq \sqrt{n},
\end{equation}

the set $\mathcal{F}(Z^n)$ for a fixed $Z^n$ satisfies the conditions of the Finite Class Lemma with $N = |\mathcal{F}(Z^n)| \leq 2^n$ and $L = \sqrt{n}$. Hence,

\begin{equation}
R_n(\mathcal{F}(Z^n)) \leq 2\sqrt{\frac{\log |\mathcal{F}(Z^n)|}{n}}.
\end{equation}

In general, since $\log |\mathcal{F}(Z^n)| \leq n$, the bound just says that $R_n(\mathcal{F}(Z^n)) \leq 2$, which is not that useful. However, as we will see in the next few lectures, for a broad range of binary function classes $\mathcal{F}$ it will not be possible to pick out every single element in $\{0, 1\}^n$ by taking

\footnotesize
\textsuperscript{1}See Problem 2 in http://maxim.ece.illinois.edu/teaching/spring11/homework/homework_1.pdf
the random “slices” \( F(Z^n) \), provided \( n \) is sufficiently large. To make these notions precise, let us define the quantity

\[
S_n(F) := \sup_{z^n \in Z^n} |F(z^n)|,
\]

which is called the \( n \)th shatter coefficient of \( F \). Then we have the bound

\[
R_n(F(Z^n)) \leq 2 \sqrt{\log S_n(F) \over n}.
\]

Next, let

\[
V(F) := \max \{ n \in \mathbb{N} : S_n(F) = 2^n \}.
\]

This number is the famous Vapnik–Chervonenkis (or VC) dimension of \( F \), which has originated in their work \([VC71]\). It is clear that if \( S_n(F) < 2^n \) for some \( n \), then \( S_m(F) < 2^m \) for all \( m > n \). Hence, \( V(F) \) is always well-defined (though it may be infinite). When it is finite, we say that \( F \) is a VC class. What this means is that, for \( n \) large enough, a certain structure emerges in the sets \( F(z^n) \), which prevents us from being able to form any combination of binary labels by sweeping through the entire \( F \). A fundamental result, which was independently derived by Sauer \([Sau72]\) and Shelah \([She72]\) in different contexts (combinatorics and mathematical logic respectively) and also appeared in a weaker form in the original work of Vapnik and Chervonenkis \([VC71]\), says the following:

**Lemma 4.5 (Sauer–Shelah).** If \( F \) is a VC class, i.e., \( V(F) < \infty \), then

\[
S_n(F) \leq \sum_{i=1}^{V(F)} \binom{n}{i} \leq (n + 1)^{V(F)}.
\]

Thus, we arrive at the following important result, which we will revisit in the next lecture:

**Theorem 4.2.** If \( F \) is a VC class of binary functions, then

\[
\text{ER}_n(F(Z^n)) \leq 2 \sqrt{V(F) \log(n + 1) \over n}.
\]

Consequently, for a VC class \( F \), the risk of ERM computed on an i.i.d. sample of size \( n \) from an arbitrary distribution \( P \in \mathcal{P}(Z) \) is bounded by

\[
P(\hat{f}_n) \leq L^*(F) + 8 \sqrt{V(F) \log(n + 1) \over n} + \sqrt{2 \log \left( \frac{1}{\delta} \right) \over n}
\]

with probability at least \( 1 - \delta \). In fact, using a much more refined technique called chaining originating in the work of Dudley \([Dud78]\), it is possible to remove the logarithm in (4.79) to obtain the bound

\[
\text{ER}_n(F(Z^n)) \leq C \sqrt{V(F) \over n},
\]

where \( C > 0 \) is some universal constant independent of \( n \) and \( F \). We will not cover chaining in this class, but we will use the above formula.
A key result on the ERM algorithm, proved in the previous lecture, was that

$$P(\hat{f}_n) \leq L^*(F) + 4ER_n(F(Z^n)) + \frac{\sqrt{2\log(1/\delta)}}{n}$$

with probability at least $1 - \delta$. The quantity $R_n(F(Z^n))$ appearing on the right-hand side of the above bound is the *Rademacher average* of the random set

$$F(Z^n) = \{(f(Z_1), \ldots, f(Z_n)) : f \in F\},$$

often referred to as the *projection* of $F$ onto the sample $Z^n$. From this we see that a sufficient condition for the ERM algorithm to produce near-optimal hypotheses with high probability is that the expected Rademacher average $ER_n(F(Z^n)) = \tilde{O}(1/\sqrt{n})$, where the $\tilde{O}(\cdot)$ notation indicates that the bound holds up to polylogarithmic factors in $n$, i.e., there exists some positive polynomial function $p(\cdot)$ such that

$$ER_n(F(Z^n)) \leq O(\sqrt{p(\log n)/n}).$$

Hence, a lot of effort in statistical learning theory is devoted to obtaining tight bounds on $ER_n(F(Z^n))$.

One way to guarantee an $\tilde{O}(1/\sqrt{n})$ bound on $ER_n$ is if the “effective size” of the random set $F(Z^n)$ is finite and grows polynomially with $n$. Then the Finite Class Lemma will tell us that

$$R_n(F(Z^n)) = O\left(\sqrt{\frac{\log n}{n}}\right).$$

In general, a reasonable notion of “effective size” is captured by various *covering numbers* (see, e.g., the lecture notes by Mendelson [Men03] or the recent monograph by Talagrand [Tal05] for detailed expositions of the relevant theory). In this lecture, we will look at a simple combinatorial notion of effective size for classes of *binary-valued* functions. This particular notion has originated with the work of Vapnik and Chervonenkis [VC71], and was historically the first such notion to be introduced into statistical learning theory. It is now known as the *Vapnik–Chervonenkis (or VC) dimension*.

1. Vapnik–Chervonenkis dimension: definition

**Definition 5.1.** Let $C$ be a class of (measurable) subsets of some space $Z$. We say that a finite set $S = \{z_1, \ldots, z_n\} \subset Z$ is shattered by $C$ if for every subset $S' \subset S$ there exists some $C \in C$ such that $S' = S \cap C$. 

50
In other words, $S = \{z_1, \ldots, z_n\}$ is shattered by $\mathcal{C}$ if for any binary $n$-tuple $b = (b_1, \ldots, b_n) \in \{0, 1\}^n$ there exists some $C \in \mathcal{C}$ such that
\[
(1_{\{z_1 \in C\}}, \ldots, 1_{\{z_n \in C\}}) = b
\]
or, equivalently, if
\[
\{ (1_{\{z_1 \in C\}}, \ldots, 1_{\{z_n \in C\}}) : C \in \mathcal{C} \} = \{0, 1\}^n,
\]
where we consider any two $C_1, C_2 \in \mathcal{C}$ as equivalent if $1_{\{z_i \in C_1\}} = 1_{\{z_i \in C_2\}}$ for all $1 \leq i \leq n$.

**Definition 5.2.** The Vapnik–Chervonenkis dimension (or the VC dimension) of $\mathcal{C}$ is
\[
V(\mathcal{C}) := \max \left\{ n \in \mathbb{N} : \exists S \subset \mathbb{Z} \text{ such that } |S| = n \text{ and } S \text{ is shattered by } \mathcal{C} \right\}.
\]
If $V(\mathcal{C}) < \infty$, we say that $\mathcal{C}$ is a VC class (of sets).

We can express the VC dimension in terms of shatter coefficients of $\mathcal{C}$: Let
\[
S_n(\mathcal{C}) := \sup_{S \subset \mathbb{Z}, |S| = n} |\{S \cap C : C \in \mathcal{C}\}|
\]
denote the $n$th shatter coefficient of $\mathcal{C}$, where for each fixed $S$ we consider any two $C_1, C_2 \in \mathcal{C}$ as equivalent if $S \cap C_1 = S \cap C_2$. Then
\[
V(\mathcal{C}) = \max \left\{ n \in \mathbb{N} : S_n(\mathcal{C}) = 2^n \right\}.
\]
The VC dimension $V(\mathcal{C})$ may be infinite, but it is always well-defined. This follows from the following lemma:

**Lemma 5.1.** If $S_n(\mathcal{C}) < 2^n$, then $S_m(\mathcal{C}) < 2^m$ for all $m > n$.

**Proof.** Suppose $S_n(\mathcal{C}) < 2^n$. Consider any $m > n$. We will suppose that $S_m(\mathcal{C}) = 2^m$ and derive a contradiction. By our assumption that $S_m(\mathcal{F}) = 2^m$, there exists $S = \{z_1, \ldots, z_m\} \in \mathbb{Z}^m$, such that for every binary $n$-tuple $b = (b_1, \ldots, b_n)$ we can find some $C \in \mathcal{C}$ satisfying
\[
(1_{\{z_1 \in C\}}, \ldots, 1_{\{z_n \in C\}}, 1_{\{z_{n+1} \in C\}}, \ldots, 1_{\{z_m \in C\}}) = (b_1, \ldots, b_n, 0, \ldots, 0).
\]
From (5.1) it immediately follows that
\[
(1_{\{z_1 \in C\}}, \ldots, 1_{\{z_n \in C\}}) = (b_1, \ldots, b_n).
\]
Since $b = (b_1, \ldots, b_n)$ was arbitrary, we see from (5.2) that $S_n(\mathcal{C}) = 2^n$. This contradicts our assumption that $S_n(\mathcal{C}) < 2^n$, so we conclude that $S_m(\mathcal{C}) < 2^m$ whenever $m > n$ and $S_n(\mathcal{F}) < 2^n$. \qed

There is a one-to-one correspondence between binary-valued functions $f : \mathbb{Z} \to \{0, 1\}$ and subsets of $\mathbb{Z}$:
\[
\forall f : \mathbb{Z} \to \{0, 1\} \text{ let } C_f := \{z : f(z) = 1\}
\]
\[
\forall C \subseteq \mathbb{Z} \text{ let } f_C := 1_{\{C\}}.
\]
Thus, we can extend the concept of shattering, as well as the definition of the VC dimension, to any class $\mathcal{F}$ of functions $f : \mathbb{Z} \to \{0, 1\}$:
DEFINITION 5.3. Let \( \mathcal{F} \) be a class of functions \( f : \mathbb{Z} \to \{0, 1\} \). We say that a finite set \( S = \{z_1, \ldots, z_n\} \subset \mathbb{Z} \) is shattered by \( \mathcal{F} \) if it is shattered by the class
\[
\mathcal{C}_\mathcal{F} := \{1_{\{f=1\}} : f \in \mathcal{F}\},
\]
where \( 1_{\{f=1\}} \) is the indicator function of the set \( \mathcal{C}_f := \{z \in \mathbb{Z} : f(z) = 1\} \). The nth shatter coefficient of \( \mathcal{F} \) is \( \mathbb{S}_n(\mathcal{F}) = \mathbb{S}_n(\mathcal{C}_\mathcal{F}) \), and the VC dimension of \( \mathcal{F} \) is defined as \( V(\mathcal{F}) = V(\mathcal{C}_\mathcal{F}) \).

In light of these definitions, we can equivalently speak of the VC dimension of a class of sets or a class of binary-valued functions.

2. Examples of Vapnik–Chervonenkis classes

2.1. Semi-infinite intervals. Let \( \mathbb{Z} = \mathbb{R} \) and take \( \mathcal{C} \) to be the class of all intervals of the form \( (-\infty, t] \) as \( t \) varies over \( \mathbb{R} \). We will prove that \( V(\mathcal{C}) = 1 \). In view of Lemma 5.1, it suffices to show that (1) any one-point set \( S = \{a\} \) is shattered by \( \mathcal{C} \), and (2) no two-point set \( S = \{a, b\} \) is shattered by \( \mathcal{C} \).

Given \( S = \{a\} \), choose any \( t_1 < a \) and \( t_2 > a \). Then \( (-\infty, t_1] \cap S = \emptyset \) and \( (-\infty, t_2] \cap S = S \). Thus, \( S \) is shattered by \( \mathcal{C} \). This holds for every one-point set \( S \), and therefore we have proved (1). To prove (2), let \( S = \{a, b\} \) and suppose, without loss of generality, that \( a < b \). Then there exists no \( t \in \mathbb{R} \) such that \( (-\infty, t] \cap S = \{b\} \). This follows from the fact that if \( b \in (-\infty, t] \cap S \), then \( t \geq b \). Since \( b > a \), we must have \( t > a \), so that \( a \in (-\infty, t] \cap S \) as well. Since \( a \) and \( b \) are arbitrary, we see that no two-point subset of \( \mathbb{R} \) can be shattered by \( \mathcal{C} \).

2.2. Closed intervals. Again, let \( \mathbb{Z} = \mathbb{R} \) and take \( \mathcal{C} \) to be the class of all intervals of the form \( [s, t] \) for all \( s, t \in \mathbb{R} \). Then \( V(\mathcal{C}) = 2 \). To see this, we will show that (1) any two-point set \( S = \{a, b\} \) can be shattered by \( \mathcal{C} \) and that (2) no three-point set \( S = \{a, b, c\} \) can be shattered by \( \mathcal{C} \).

For (1), let \( S = \{a, b\} \) and suppose, without loss of generality, that \( a < b \). Choose four points \( t_1, t_2, t_3, t_4 \in \mathbb{R} \) such that \( t_1 < t_2 < a < t_3 < b < t_4 \). There are four subsets of \( S \): \( \emptyset \), \( \{a\} \), \( \{b\} \), and \( \{a, b\} = S \). Then
\[
[t_1, t_2] \cap S = \emptyset, \quad [t_2, t_3] \cap S = \{a\}, \quad [t_3, t_4] \cap S = \{b\}, \quad [t_1, t_4] \cap S = S.
\]
Hence, \( S \) is shattered by \( \mathcal{C} \). This holds for every two-point set in \( \mathbb{R} \), which proves (1).

To prove (2), let \( S = \{a, b, c\} \) be an arbitrary three-point set with \( a < b < c \). Then the intersection of any \( [t_1, t_2] \in \mathcal{C} \) with \( S \) containing \( a \) and \( c \) must necessarily contain \( b \) as well. This shows that no three-point set can be shattered by \( \mathcal{C} \), so by Lemma 5.1 we conclude that \( V(\mathcal{C}) = 2 \).

2.3. Closed halfspaces. Let \( \mathbb{Z} = \mathbb{R}^2 \), and let \( \mathcal{C} \) consist of all closed halfspaces, i.e., sets of the form
\[
\{z = (z_1, z_2) \in \mathbb{R}^2 : w_1z_1 + w_2z_2 \geq b\}
\]
for all choices of \( w_1, w_2, b \in \mathbb{R} \) such that \( (w_1, w_2) \neq (0, 0) \). Then \( V(\mathcal{C}) = 3 \).

To see that \( \mathbb{S}_3(\mathcal{C}) = 2^3 = 8 \), it suffices to consider any set \( S = \{z_1, z_2, z_3\} \) of three non-collinear points. Then it is not hard to see that for any \( S' \subseteq S \) it is possible to choose a closed halfspace \( C \in \mathcal{C} \) that would contain \( S' \), but not \( S \). To see that \( \mathbb{S}_4(\mathcal{C}) = 2^4 \), we must look at all four-point sets \( S = \{z_1, z_2, z_3, z_4\} \). There are two cases to consider:
Figure 1. Impossibility of shattering an affinely independent four-point set in $\mathbb{R}^2$ by closed halfspaces.

(1) One point in $S$ lies in the convex hull of the other three. Without loss of generality, let's suppose that $z_1 \in \text{conv}(S')$ with $S' = \{z_2, z_3, z_4\}$. Then there is no $C \in \mathcal{C}$ such that $C \cap S = S'$. The reason for this is that every $C \in \mathcal{C}$ is a convex set. Hence, if $S' \subset C$, then any point in $\text{conv}(S')$ is contained in $C$ as well.

(2) No point in $S$ is in the convex hull of the remaining points. This case, when $S$ is an affinely independent set, is shown in Figure 1. Let us partition $S$ into two disjoint subsets, $S_1$ and $S_2$, each consisting of “opposite” points. In the figure, $S_1 = \{z_1, z_3\}$ and $S_2 = \{z_2, z_4\}$. Then it is easy to see that there is no halfspace $C$ whose boundary could separate $S_1$ from its complement $S_2$. This is, in fact, the (in)famous “XOR counterexample” of Minsky and Papert [MP69], which has demonstrated the impossibility of universal concept learning by one-layer perceptrons.

Since any four-point set in $\mathbb{R}^2$ falls under one of these two cases, we have shown that no such set can be shattered by $\mathcal{C}$. Hence, $V(\mathcal{C}) = 3$.

More generally, if $Z = \mathbb{R}^d$ and $\mathcal{C}$ is the class of all closed halfspaces

$$\left\{ z \in \mathbb{R}^d : \sum_{j=1}^{d} w_j z_j \geq b \right\}$$

for all $w = (w_1, \ldots, w_d) \in \mathbb{R}^d$ such that at least one of the $w_j$’s is nonzero and all $b \in \mathbb{R}$, then $V(\mathcal{C}) = d + 1$ [WD81]; we will see a proof of this fact shortly.

2.4. Axis-parallel rectangles. Let $Z = \mathbb{R}^2$, and let $\mathcal{C}$ consist of all “axis-parallel” rectangles, i.e., sets of the form $C = [a_1, b_1] \times [a_2, b_2]$ for all $a_1, b_1, a_2, b_2 \in \mathbb{R}$. Then $V(\mathcal{C}) = 4$.

First we exhibit a four-point set $S = \{z_1, z_2, z_3, z_4\}$ that is shattered by $\mathcal{C}$. It suffices to take $z_1 = (-2, -1)$, $z_2 = (1, -2)$, $z_3 = (2, 1)$, $z_4 = (-1, 2)$. To show that no five-point set is shattered by $\mathcal{C}$, consider an arbitrary $S = \{z_1, z_2, z_3, z_4, z_5\}$. Of these, pick any one point with the smallest first coordinate and any one point with the largest first coordinate, and likewise for the second coordinate (refer to Figure 2), for a total of at most four. Let $S'$ denote the set consisting of these points; in Figure 2, $S' = \{z_1, z_2, z_3, z_4\}$. Then it is easy
to see that any $C \in C$ that contains the points in $S'$ must contain all the points in $S \setminus S'$ as well. Hence, no five-point set in $\mathbb{R}^2$ can be shattered by $C$, so $V(C) = 5$.

The same argument also works for axis-parallel rectangles in $\mathbb{R}^d$, i.e., all sets of the form $C = [a_1, b_1] \times [a_2, b_2] \times \ldots \times [a_d, b_d]$, leading to the conclusion that the VC dimension of the set of all axis-parallel rectangles in $\mathbb{R}^d$ is equal to $2d$.

2.5. Sets determined by finite-dimensional function spaces. The following result is due to Dudley [Dud78]. Let $Z$ be arbitrary, and let $G$ be an $m$-dimensional linear space of functions $g : Z \to \mathbb{R}$, which means that each $g \in G$ has a unique representation of the form

$$g = \sum_{j=1}^{m} c_j \psi_j,$$

where $\psi_1, \ldots, \psi_m : Z \to \mathbb{R}$ form a fixed linearly independent set and $c_1, \ldots, c_m$ are real coefficients. Consider the class

$$C = \{\{z \in Z : g(z) \geq 0\} : g \in G\}.$$  

Then $V(C) \leq m$.

To prove this, we need to show that no set of $m + 1$ points in $Z$ can be shattered by $C$. To that end, let us fix $m + 1$ arbitrary points $z_1, \ldots, z_{m+1} \in Z$ and consider the mapping $L : G \to \mathbb{R}^{m+1}$ defined by

$$L(g) := (g(z_1), \ldots, g(z_{m+1})).$$

It is easy to see that because $G$ is a linear space, $L$ is a linear mapping, i.e., for any $g_1, g_2 \in G$ and any $c_1, c_2 \in \mathbb{R}$ we have $L(c_1 g_1 + c_2 g_2) = c_1 L(g_1) + c_2 L(g_2)$. Since $\dim G = m$, the image of $G$ under $L$, i.e., the set

$$L(G) = \{(g(z_1), \ldots, g(z_{m+1})) \in \mathbb{R}^{m+1} : g \in G\},$$

is a linear subspace of $\mathbb{R}^{m+1}$ of dimension at most $m$. This means that there exists some nonzero vector $v = (v_1, \ldots, v_{m+1}) \in \mathbb{R}^{m+1}$ orthogonal to $L(G)$, i.e., for every $g \in G$

$$v_1 g(z_1) + \ldots + v_{m+1} g(z_{m+1}) = 0. \quad (5.3)$$

Without loss of generality, we may assume that at least one component of $v$ is strictly negative (otherwise we can take $-v$ instead of $v$ and still get (5.3)). Hence, we can rearrange
the equality in (5.3) as
\[
\sum_{i;m_i \geq 0} v_i g(z_i) = - \sum_{i;m_i < 0} v_i g(z_i), \quad \forall g \in \mathcal{G}.
\] (5.4)

Now let us suppose that \( S_{m+1}(\mathcal{C}) = 2^{m+1} \) and derive a contradiction. Consider a binary \((m + 1)\)-tuple \( b = (b_1, \ldots, b_{m+1}) \) \( \in \{0,1\}^{m+1} \), where \( b_j = 1 \) if and only if \( v_j \geq 0 \), and 0 otherwise. Since we assumed that \( S_{m+1}(\mathcal{C}) = 2^{m+1} \), there exists some \( g \in \mathcal{G} \) such that
\[
(1_{\{g(z_i) \geq 0\}}, \ldots, 1_{\{g(z_{m+1}) \geq 0\}}) = b.
\]

By our definition of \( b \), this means that the left-hand side of (5.4) is nonnegative, while the right-hand side is negative, which is a contradiction. Hence, \( S_{m+1}(\mathcal{C}) < 2^{m+1} \), so \( V(\mathcal{C}) \leq m \).

This result can be used to bound the VC dimension of many classes of sets:

- Let \( \mathcal{C} \) be the class of all closed halfspaces in \( \mathbb{R}^d \). Then any \( C \in \mathcal{C} \) can be represented in the form \( C = \{ z : g(z) \geq 0 \} \) for \( g(z) = \langle w, z \rangle - b \) with some nonzero \( w \in \mathbb{R}^d \) and \( b \in \mathbb{R} \). The set \( \mathcal{G} \) of all such affine functions on \( \mathbb{R}^d \) is a linear space of dimension \( d+1 \), so by the above result we have \( V(\mathcal{C}) \leq d+1 \). In fact, we know that this holds with equality [WD81]. This can also be seen from the following result, due to Cover [Cov65]: Let \( \mathcal{G} \) be the linear space of functions spanned by functions \( \psi_1, \ldots, \psi_m \), and let \( \{z_1, \ldots, z_n\} \subset Z \) be such that the vectors \( \Psi(z_i) = (\psi_1(z_i), \ldots, \psi_m(z_i)) \), \( 1 \leq i \leq n \), form a linearly independent set. Then for the class of sets \( \mathcal{C} = \{\{ z : g(z) \geq 0 \} : z \in Z \} \) we have
\[
|C \cap \{z_1, \ldots, z_n\} : C \in \mathcal{C}| = \sum_{i=0}^{m-1} \binom{n-1}{i}.
\]

The conditions needed for Cover’s result are seen to hold for indicators of halfspaces, so letting \( n = m = d+1 \) we see that \( S_d(\mathcal{C}) = \sum_{i=0}^{d} \binom{d}{i} = 2^d \). Hence, \( V(\mathcal{C}) = d+1 \).

- Let \( \mathcal{C} \) be the class of all closed balls in \( \mathbb{R}^d \), i.e., sets of the form
\[
C = \{ z \in \mathbb{R}^d : \|z - x\|^2 \leq r^2 \}
\]
where \( x \in \mathbb{R}^d \) is the center of \( C \) and \( r \in \mathbb{R}^+ \) is its radius. Then we can write \( C = \{ z : g(z) \geq 0 \} \), where
\[
g(z) = r^2 - \|z - x\|^2 = r^2 - \sum_{j=1}^{d} |z_j - x_j|^2.
\] (5.5)

Expanding the second expression for \( g \) in (5.5), we get
\[
g(z) = r^2 - \sum_{j=1}^{d} x_j^2 + 2 \sum_{j=1}^{d} x_j z_j - \sum_{j=1}^{d} z_j^2,
\]
which can be written in the form \( g(z) = \sum_{k=1}^{d+2} c_k \psi_k(z) \), where \( \psi_1(z) = 1 \), \( \psi_k(z) = z_k-1 \) for \( k = 2, \ldots, d+1 \), and \( \psi_{d+2} = \sum_{j=1}^{d} z_j^2 \). It can be shown that the functions \( \{ \psi_k \}_{k=1}^{d+2} \) are linearly independent. Hence, \( V(\mathcal{C}) \leq d + 2 \). This bound, however, is not tight; as shown by Dudley [Dud79], the class of closed balls in \( \mathbb{R}^d \) has VC dimension \( d+1 \).
2.6. VC dimension vs. number of parameters. Looking back at all these examples, one may get the impression that the VC dimension of a set of binary-valued functions is just the number of parameters. This is not the case. Consider the following one-parameter family of functions:

\[ g_{\theta}(z) := \sin(\theta z), \quad \theta \in \mathbb{R}. \]

However, the class of sets

\[ C = \left\{ \{ z \in \mathbb{R} : g_{\theta}(z) \geq 0 \} : \theta \in \mathbb{R} \right\} \]

has infinite VC dimension. Indeed, for any \( n \), any collection of numbers \( z_1, \ldots, z_n \in \mathbb{R} \), and any binary string \( b \in \{0, 1\}^n \), one can always find some \( \theta \in \mathbb{R} \) such that

\[ \text{sgn}(\sin(\theta z_i)) = \begin{cases} +1, & \text{if } b_i = 1 \\ -1, & \text{if } b_i = 0 \end{cases}. \]


The importance of VC classes in learning theory arises from the fact that, as \( n \) tends to infinity, the fraction of subsets of any \( \{z_1, \ldots, z_n\} \subset \mathbb{Z} \) that are shattered by a given VC class \( C \) tends to zero. We will prove this fact in this section by deriving a sharp bound on the shatter coefficients \( S_n(C) \) of a VC class \( C \). This bound have been (re)discovered at least three times, first in a weak form by Vapnik and Chervonenkis [VC71] in 1971, then independently and in different contexts by Sauer [Sau72] and Shelah [She72] in 1972. In strict accordance with Stigler’s law of eponymy\(^1\), it is known in the statistical learning literature as the Sauer–Shelah lemma.

Before we state and prove this result, we will collect some preliminaries and set up some notation. Given integers \( n, d \geq 1 \), let

\[ \phi(n, d) := \begin{cases} \sum_{i=0}^{d} \binom{n}{i}, & \text{if } n > d \\ 2^n, & \text{if } n \leq d \end{cases} \]

If we adopt the convention that \( \binom{n}{i} = 0 \) for \( i > n \), we can write

\[ \phi(n, d) = \sum_{i=0}^{d} \binom{n}{i} \]

for all \( n, d \geq 1 \). We will find the following recursive relation useful:

**Lemma 5.2.**

\[ \phi(n, d) = \phi(n - 1, d) + \phi(n - 1, d - 1). \]

**Proof.** We have

\[ \binom{n-1}{i-1} + \binom{n-1}{i} = \frac{(n-1)!}{(i-1)!(n-i)!} + \frac{(n-1)!}{i!(n-i-1)!}. \]

\(^1\)“No scientific discovery is named after its original discoverer” (http://en.wikipedia.org/wiki/Stigler’s_law_of_eponymy)
Multiplying both sides by \(i!(n-i)!\), we obtain

\[
i!(n-i)! \left[ \binom{n-1}{i-1} + \binom{n-1}{i} \right] = i(n-1)! + (n-i)(n-1)! = n!
\]

Hence,

\[
\binom{n-1}{i-1} + \binom{n-1}{i} = \frac{n!}{i!(n-i)!} = \binom{n}{i}.
\]

Using the definition of \(\phi(n, d)\), as well as (5.6), we get

\[
\phi(n, d) = \sum_{i=0}^{d} \binom{n}{i} = 1 + \sum_{i=1}^{d} \binom{n-1}{i} = 1 + \sum_{i=1}^{d-1} \binom{n-1}{i-1} = \phi(n-1, d) + \phi(n-1, d-1)
\]

and the lemma is proved. \(\square\)

Now for the actual result:

**Theorem 5.1 (Sauer–Shelah lemma).** Let \(C\) be a class of subsets of some space \(Z\) with \(V(C) = d < \infty\). Then for all \(n\),

\[
S_n(C) \leq \phi(n, d).
\]

**Proof.** There are several different proofs in the literature; we will use an inductive argument following Blumer et al. [BEHW89].

We can assume, without loss of generality, that \(n > d\), for otherwise \(S_n(C) = 2^n = \phi(n, d)\).

For an arbitrary finite set \(S \subset Z\), let

\[
S(S, C) := |\{S \cap C : C \in C\}|
\]

where, as before, we count only the distinct sets of the form \(S \cap C\). By definition, \(S_n(C) = \sup_{S:|S|=n} S(S, C)\). Thus, it suffices the prove the following: For any \(S \subset Z\) with \(|S| = n > d\), \(S(S, C) \leq \phi(n, d)\).

For the purpose of computing \(S(S, C)\), any two \(C_1, C_2 \in C\) such that \(S \cap C_1 = S \cap C_2\) are deemed equivalent. Hence, let

\[
\mathcal{A} := \{A \subseteq S : A = S \cap C\text{ for some }C \in C\}.
\]

Then we may write

\[
S(S, C) = |\{S \cap C : C \in C\}| = |\{A \subseteq S : A = S \cap C\text{ for some }C \in C\}| = |\mathcal{A}|.
\]

Moreover, it is easy to see that \(V(\mathcal{A}) \leq V(C) = d\).

Thus, the desired result is equivalent to saying that if \(\mathcal{A}\) is a collection of subsets of an \(n\)-element set \(S\) (which we may, without loss of generality, take to be \([n] := \{1, \ldots, n\}\) with \(V(\mathcal{A}) \leq d < n\), then \(|\mathcal{A}| \leq \phi(n, d)\). We will prove this statement by “double induction” on \(n\) and \(d\). First of all, the statement (5.7) holds for all \(n \geq 1\) and \(d = 0\). Indeed, if \(V(\mathcal{A}) = 0\), then \(|\mathcal{A}| = 1 \leq 2^n\). Now assume that (5.7) holds for all \(n\) and all \(\mathcal{A}\) with \(V(\mathcal{A}) \leq d - 1\), and for all integers up to \(n - 1\) and all \(\mathcal{A}\) with \(V(\mathcal{A}) \leq d\). Now let \(S = [n]\), and let \(\mathcal{A}\) be a collection of subsets of \([n]\) with \(V(\mathcal{A}) = d < n\). We will show that \(|\mathcal{A}| \leq \phi(n, d)\).
To prove this claim, let us choose an arbitrary \( i \in S \) and define
\[
\mathcal{A}\setminus\{i\} := \{A \setminus \{i\} : A \in \mathcal{A}\}
\]
\[
\mathcal{A}_i := \{A \in \mathcal{A} : i \notin A, A \cup \{i\} \in \mathcal{A}\}
\]
Observe that both \( \mathcal{A}\setminus\{i\} \) and \( \mathcal{A}_i \) are classes of subsets of \( S \setminus \{i\} \). Moreover, since \( A \) and \( A \cup \{i\} \) map to the same element of \( \mathcal{A}\setminus\{i\} \), while \( |\mathcal{A}_i| \) is the number of pairs of sets in \( \mathcal{A} \) that map into the same set in \( \mathcal{A}\setminus\{i\} \), we have
\[
|\mathcal{A}| = |\mathcal{A}\setminus\{i\}| + |\mathcal{A}_i|.
\]
(5.8)

Since \( \mathcal{A}\setminus\{i\} \subseteq \mathcal{A} \), we have \( V(\mathcal{A}\setminus\{i\}) \leq V(\mathcal{A}) \leq d \). Also, every set in \( \mathcal{A}\setminus\{i\} \) is a subset of \( S \setminus \{i\} \), which has cardinality \( n - 1 \). Therefore, by the inductive hypothesis \( |\mathcal{A}\setminus\{i\}| \leq \phi(n - 1, d) \).

Next, we show that \( V(\mathcal{A}_i) \leq d - 1 \). Suppose, to the contrary, that \( V(\mathcal{A}_i) = d \). Then there must exist some \( T \subseteq S \setminus \{i\} \) with \( |T| = d \) that is shattered by \( \mathcal{A}_i \). But then \( T \cup \{i\} \) is shattered by \( \mathcal{A} \). To see this, given any \( T' \subseteq T \) choose some \( A \in \mathcal{A}_i \) such that \( T \cap A = T' \) (this is possible since \( T \) is shattered by \( \mathcal{A}_i \)). But then \( A \cup \{i\} \in \mathcal{A} \) (by definition of \( \mathcal{A}_i \)), and
\[
(T \cup \{i\}) \cap (A \cup \{i\}) = (T \cap A) \cup \{i\} = T' \cup \{i\}.
\]

Since this is possible for an arbitrary \( T' \subseteq T \), we conclude that \( T \cup \{i\} \) is shattered by \( \mathcal{A} \).

Now, since \( T \subseteq S \setminus \{i\} \), we must have \( i \neq T \), so \( |T \cup \{i\}| = |T| + 1 = d + 1 \), which means that there exists a \((d + 1)\)-element subset of \( S = [n] \) that is shattered by \( \mathcal{A} \). But this contradicts our assumption that \( V(\mathcal{A}) \leq d \). Hence, \( V(\mathcal{A}_i) \leq d - 1 \). Since \( \mathcal{A}_i \) is a collection of subsets of \( S \setminus \{i\} \), we must have \( |\mathcal{A}_i| \leq \phi(n - 1, d - 1) \) by the inductive hypothesis. Hence, from (5.8) and from Lemma 5.2 we have
\[
|\mathcal{A}| = |\mathcal{A}\setminus\{i\}| + |\mathcal{A}_i| \leq \phi(n - 1, d) + \phi(n - 1, d - 1) = \phi(n, d).
\]

This completes the induction argument and proves (5.7). \( \square \)

**Corollary 5.1.** If \( \mathcal{C} \) is a collection of sets with \( V(\mathcal{C}) \leq d < \infty \), then
\[
\mathcal{S}_n(\mathcal{C}) \leq (n + 1)^d.
\]
Moreover, if \( n \geq d \), then
\[
\mathcal{S}_n(\mathcal{C}) \leq \left(\frac{en}{d}\right)^d,
\]
where \( e \) is the base of the natural logarithm.

**Proof.** For the first bound, write
\[
\phi(n, d) = \sum_{i=0}^{d} \left(\frac{n}{i}\right) = \sum_{i=1}^{d} \frac{n!}{i!(n-i)!} \leq \sum_{i=1}^{d} \frac{n^i}{i!} \leq \sum_{i=0}^{d} \frac{n^i d!}{i!(d-i)!} = \sum_{i=0}^{d} n^i \binom{d}{i} = (n + 1)^d,
\]
where the last step uses the binomial theorem. On the other hand, if \( d/n \leq 1 \), then
\[
\left(\frac{d}{n}\right)^d \phi(n, d) = \left(\frac{d}{n}\right)^d \sum_{i=0}^{d} \binom{n}{i} \leq \sum_{i=1}^{d} \left(\frac{d}{n}\right)^i \binom{n}{i} \leq \sum_{i=1}^{n} \left(\frac{d}{n}\right)^i \binom{n}{i} = \left(1 + \frac{d}{n}\right)^n \leq e^d,
\]
where we again used the binomial theorem. Dividing both sides by \( (d/n)^d \), we get the second bound. \( \square \)
Let $\mathcal{C}$ be a VC class of subsets of some space $Z$. From the above corollary we see that
\[
\limsup_{n \to \infty} \frac{S_n(\mathcal{C})}{2^n} \leq \lim_{n \to \infty} \frac{(n + 1)^{V(\mathcal{C})}}{2^n} = 0.
\]
In other words, as $n$ becomes large, the fraction of subsets of an arbitrary $n$-element set $\{z_1, \ldots, z_n\} \subset Z$ that are shattered by $\mathcal{C}$ becomes negligible. Moreover, combining the bounds of the corollary with the Finite Class Lemma for Rademacher averages, we get the following:

**Theorem 5.2.** Let $\mathcal{F}$ be a VC class of binary-valued functions $f : Z \to \{0, 1\}$ on some space $Z$. Let $Z^n$ be an i.i.d. sample of size $n$ drawn according to an arbitrary probability distribution $P \in \mathcal{P}(Z)$. Then
\[
\mathbb{E}R_n(\mathcal{F}(Z^n)) \leq 2 \sqrt{\frac{V(\mathcal{F}) \log(n + 1)}{n}}.
\]
A more refined chaining technique [Dud78] can be used to remove the logarithm in the above bound:

**Theorem 5.3.** There exists an absolute constant $C > 0$, such that under the conditions of the preceding theorem
\[
\mathbb{E}R_n(\mathcal{F}(Z^n)) \leq C \sqrt{\frac{V(\mathcal{F})}{n}}.
\]
CHAPTER 6

Binary classification

The problem of binary classification can be stated as follows. We have a random couple $Z = (X, Y)$, where $X \in \mathbb{R}^d$ is called the feature vector and $Y \in \{-1, 1\}$ is called the label. In the spirit of the model-free framework, we assume that the relationship between the features and the labels is stochastic and described by an unknown probability distribution $P \in \mathcal{P}(Z)$, where $Z = \mathbb{R}^d \times \{-1, 1\}$. In these lectures on binary classification, I will be following mainly two excellent sources: the book by Devroye, Györfi, and Lugosi [DGL96] and the comprehensive survey article by Bousquet, Boucheron, and Lugosi [BBL05].

As usual, we consider the case when we are given an i.i.d. sample of length $n$ from $P$. The goal is to learn a classifier, i.e., a mapping $g : \mathbb{R}^d \to \{-1, 1\}$, such that the probability of classification error, $P(g(X) \neq Y)$, is small. As we have seen before, the optimal choice is the Bayes classifier

$$g^*(x) := \begin{cases} 1, & \text{if } \eta(x) > 1/2 \\ -1, & \text{otherwise} \end{cases}$$

(6.1)

where $\eta(x) := P[Y = 1|X = x]$ is the regression function. However, since we make no assumptions on $P$, in general we cannot hope to learn the Bayes classifier $g^*$. Instead, we focus on a more realistic goal: We fix a collection $\mathcal{G}$ of classifiers and then use the training data to come up with a hypothesis $\hat{g}_n \in \mathcal{G}$, such that

$$P(\hat{g}_n(X) \neq Y) \approx \inf_{g \in \mathcal{G}} P(g(X) \neq Y)$$

with high probability.

By way of notation, let us write $L(g)$ for the classification error of $g$, i.e., $L(g) := P(g(X) \neq Y)$, and let $L^*(\mathcal{G})$ denote the smallest classification error attainable over $\mathcal{G}$:

$$L^*(\mathcal{G}) := \inf_{g \in \mathcal{G}} L(g).$$

We will assume that a minimizing $g^* \in \mathcal{G}$ exists. For future reference, we note that

$$L(g) = P(g(X) \neq Y) = P(g(X) < 0).$$

(6.2)

**Warning:** In what follows, we will use $C$ or $c$ to denote various absolute constants; their values may change from line to line.

---

1The reason why we chose $\{-1, 1\}$, rather than $\{0, 1\}$, for the label space is merely convenience.
1. Learning linear discriminant rules

One of the simplest classification rules (and one of the first to be studied) is a linear discriminant rule: given a nonzero vector \( w = (w^{(1)}, \ldots, w^{(d)}) \in \mathbb{R}^d \) and a scalar \( b \in \mathbb{R} \), let

\[
 g(x) \equiv g_{w,b}(x) := \begin{cases} 
 1, & \text{if } \langle w, x \rangle + b > 0 \\
 -1, & \text{otherwise}
\end{cases}
\]  

(6.3)

Let \( \mathcal{G} \) be the class of all such linear discriminant rules as \( w \) ranges over all nonzero vectors in \( \mathbb{R}^d \) and \( b \) ranges over all reals: \( \mathcal{G} = \{ g_{w,b} : w \in \mathbb{R}^d \setminus \{0\}, b \in \mathbb{R} \} \).

Given the training sample \( Z^n \), let \( \hat{g}_n \in \mathcal{G} \) be the output of the ERM algorithm, i.e.,

\[
 \hat{g}_n := \arg \min_{g \in \mathcal{G}} \frac{1}{n} \sum_{i=1}^n 1_{\{ g(X_i) \neq Y_i \}}.
\]

In other words, \( \hat{g}_n \) is any classifier of the form (6.3) that minimizes the number of misclassifications on the training sample. Then we have the following:

**Theorem 6.1.** There exists an absolute constant \( C > 0 \), such that for any \( n \in \mathbb{N} \) and any \( \delta \in (0,1) \), the bound

\[
 L(\hat{g}_n) \leq L^*(\mathcal{G}) + C \sqrt{\frac{d + 1}{n} + \frac{2 \log(1/\delta)}{n}}
\]  

(6.4)

holds with probability at least \( 1 - \delta \).

**Proof.** A standard argument leads to the bound

\[
 L(\hat{g}_n) \leq L^*(\mathcal{G}) + 2 \Delta_n(Z^n),
\]

(6.5)

where

\[
 \Delta_n(Z^n) := \sup_{g \in \mathcal{G}} |L(g) - L_n(g)|
\]

is the uniform deviation and \( L_n(g) \) denotes the empirical classification error of \( g \) on \( Z^n \):

\[
 L_n(g) = \frac{1}{n} \sum_{i=1}^n 1_{\{ g(X_i) \neq Y_i \}},
\]

which is the fraction of incorrectly labeled points in the training sample \( Z^n \). Consider a classifier \( g \in \mathcal{G} \) and define the set

\[
 C_g := \{ (x,y) \in \mathbb{R}^d \times \{-1,1\} : y \cdot (\langle w, x \rangle + b) \leq 0 \}.
\]

Then it is easy to see that

\[
 L(g) = P(C_g) \quad \text{and} \quad L_n(g) = P_n(C_g),
\]

where, as before,

\[
 P_n = \frac{1}{n} \sum_{i=1}^n \delta_{Z_i} = \frac{1}{n} \sum_{i=1}^n \delta_{(X_i,Y_i)}
\]

is the empirical distribution of the sample \( Z^n \). Let \( \mathcal{C} \) denote the collection of all sets of the form \( C = C_g \) for some \( g \in \mathcal{G} \). Then

\[
 \Delta_n(Z^n) = \sup_{C \in \mathcal{C}} |P_n(C) - P(C)|.
\]
Let $\mathcal{F} = \mathcal{F}_C$ denote the class of indicator functions of the sets in $\mathcal{C}$: $\mathcal{F}_C = \{1_{\cdot \in C} : C \in \mathcal{C}\}$. Then we know that, with probability at least $1 - \delta$,

$$\Delta_n(Z^n) \leq 2E_Rn(\mathcal{F}(Z^n)) + \sqrt{\frac{\log(1/\delta)}{2n}},$$

(6.6)

where $R_n(\mathcal{F}(Z^n))$ is the Rademacher average of the projection of $\mathcal{F}$ onto the sample $Z^n$. Now,

$$\mathcal{F}(Z^n) = \{(f(Z_1), \ldots, f(Z_n)) : f \in \mathcal{F}\}
= \{(1_{\{Z_1 \in C\}}, \ldots, 1_{\{Z_n \in C\}}) : C \in \mathcal{C}\}.$$  

Therefore, if we prove that $\mathcal{C}$ is a VC class, then

$$R_n(\mathcal{F}(Z^n)) \leq C\sqrt{\frac{V(\mathcal{C})}{n}}.$$  

But this follows from the fact that any $C \in \mathcal{C}$ has the form

$$C = \left\{(x, y) \in \mathbb{R}^d \times \{-1, 1\} : \sum_{j=1}^d w^{(j)} y x^{(j)} + by \leq 0 \right\}$$

for some $w \in \mathbb{R}^d \backslash \{0\}$ and some $b \in \mathbb{R}$, and the functions $(x, y) \mapsto y$ and $(x, y) \mapsto y x^{(j)}$, $1 \leq j \leq d$, span a linear space of dimension no greater than $d + 1$. Hence, $V(\mathcal{C}) \leq d + 1$, so that

$$R_n(\mathcal{F}(Z^n)) \leq C\sqrt{\frac{V(\mathcal{C})}{n}} \leq C\sqrt{\frac{d + 1}{n}}.$$  

Combining this with (6.5) and (6.6), we see that (6.4) holds with probability at least $1 - \delta$.  

1.1. **Generalized linear discriminant rules.** In the same vein, we may consider classification rules of the form

$$g(x) = \begin{cases} 1, & \text{if } \sum_{j=1}^k w^{(j)} \psi_j(x) + b > 0 \\ -1, & \text{otherwise} \end{cases}$$

(6.7)

where $k$ is some positive integer (not necessarily equal to $d$), $w = (w^{(1)}, \ldots, w^{(k)}) \in \mathbb{R}^k$ is a nonzero vector, $b \in \mathbb{R}$ is an arbitrary scalar, and $\Psi = \{\psi_j : \mathbb{R}^d \to \mathbb{R}\}_{j=1}^k$ is some fixed “dictionary” of real-valued functions on $\mathbb{R}^d$. For a fixed $\Psi$, let $\mathcal{G}$ denote the collection of all classifiers of the form (6.7) as $w$ ranges over all nonzero vectors in $\mathbb{R}^k$ and $b$ ranges over all reals. Then the ERM rule is, again, given by

$$\hat{g}_n := \inf_{g \in \mathcal{G}} L_n(g) \equiv \inf_{g \in \mathcal{G}} \frac{1}{n} \sum_{i=1}^n 1_{\{g(X_i) \neq Y_i\}}.$$  

The following result can be proved pretty much along the same lines as Theorem 6.1:

**Theorem 6.2.** There exists an absolute constant $C > 0$, such that for any $n \in \mathbb{N}$ and any $\delta \in (0, 1)$, the bound

$$L(\hat{g}_n) \leq L^*(\mathcal{G}) + C\sqrt{\frac{k + 1}{n}} + \sqrt{\frac{2 \log(1/\delta)}{n}}$$

(6.8)

holds with probability at least $1 - \delta$.  

62
1.2. Two fundamental issues. As Theorems 6.1 and 6.2 show, the ERM algorithm applied to the collection of all (generalized) linear discriminant rules is guaranteed to work well in the sense that the classification error of the output hypothesis will, with high probability, be close to the optimum achievable by any discriminant rule with the given structure. The same argument extends to any collection of classifiers $G$, for which the “error sets” $(x,y) : y \cdot g(x) \leq 0, \ g \in G$, form a VC class of dimension much smaller than the sample size $n$. In other words, with high probability the difference

$$L(\hat{g}_n) - L^*(G) = L(\hat{g}_n) - \inf_{g \in G} L(g)$$

will be small. However, precisely because the VC dimension of $G$ cannot be too large, the approximation properties of $G$ will be limited. Another problem is computational. For instance, the problem of finding an empirically optimal linear discriminant rule is NP-hard. In other words, unless P is equal to NP, there is no hope of coming up with an efficient ERM algorithm for linear discriminant rules that would work for all feature space dimensions $d$. If $d$ is fixed, then it is possible to enumerate all projections of a given sample $Z^n$ onto the class of indicators of all halfspaces in $O(n^{d-1} \log n)$ time, which allows for an exhaustive search for an ERM solution, but the usefulness of this naive approach is limited to $d < 5$.

2. Risk bounds for combined classifiers via surrogate loss functions

One way to sidestep the above approximation-theoretic and computational issues is to replace the 0–1 Hamming loss function that gives rise to the probability of error criterion with some other loss function. What we gain is the ability to bound the performance of various complicated classifiers built up by combining simpler base classifiers in terms of the complexity (e.g., the VC dimension) of the collection of the base classifiers, as well as considerable computational advantages, especially if the problem of minimizing the empirical surrogate loss turns out to be a convex programming problem. What we lose, though, is that, in general, we will not be able to compare the generalization error of the learned classifier to the minimum classification risk. Instead, we will have to be content with the fact that the generalization error will be close to the smallest surrogate loss.

We will consider classifiers of the form

$$g_f(x) = \text{sgn} f(x) \equiv \begin{cases} 1, & \text{if } f(x) \geq 0 \\ -1, & \text{otherwise} \end{cases}$$

(6.9)

where $f : \mathbb{R}^d \to \mathbb{R}$ is some function. From (6.2) we have

$$L(g_f) = \mathbb{P}(g_f(X) \neq Y) \leq \mathbb{P}(Yg_f(X) < 0) = \mathbb{P}(Yf(X) < 0).$$

From now on, when dealing with classifiers of the form (6.9), we will write $L(f)$ instead of $L(g_f)$ to keep the notation simple. Now we introduce the notion of a surrogate loss function.

Definition 6.1. A surrogate loss function is any nondecreasing function $\varphi : \mathbb{R} \to \mathbb{R}_+$, such that

$$\varphi(x) \geq 1_{\{x > 0\}}.$$ 

(6.10)

Some examples of commonly used surrogate losses:

1. Exponential, $\varphi(x) = e^x$
Let $\phi$ be a surrogate loss. Then for any $(x, y) \in \mathbb{R}^d \times \{-1, 1\}$ and any $f : \mathbb{R}^d \to \mathbb{R}$ we have
\[
yf(x) < 0 \implies \phi(-yf(x)) \geq 1_{\{-yf(x) > 0\}} = 1_{\{yf(x) < 0\}}.
\]
Therefore, defining the $\phi$-risk of $f$ by
\[
A_\phi(f) := \mathbb{E}[\phi(-Yf(X))]
\]
and its empirical version
\[
A_{\phi,n}(f) := \frac{1}{n} \sum_{i=1}^{n} \phi(-Y_if(X_i)),
\]
we see from (6.11) that
\[
L(f) \leq A_\phi(f) \quad \text{and} \quad L_n(f) \leq A_{\phi,n}(f).
\]

**Theorem 6.3.** Consider any learning algorithm $A = \{A_n\}_{n=1}^\infty$, where, for each $n$, the mapping $A_n$ receives the training sample $Z^n = (Z_1, \ldots, Z_n)$ as input and produces a function $\hat{f}_n : \mathbb{R}^d \to \mathbb{R}$ from some class $F$. Suppose that $F$ and the surrogate loss $\phi$ are chosen so that the following conditions are satisfied:

1. There exists some constant $B > 0$ such that
   \[
   \sup_{(x,y) \in \mathbb{R}^d \times \{-1,1\}} \sup_{f \in F} \phi(-yf(x)) \leq B
   \]
2. There exists some constant $M_\phi > 0$ such that $\phi$ is $M_\phi$-Lipschitz, i.e.,
   \[
   |\phi(u) - \phi(v)| \leq M_\phi |u - v|, \quad \forall u,v \in \mathbb{R}.
   \]

Then for any $n$ and any $\delta \in (0, 1)$ the following bound holds with probability at least $1 - \delta$:
\[
L(\hat{f}_n) \leq A_{\phi,n}(\hat{f}_n) + 4M_\phi \mathbb{E}R_n(F(X^n)) + B \sqrt{\frac{\log(1/\delta)}{2n}}.
\]

**Proof.** Using (6.12), we can write
\[
L(\hat{f}_n) \leq A_\phi(\hat{f}_n)
\]
\[
= A_{\phi,n}(\hat{f}_n) + A_\phi(\hat{f}_n) - A_{\phi,n}(\hat{f}_n)
\]
\[
\leq A_{\phi,n}(\hat{f}_n) + \sup_{f \in F} |A_\phi(f) - A_{\phi,n}(f)|.
\]
Now let $\mathcal{H}$ denote the class of functions $h : \mathbb{R}^d \times \{-1, 1\} \to \mathbb{R}$ of the form $h(x, y) = -yf(x)$, $f \in F$. Then
\[
\sup_{f \in F} |A_\phi(f) - A_{\phi,n}(f)| = \sup_{f \in F} \left| \mathbb{E}[\phi(-Yf(X))] - \frac{1}{n} \sum_{i=1}^{n} \phi(-Y_if(X_i)) \right|
\]
\[
= \sup_{h \in \mathcal{H}} \left| P(\phi \circ h) - P_n(\phi \circ h) \right|,
\]

(6.13)
where \( \varphi \circ h(z) := \varphi(h(z)) \) for every \( z = (x, y) \in \mathbb{R}^d \times \{-1, 1\} \). Let
\[
\Delta_n(Z^n) := \sup_{h \in \mathcal{H}} |P(\varphi \circ h) - P_n(\varphi \circ h)|
\]
\[
= \sup_{h \in \mathcal{H}} |P(\varphi \circ h - \varphi(0)) - P_n(\varphi \circ h - \varphi(0))|;
\]
where the second line follows from the fact that adding the same constant to each \( \varphi \circ h \) does not change the value of \( P_n(\varphi \circ h) - P(\varphi \circ h) \). Using the familiar symmetrization argument, we can write
\[
(6.14) \quad \mathbb{E}\Delta_n(Z^n) \leq 2\mathbb{E}R_n(\mathcal{H}_\varphi(Z^n)),
\]
where \( \mathcal{H}_\varphi \) denotes the class of all functions of the form \((x, y) \mapsto \varphi(h(x, y)) - \varphi(0), h \in \mathcal{H}\). We now use a very powerful result about the Rademacher averages called the contraction principle, which states the following \cite{LT91}: If \( \mathcal{A} \subset \mathbb{R}^n \) is a bounded set and \( F : \mathbb{R} \to \mathbb{R} \) is an \( M \)-Lipschitz function satisfying \( F(0) = 0 \), then
\[
(6.15) \quad R_n(F \circ \mathcal{A}) \leq 2MR_n(\mathcal{A}),
\]
where \( F \circ \mathcal{A} := \{(F(a_1), \ldots, F(a_n)) : a = (a_1, \ldots, a_n) \in \mathcal{A}\} \). (The proof of the contraction principle is somewhat involved, and we do not give it here.) Consider the function \( F(u) = \varphi(u) - \varphi(0) \). This function clearly satisfies \( F(0) = 0 \), and it is \( M_\varphi \)-Lipschitz, by our assumptions on \( \varphi \). Moreover, from our definition of \( \mathcal{H}_\varphi \), we immediately see that
\[
\mathcal{H}_\varphi(Z^n) = \{(\varphi(h(Z_1) - \varphi(0), \ldots, \varphi(h(Z_n) - \varphi(0)) : h \in \mathcal{H}\}
\]
\[
= \{(F(h(Z_1)), \ldots, F(h(Z_n))) : h \in \mathcal{H}\}
\]
\[
= F \circ \mathcal{H}(Z^n).
\]
Therefore, applying (6.15) to \( \mathcal{A} = \mathcal{H}(Z^n) \) and then using the resulting bound in (6.14), we obtain
\[
\mathbb{E}\Delta_n(Z^n) \leq 4M_\varphi \mathbb{E}R_n(\mathcal{H}(Z^n)).
\]
Furthermore, letting \( \sigma^n \) be an i.i.d. Rademacher tuple independent of \( Z^n \), we have
\[
R_n(\mathcal{H}(Z^n)) = \frac{1}{n} \mathbb{E}_{\sigma^n} \left[ \sup_{h \in \mathcal{H}} \left| \sum_{i=1}^{n} \sigma_i h(Z_i) \right| \right]
\]
\[
= \frac{1}{n} \mathbb{E}_{\sigma^n} \left[ \sup_{f \in \mathcal{F}} \left| \sum_{i=1}^{n} \sigma_i f(X_i) \right| \right]
\]
\[
= \frac{1}{n} \mathbb{E}_{\sigma^n} \left[ \sup_{f \in \mathcal{F}} \left| \sum_{i=1}^{n} \sigma_i f(X_i) \right| \right]
\]
\[
\equiv R_n(\mathcal{F}(X^n)),
\]
which leads to
\[
(6.16) \quad \mathbb{E}\Delta_n(Z^n) \leq 4M_\varphi \mathbb{E}R_n(\mathcal{F}(X^n)).
\]
Now, since every function \( \varphi \circ h \) is bounded between 0 and \( B \), the function \( \Delta_n(Z^n) \) has bounded differences with \( c_1 = \ldots = c_n = B/n \). Therefore, from (6.16) and from McDiarmid’s
inequality, we have for every $t > 0$ that
\[
P\left( \Delta_n(Z^n) \geq 4M_{\varphi}E_{\cal R}(\mathcal{F}(X^n)) + t \right) \leq P\left( \Delta_n(Z^n) \geq E\Delta_n(Z^n) + t \right) \leq e^{-2nt^2/B^2}.
\]
Choosing $t = B \sqrt{(2n)^{-1} \log(1/\delta)}$, we see that
\[
\Delta_n(Z^n) \leq 4M_{\varphi}E_{\cal R}(\mathcal{F}(X^n)) + B \sqrt{\frac{\log(1/\delta)}{2n}}
\]
with probability at least $1 - \delta$. Therefore, since
\[
L(\hat{f}_n) \leq A_{\varphi,n}(\hat{f}_n) + \Delta_n(Z^n),
\]
we see that (6.13) holds with probability at least $1 - \delta$. □

What the above theorem tells us is that the performance of the learned classifier $\hat{f}_n$ is controlled by the Rademacher average of the class $\mathcal{F}$, and we can always arrange it to be relatively small. We will now look at several specific examples.

3. Weighted linear combination of classifiers

Let $\mathcal{G} = \{g : \mathbb{R}^d \to \{-1, 1\}\}$ be a class of base classifiers (not to be confused with Bayes classifiers!), and consider the class
\[
\mathcal{F}_\lambda := \left\{ f = \sum_{j=1}^{N} c_j g_j : N \in \mathbb{N}, \sum_{j=1}^{N} |c_j| \leq \lambda; g_1, \ldots, g_N \in \mathcal{G} \right\},
\]
where $\lambda > 0$ is a tunable parameter. Then for each $f = \sum_{j=1}^{N} c_j g_j \in \mathcal{F}_\lambda$ the corresponding classifier $g_f$ of the form (6.9) is given by
\[
g_f(x) = \text{sgn} \left( \sum_{j=1}^{N} c_j g_j(x) \right).
\]
A useful way of thinking about $g_f$ is that, upon receiving a feature $x \in \mathbb{R}^d$, it computes the outputs $g_1(x), \ldots, g_N(x)$ of the $N$ base classifiers from $\mathcal{G}$ and then takes a weighted “majority vote” – indeed, if we had $c_1 = \ldots = c_N = \lambda/N$, then $\text{sgn}(g_f(x))$ would precisely correspond to taking the majority vote among the $N$ base classifiers. Note, by the way, that the number of base classifiers is not fixed, and can be learned from the data.

Now, Theorem 6.3 tells us that the performance of any learning algorithm that accepts a training sample $Z^n$ and produces a function $\hat{f}_n \in \mathcal{F}_\lambda$ is controlled by the Rademacher average $R_n(\mathcal{F}_\lambda(X^n))$. It turns out, moreover, that we can relate it to the Rademacher average of the base class $\mathcal{G}$. To start, note that
\[
\mathcal{F}_\lambda = \lambda \cdot \text{absconv} \mathcal{G},
\]
where
\[
\text{absconv} \mathcal{G} = \left\{ \sum_{j=1}^{N} c_j g_j : N \in \mathbb{N}; \sum_{j=1}^{N} c = |c_j| \leq 1; g_1, \ldots, g_N \in \mathcal{G} \right\}
\]
is the absolute convex hull of $\mathcal{G}$. Therefore
\[
R_n(\mathcal{F}_\lambda(X^n)) = \lambda \cdot R_n(\mathcal{G}(X^n)).
\]

66
Now note that the functions in $\mathcal{G}$ are binary-valued. Therefore, assuming that the base class $\mathcal{G}$ is a VC class, we will have

$$R_n(\mathcal{G}(X^n)) \leq C\sqrt{\frac{V(\mathcal{G})}{n}}.$$  

Combining these bounds with the bound of Theorem 6.3, we conclude that for any $\hat{f}_n$ selected from $\mathcal{F}_\lambda$ based on the training sample $Z^n$, the bound

$$L(\hat{f}_n) \leq A_{\varphi,n}(\hat{f}_n) + C\lambda M_{\varphi}\sqrt{\frac{V(\mathcal{G})}{n}} + B\sqrt{\frac{\log(1/\delta)}{2n}}$$

will hold with probability at least $1 - \delta$, where $B$ is the uniform upper bound on $\varphi(-yf(x))$, $f \in \mathcal{F}_\lambda$, $(x, y) \in \mathbb{R}^d \times \{-1, 1\}$ and $M_{\varphi}$ is the Lipschitz constant of the surrogate loss $\varphi$.

Note that the above bound involves only the VC dimension of the base class, which is typically small. On the other hand, the class $\mathcal{F}_\lambda$ obtained by forming weighted combinations of classifiers from $\mathcal{G}$ is extremely rich, and will generally have infinite VC dimension! But there is a price we pay: The first term is the empirical surrogate loss $A_{\varphi,n}(\hat{f}_n)$, rather than the empirical classification error $L_n(\hat{f}_n)$. However, it is possible to choose the surrogate $\varphi$ in such a way that $A_{\varphi,n}(\cdot)$ can be bounded in terms of a quantity related to the number of misclassified training examples. Here is an example.

Fix a positive parameter $\gamma > 0$ and consider

$$\varphi(x) = \begin{cases} 
0, & \text{if } x \leq -\gamma \\
1, & \text{if } x \geq 0 \\
1 + x/\gamma, & \text{otherwise}
\end{cases}$$

This is a valid surrogate loss with $B = 1$ and $M_{\varphi} = 1/\gamma$, but in addition we have $\varphi(x) \leq 1_{\{x > -\gamma\}}$, which implies that $\varphi(-yf(x)) \leq 1_{\{yf(x) < \gamma\}}$. Therefore, for any $f$ we have

$$A_{\varphi,n}(f) = \frac{1}{n} \sum_{i=1}^{n} \varphi(-Y_if(X_i)) \leq \frac{1}{n} \sum_{i=1}^{n} 1_{\{Y_if(X_i) < \gamma\}}.$$  

The quantity

$$L_n^\gamma(f) := \frac{1}{n} \sum_{i=1}^{n} 1_{\{Y_if(X_i) < \gamma\}}$$

is called the margin error of $f$. Notice that:

- For any $\gamma > 0$, $L_n^\gamma(f) \geq L_n(f)$
- The function $\gamma \mapsto L_n^\gamma(f)$ is increasing.

Notice also that we can write

$$L_n(f) = \frac{1}{n} \sum_{i=1}^{n} 1_{\{Y_if(X_i) < 0\}} + \frac{1}{n} \sum_{i=1}^{n} 1_{\{0 \leq Y_if(X_i) < \gamma\}},$$

where the first term is just $L_n(f)$, while the second term is the number of training examples that were classified correctly, but only with small “margin” (the quantity $Yf(X)$ is often called the margin of the classifier $f$).
Theorem 6.4 (Margin-based risk bound for weighted linear combinations). For any \( \gamma > 0 \), the bound

\[
L(\hat{f}_n) \leq L^*_{n}(\hat{f}_n) + \frac{C\lambda}{\gamma} \sqrt{\frac{V(G)}{n}} + \sqrt{\frac{\log(1/\delta)}{n}}
\]

holds with probability at least \( 1 - \delta \).

Remark 6.1. Note that the first term on the right-hand side of (6.19) increases with \( \gamma \), while the second term decreases with \( \gamma \). Hence, if the learned classifier \( \hat{f}_n \) has a small margin error for a large \( \gamma \), i.e., it classifies the training samples well and with high “confidence,” then its generalization error will be small.

4. Kernel machines

Another powerful way of building complicated classifiers from simple functions is by means of kernels. Kernel methods are popular in machine learning for a variety of reasons, not the least of which is that any algorithm that operates in a Euclidean space and relies only on the computation of inner products between feature vectors can be modified to work with any suitably well-behaved kernel.

To start with, let us define what we mean by a kernel. We will stick to Euclidean feature spaces, although everything works out for arbitrary separable metric spaces.

Definition 6.2. Let \( X \) be a closed subset of \( \mathbb{R}^d \). A real-valued function \( K : X \times X \rightarrow \mathbb{R} \) is called a Mercer kernel provided the following conditions are met:

1. It is symmetric, i.e., \( K(x, x') = K(x', x) \) for any \( x, x' \in X \).
2. It is continuous, i.e., if \( \{x_n\} \) is a sequence of points in \( X \) converging to a point \( x \), then
   \[
   \lim_{n \rightarrow \infty} K(x_n, x') = K(x, x'), \quad \forall x' \in X.
   \]
3. It is positive semidefinite, i.e., for all \( \alpha_1, \ldots, \alpha_n \in \mathbb{R} \) and all \( x_1, \ldots, x_n \in X \),

\[
\sum_{i,j=1}^{n} \alpha_i \alpha_j K(x_i, x_j) \geq 0.
\]

Remark 6.2. Another way to interpret the positive semidefiniteness condition is as follows. For any \( n \)-tuple \( x^n = (x_1, \ldots, x_n) \in X^n \), define the \( n \times n \) kernel Gram matrix

\[
G_K(x^n) := [K(x_i, x_j)]_{i,j=1}^{n}.
\]

Then (6.20) is equivalent to saying that \( G_K(x^n) \) is positive semidefinite in the usual sense, i.e., for any vector \( v \in \mathbb{R}^n \) we have

\[
\langle v, G_K(x^n)v \rangle \geq 0.
\]

Remark 6.3. From now on, we will just say “kernel,” but always mean “Mercer kernel.”

Here are some examples of kernels:

1. With \( X = \mathbb{R}^d \), \( K(x, x') = \langle x, x' \rangle \), the usual Euclidean inner product.
A more general class of kernels based on the Euclidean inner product can be constructed as follows. Let $X = \{ x \in \mathbb{R}^d : \| x \| \leq R \}$; choose any sequence $\{a_j\}_{j=0}^{\infty}$ of nonnegative reals such that

$$
\sum_{j=0}^{\infty} a_j R^{2j} < \infty.
$$

Then

$$
K(x, x') = \sum_{j=0}^{\infty} a_j \langle x, x' \rangle^j
$$

is a kernel.

(3) Let $X = \mathbb{R}^d$, and let $k : \mathbb{R}^d \to \mathbb{R}$ be a continuous function, which is reflection-symmetric, i.e., $k(-x) = k(x)$ for all $x$. Then $K(x, x') := k(x - x')$ is a kernel provided the Fourier transform of $k$,

$$
\hat{k}(\xi) := \int_{\mathbb{R}^d} e^{-i\langle \xi, x \rangle} k(x) dx,
$$

is nonnegative. A prime example is the Gaussian kernel, induced by the function $k(x) = e^{-\gamma \| x \|^2}$.

In all of the above cases, the first two properties of a Mercer kernel are easy to check. The third, i.e., positive semidefiniteness, requires a bit more work. For details, consult Section 2.5 of the book by Cucker and Zhou [CZ07].

The importance of kernels in machine learning stems from the fact that we can use them to represent (or approximate) arbitrarily complicated continuous functions on the feature space $X$. In order to take full advantage of this representational power, we must take a detour into the theory of Hilbert spaces.

4.1. A crash course on Hilbert spaces. Hilbert spaces are a powerful generalization of the usual Euclidean space with an inner product; once we have an inner product, we can introduce the notion of an angle and, consequently, orthogonality. Moreover, a Hilbert space has certain favorable convergence properties, so we can speak about (unique) linear projections of their elements onto closed linear subspaces. Let us make these ideas precise.

**Definition 6.3.** A real vector space $V$ is an inner product space if there exists a function $\langle \cdot, \cdot \rangle_V : V \times V \to \mathbb{R}$, which is:

1. **Symmetric:** $\langle v, v' \rangle_V = \langle v', v \rangle_V$ for all $v, v' \in V$
2. **Linear:** $\langle \alpha v_1 + \beta v_2, v' \rangle_V = \alpha \langle v_1, v' \rangle_V + \beta \langle v_2, v' \rangle_V$ for all $\alpha, \beta \in \mathbb{R}$ and all $v_1, v_2, v' \in V$
3. **Positive definite:** $\langle v, v \rangle_V \geq 0$ for all $v \in V$, and $\langle v, v \rangle_V = 0$ if and only if $v = 0$

Let $(V, \langle \cdot, \cdot \rangle_V)$ be an inner product space. Then we can define a norm on $V$ via

$$
\| v \|_V := \sqrt{\langle v, v \rangle_V}.
$$

It is easy to check that this is, indeed, a norm —

1. It is homogeneous: for any $v \in V$ and any $\alpha \in \mathbb{R}$,

$$
\| \alpha v \|_V = \sqrt{\langle \alpha v, \alpha v \rangle_V} = |\alpha| \sqrt{\langle v, v \rangle_V} = |\alpha| \cdot \| v \|_V
$$
(2) It satisfies the triangle inequality: for any \(v, v' \in V\),

\[
\|v + v'\|_V \leq \|v\|_V + \|v'\|_V. \tag{6.21}
\]

To prove this, we first need to establish another key property of \(\|\cdot\|_V\): the *Cauchy–Schwarz inequality*, which generalizes its classical Euclidean counterpart and says that

\[
|\langle v, v' \rangle_V| \leq \|v\|_V \|v'\|_V. \tag{6.22}
\]

To prove (6.22), we start with the observation that

\[
\|v - \lambda v'\|_V^2 = \langle v - \lambda v', v - \lambda v' \rangle_V \geq 0 \text{ for any } \lambda \in \mathbb{R}.
\]

Expanding this, we get

\[
\langle v - \lambda v', v - \lambda v' \rangle_V = \lambda^2 \|v'\|_V^2 - 2\lambda \langle v, v' \rangle_V + \|v\|_V^2 \geq 0.
\]

This is a quadratic function of \(\lambda\), and from the above we see that its graph does not cross the horizontal axis. Therefore, we must have

\[
4 |\langle v, v' \rangle_V|^2 \leq 4 \|v\|_V^2 \|v'\|_V^2 \iff |\langle v, v' \rangle_V| \leq \|v\|_V \|v'\|_V.
\]

Now we can write

\[
\begin{align*}
(\|v\|_V + \|v'\|_V)^2 &= \|v\|_V^2 + 2\|v\|_V \|v'\|_V + \|v'\|_V^2 \\
&\geq \|v\|_V^2 + 2\langle v, v' \rangle_V + \|v'\|_V^2 \\
&= \langle v, v \rangle_V + \langle v, v' \rangle_V + \langle v', v \rangle_V + \langle v', v' \rangle_V \\
&= \langle v + v', v + v' \rangle_V \\
&\equiv \|v + v'\|_V^2,
\end{align*}
\]

where the first step uses the Cauchy–Schwarz inequality, the second step uses the definition of \(\|\cdot\|_V\) and the symmetry of \(\langle \cdot, \cdot \rangle_V\), the third step uses the linearity of \(\langle \cdot, \cdot \rangle_V\), and the final step is, again, by definition. Since all norms are nonnegative, we can take square roots of both sides to get the triangle inequality.

(3) Finally, \(\|v\|_V \geq 0\), and \(\|v\|_V = 0\) if and only if \(v = 0\) – this is obvious from definitions.

Thus, an inner product space can be equipped with a norm that has certain special properties (mainly, the Cauchy–Schwarz inequality, since a lot of useful things follow from it alone).

Now that we have a norm, we can talk about *convergence* of sequences in \(V\):

**Definition 6.4.** Let \(\{v_n\}_{n=1}^{\infty}\) be a sequence of elements of \(V\). We say that it converges to \(v \in V\) if

\[
\lim_{n \to \infty} \|v_n - v\|_V = 0. \tag{6.23}
\]

**Remark 6.4.** This definition is valid for any norm on \(V\), not necessarily a norm induced by an inner product.

Any norm-convergent sequence has the property that, as \(n\) gets larger, its elements get closer and closer to one another. Specifically, suppose that \(\{v_n\}\) converges to \(v\). Then (6.23) implies that for any \(\varepsilon > 0\) we can choose \(n\) large enough, so that \(\|v_n - v\|_V < \varepsilon/2\) for all \(m \geq n\). But the triangle inequality gives

\[
\|v_n - v_m\|_V \leq \|v_n - v\|_V + \|v_m - v\|_V < \varepsilon, \quad \forall m \geq n.
\]
In other words, we have
\[ \lim_{m \to \infty} \| v_n - v_m \| = 0. \]
Since this holds for every \( n \), we can write
\[ \lim_{\min(m,n) \to \infty} \| v_n - v_m \| = 0. \] (6.24)

Any sequence \( \{v_n\} \) that has the property (6.24) is called a Cauchy sequence. We have just proved that any convergent sequence is Cauchy. However, the converse is not necessarily true: a Cauchy sequence does not have to be convergent. This motivates the following definition:

**Definition 6.5.** A normed space \((V, \| \cdot \|_V)\) is complete if any Cauchy sequence \( \{v_n\} \) of its elements is convergent. If the norm \( \| \cdot \|_V \) is induced by an inner product, then we say that \( V \) is a Hilbert space.

There is a standard procedure of starting with an inner product and the corresponding normed space and then completing it by adding the limits of all Cauchy sequences. We will not worry too much about this procedure. Here are a few standard examples of Hilbert spaces:

1. The Euclidean space \( V = \mathbb{R}^d \) with the usual inner product
   \[ \langle v, v' \rangle = \sum_{j=1}^{d} v_j v'_j. \]
   The corresponding norm is the familiar \( \ell_2 \) norm, \( \|v\| = \sqrt{\langle v, v \rangle} \).

2. More generally, if \( A \) is a positive definite \( d \times d \) matrix, then the inner product
   \[ \langle v, v' \rangle_A := \langle v, Av' \rangle \]
   induces the \( A \)-weighted norm \( \|v\|_A := \sqrt{\langle v, v \rangle_A} = \sqrt{\langle v, Av \rangle} \), which makes \( \mathbb{R}^d \) into a Hilbert space. The preceding example is a special case with \( A = I_d \), the \( d \times d \) identity matrix.

3. The space \( L^2(\mathbb{R}^d) \) of all square-integrable functions \( f : \mathbb{R}^d \to \mathbb{R} \), i.e.,
   \[ \int_{\mathbb{R}^d} f^2(x)dx < \infty, \]
   is a Hilbert space with the inner product
   \[ \langle f, g \rangle_{L^2(\mathbb{R}^d)} := \int_{\mathbb{R}^d} f(x)g(x)dx \]
   and the corresponding norm
   \[ \|f\|_{L^2(\mathbb{R}^d)} := \sqrt{\int_{\mathbb{R}^d} f^2(x)dx}. \]

4. Let \( (\Omega, \mathcal{B}, P) \) be a probability space. Then the space \( L^2(P) \) space of all real-valued random variables \( X : \Omega \to \mathbb{R} \) with finite second moment, i.e.,
   \[ \mathbb{E}X^2 = \int_{\Omega} X^2(\omega)P(d\omega) < +\infty, \]
is a Hilbert space with the inner product
\[ \langle X, X' \rangle_{L^2(P)} := \mathbb{E}[XX'] = \int \Omega X(\omega)X'(\omega)P(d\omega) \]
and the corresponding norm
\[ \|X\|_{L^2(P)} := \sqrt{\int \Omega |X(\omega)|^2P(d\omega)} \equiv \sqrt{\mathbb{E}X^2}. \]
From now on, we will denote a typical Hilbert space by \((H, \langle \cdot, \cdot \rangle_H)\); the induced norm will be denoted by \(\|\cdot\|_H\).

An enormous advantage of working with Hilbert spaces is the availability of the notion of orthogonality and orthogonal projection. Two elements \(h, g\) of a Hilbert space \(H\) are said to be orthogonal if \(\langle h, g \rangle_H = 0\).

Now consider a closed linear subspace \(H_1\) of \(H\), where “closed” means that the limit of any convergent sequence \(\{h_n\}\) of elements of \(H_1\) is also contained in \(H_1\). Then we have the following basic facts:

**Theorem 6.5.** Let \(H_1^\perp\) be the set of all \(h^\perp \in H\), such that \(\langle g, h^\perp \rangle_H = 0\) for all \(g \in H_1\). Then:

1. \(H_1^\perp\) is also a closed linear subspace of \(H\).
2. Any element \(g\) of \(H\) can be uniquely decomposed as \(g = h + h^\perp\), where \(h \in H_1\) and \(h^\perp \in H_1^\perp\).
3. Define the orthogonal projection \(\Pi : H \rightarrow H_1\) onto \(H_1\) through
   \[ \Pi g := h \quad \text{if} \ g = h + h^\perp \ \text{with} \ h \in H_1, \ h^\perp \in H_1^\perp. \]
   Then \(\Pi\) has the following properties:
   (a) It is a linear operator.
   (b) \(\Pi^2 = \Pi\), i.e., \(\Pi(\Pi g) = \Pi g\) for any \(g \in H\).
   (c) If \(g \in H_1\), then \(\Pi g = g\).
   (d) For any \(g \in H\) and any \(h \in H_1\),
   \[ \langle \Pi g, h \rangle_H = \langle g, h \rangle_H. \]
   (e) For any \(g \in H\), \(h = \Pi g \in H_1\) is the unique solution of the optimization problem minimize \(\|h - g\|\) subject to \(h \in H_1\).

**Remark 6.5.** It is important for \(H_1\) to be a closed linear subspace of \(H\) for the above results to hold.

**4.2. Reproducing kernel Hilbert spaces.** Now let us return to our original goal. Suppose we have a fixed kernel \(K\) on our feature space \(X\) (which we assume to be a closed subset of \(\mathbb{R}^d\)). Let \(L_K(X)\) be the linear span of the set \(\{K(x', \cdot) : x' \in X\}\), i.e., the set of all functions \(f : X \rightarrow \mathbb{R}\) of the form
\[ f(x) = \sum_{j=1}^N c_j K(x_j, x) \]
for all possible choices of \(N \in \mathbb{N}, c_1, \ldots, c_N \in \mathbb{R}\), and \(x_1, \ldots, x_N \in X\). It is easy to see that \(L_K(X)\) is a vector space: for any two functions \(f, f'\) of the form (6.25), their sum is also of
that form; if we multiply any \( f \in \mathcal{L}_K(X) \) by a scalar \( c \in \mathbb{R} \), we will get another element of \( \mathcal{L}_K(X) \); and the zero function is clearly in \( \mathcal{L}_K(X) \). It turns out that, for any (Mercer) kernel \( K \), we can complete \( \mathcal{L}_K(X) \) into a Hilbert space of functions that can potentially represent any continuous function from \( X \) into \( \mathbb{R} \), provided \( K \) is chosen appropriately.

The following result is essential (for the proof, see Section 2.4 of Cucker and Zhou [CZ07]):

**Theorem 6.6.** Let \( X \) be a closed subset of \( \mathbb{R}^d \), and let \( K : X \times X \to \mathbb{R} \) be a Mercer kernel. Then there exists a unique Hilbert space \((\mathcal{H}_K; \langle \cdot, \cdot \rangle_K)\) of real-valued functions on \( X \) with the following properties:

1. For all \( x \in X \), the function \( K_x(\cdot) := K(x, \cdot) \) is an element of \( \mathcal{H}_K \), and \( \langle K_x, K_{x'} \rangle_K = K(x, x') \) for all \( x, x' \in X \).
2. The linear space \( \mathcal{L}_K(X) \) is dense in \( \mathcal{H}_K \), i.e., for any \( f \in \mathcal{H}_K \) and any \( \varepsilon > 0 \) there exist some \( N \in \mathbb{N}, c_1, \ldots, c_N \in \mathbb{R} \), and \( x_1, \ldots, x_N \in X \), such that

\[
\left\| f - \sum_{j=1}^{N} c_j K_{x_j} \right\|_K < \varepsilon.
\]

3. For all \( f \in \mathcal{H}_K \) and all \( x \in X \),

\[
(6.26) \quad f(x) = \langle K_x, f \rangle_K.
\]

Moreover, the functions in \( \mathcal{H}_K \) are continuous. The Hilbert space \( \mathcal{H}_K \) is called the Reproducing Kernel Hilbert Space (RKHS) associated with \( K \); the property (6.26) is referred to as the reproducing kernel property.

**Remark 6.6.** The reproducing kernel property essentially states that the value of any function \( f \in \mathcal{H}_K \) at any point \( x \in X \) can be “extracted” by projecting \( f \) onto the function \( K_x(\cdot) = K(x, \cdot) \), i.e., a copy of the kernel \( K \) “centered” at the point \( x \). It is easy to prove when \( f \in \mathcal{L}_K(X) \). Indeed, if \( f \) has the form (6.25), then

\[
\langle f, K_x \rangle_K = \left\langle \sum_{j=1}^{N} c_j K_{x_j}, K_x \right\rangle_K
= \sum_{j=1}^{N} c_j \langle K_{x_j}, K_x \rangle_K
= \sum_{j=1}^{N} c_j K(x_j, x)
= f(x).
\]

Since any \( f \in \mathcal{H}_K \) can be expressed as a limit of functions from \( \mathcal{L}_K(X) \), the proof of (6.26) for a general \( f \) follows by continuity.

Now we pick a kernel \( K \) on our feature space and consider classifiers of the form

\[
g_f(x) = \text{sgn} f(x) \equiv \begin{cases} 
1, & \text{if } f(x) \geq 0 \\
-1, & \text{otherwise}
\end{cases}
\]
with the underlying \( f \) taken from a suitable subset of the RKHS \( \mathcal{H}_K \). One choice, which underlies such things as the Support Vector Machine, is to take a ball in \( \mathcal{H}_K \): given some \( \lambda > 0 \), let

\[
\mathcal{F}_\lambda := \{ f \in \mathcal{H}_K : \| f \|_K \leq \lambda \}.
\]

This set is the closure (in the \( \| \cdot \|_K \) norm) of the convex set

\[
\left\{ \sum_{j=1}^{N} c_j K_{x_j} : N \in \mathbb{N}; c_1, \ldots, c_N \in \mathbb{R}; x_1, \ldots, x_N \in X; \sum_{i,j=1}^{N} c_i c_j K(x_i, x_j) \leq \lambda^2 \right\} \subset \mathcal{L}_K(X),
\]

and is itself convex. Now, as we already know, the performance of any learning algorithm that chooses an element \( \hat{f}_n \in \mathcal{F}_\lambda \) in a data-dependent way is controlled by the Rademacher average \( R_n(\mathcal{F}_\lambda(X^n)) \). It turns out that this Rademacher average is fairly easy to estimate. Indeed, using the reproducing kernel property (6.26) and then the linearity of the inner product \( \langle \cdot, \cdot \rangle_K \), we can write

\[
R_n(\mathcal{F}_\lambda(X^n)) = \frac{1}{n} \mathbb{E}_{\sigma^n} \sup_{f : \| f \|_K \leq \lambda} \left| \sum_{i=1}^{n} \sigma_i f(X_i) \right|
\]

\[
= \frac{1}{n} \mathbb{E}_{\sigma^n} \sup_{f : \| f \|_K \leq \lambda} \left| \sum_{i=1}^{n} \sigma_i \langle f, K_{X_i} \rangle_K \right|
\]

\[
= \frac{1}{n} \mathbb{E}_{\sigma^n} \sup_{f : \| f \|_K \leq \lambda} \left\langle f, \sum_{i=1}^{n} \sigma_i K_{X_i} \right\rangle_K.
\]

Now, using the Cauchy–Schwarz inequality (6.22), it is not hard to show that

\[
\sup_{f : \| f \|_K \leq \lambda} |\langle f, g \rangle_K| = \lambda \| g \|_K
\]

for any \( g \in \mathcal{H}_K \). Therefore,

\[
R_n(\mathcal{F}_\lambda(X^n)) = \frac{\lambda}{n} \mathbb{E}_{\sigma^n} \left\| \sum_{i=1}^{n} \sigma_i K_{X_i} \right\|_K.
\]

Now we exploit the following easily proved fact: for any \( n \) functions \( g_1, \ldots, g_n \in \mathcal{H}_K \),

\[
(6.27) \quad \mathbb{E}_{\sigma^n} \left\| \sum_{i=1}^{n} \sigma_i g_i \right\|_K \leq \sqrt{\sum_{i=1}^{n} \| g_i \|_K^2}.
\]

The proof of this is in two steps: First, we use the concavity of the square root to write

\[
\mathbb{E}_{\sigma^n} \left\| \sum_{i=1}^{n} \sigma_i g_i \right\|_K^2 \leq \mathbb{E} \left\| \sum_{i=1}^{n} \sigma_i g_i \right\|_K^2.
\]

Then we expand the squared norm:

\[
\left\| \sum_{i=1}^{n} \sigma_i g_i \right\|_K^2 = \left\langle \sum_{i=1}^{n} \sigma_i g_i, \sum_{i=1}^{n} \sigma_i g_i \right\rangle_K = \sum_{i,j=1}^{n} \sigma_i \sigma_j \langle g_i, g_j \rangle_K.
\]
And finally we take the expectation over $\sigma^n$ and use the fact that $\mathbb{E}[\sigma_i \sigma_j] = 1$ if $i = j$ and 0 otherwise to get

$$
\mathbb{E} \left\| \sum_{i=1}^n \sigma_i g_i \right\|^2_K = \sum_{i=1}^n \langle g_i, g_i \rangle_K = \sum_{i=1}^n \|g_i\|^2_K.
$$

Hence, we obtain

$$
R_n(\mathcal{F}_\lambda(X^n)) \leq \lambda \sqrt{n \sum_{i=1}^n \langle K_{X_i}, K_{X_i} \rangle_K} = \lambda \sqrt{n \sum_{i=1}^n K(X_i, X_i)}.
$$

Finally, taking the expectation w.r.t. $X^n$ and once more using concavity of the square root, we have

$$
\mathbb{E} R_n(\mathcal{F}_\lambda(X^n)) \leq \lambda \sqrt{\mathbb{E} K(X, X) / \sqrt{n}}.
$$

4.3. Empirical risk minimization in an RKHS. Another advantage of working with kernels is that, in many cases, a minimizer of empirical risk over a sufficiently regular subset of an RKHS will have the form of a linear combination of kernels centered at the training feature points. The results ensuring this are often referred to in the literature as representer theorems. Here is one such result (due, in a slightly different form, to Schölkopf, Herbrich, and Smola [SHS01]), sufficiently general for our purposes:

**Theorem 6.7 (The generalized representer theorem).** Let $X$ be a closed subset of $\mathbb{R}^d$ and let $Y$ be a subset of the reals. Consider a nonnegative loss function $\ell : Y \times Y \to \mathbb{R}^+$. Let $K$ be a Mercer kernel on $X$, and let $\mathcal{H}_K$ be the corresponding RKHS.

Let $(X_1, Y_1), \ldots, (X_n, Y_n)$ be an i.i.d. sample from some distribution $P = P_{XY}$ on $X \times Y$, let $\mathcal{H}_n$ be the closed linear subspace of $\mathcal{H}_K$ spanned by $\{K_{X_i} : 1 \leq i \leq n\}$, and let $\Pi_n$ denote the orthogonal projection onto $\mathcal{H}_n$. Let $\mathcal{F}$ be a subset of $\mathcal{H}_K$, such that $\Pi_n(\mathcal{F}) \subseteq \mathcal{F}$. Then

$$
\inf_{f \in \mathcal{F}} \frac{1}{n} \sum_{i=1}^n \ell(Y_i, f(X_i)) = \inf_{f \in \Pi_n(\mathcal{F})} \frac{1}{n} \sum_{i=1}^n \ell(Y_i, f(X_i)),
$$

and if a minimizer of the left-hand side of (6.28) exists, then it can be taken to have the form

$$
\hat{f}_n = \sum_{i=1}^n c_i K_{X_i}
$$

for some $c_1, \ldots, c_n \in \mathbb{R}$.

**Remark 6.7.** Note that both the subspace $\mathcal{H}_n$ and the corresponding orthogonal projection $\Pi_n$ are random objects, since they depend on the random features $X^n$.

**Proof.** Since $K_{X_i} \in \mathcal{H}_n$ for every $i$, by Theorem 6.5 we have

$$
\langle f, K_{X_i} \rangle_K = \langle \Pi_n f, K_{X_i} \rangle_K, \quad \forall f \in \mathcal{H}_K.
$$

Moreover, from the reproducing kernel property (6.26) we deduce that

$$
f(X_i) = \langle f, K_{X_i} \rangle_K = \langle \Pi_n f, K_{X_i} \rangle_K = \Pi_n f(X_i).
$$
Therefore, for every \( f \in \mathcal{F} \) we can write
\[
\frac{1}{n} \sum_{i=1}^{n} \ell(Y_i, f(X_i)) = \frac{1}{n} \sum_{i=1}^{n} \ell(Y_i, \Pi_n f(X_i)).
\]

This implies that
\[
\inf_{f \in \mathcal{F}} \frac{1}{n} \sum_{i=1}^{n} \ell(Y_i, f(X_i)) = \inf_{f \in \mathcal{F}} \frac{1}{n} \sum_{i=1}^{n} \ell(Y_i, \Pi_n f(X_i)) = \inf_{g \in \Pi_n(\mathcal{F})} \frac{1}{n} \sum_{i=1}^{n} \ell(Y_i, g(X_i)).
\] (6.30)

Now suppose that \( f_n \in \mathcal{F} \) achieves the infimum on the left-hand side of (6.30). Then its projection \( \hat{f}_n = \Pi_n f_n \) onto \( \mathcal{H}_n \) achieves the infimum on the right-hand side. Moreover, since \( \Pi_n(\mathcal{F}) \subseteq \mathcal{F} \) by hypothesis, we may conclude that \( \hat{f}_n \in \mathcal{H}_n \). Since every element of \( \mathcal{H}_n \) has the form (6.29), the theorem is proved. \( \square \)

In the classification setting, we may take \( Y = \{-1, +1\} \) and consider the problem of minimizing the empirical surrogate loss
\[
A_{\varphi,n}(f) = \frac{1}{n} \sum_{i=1}^{n} \varphi(-Y_i f(X_i))
\]
over the ball \( \mathcal{F}_\lambda \) in a suitable RKHS \( \mathcal{H}_K \). By the above theorem, we may write this problem in the following form:

\[
\begin{align*}
(6.31a) & \quad \min_{c_1, \ldots, c_n \in \mathbb{R}} \frac{1}{n} \sum_{i=1}^{n} \varphi \left( -Y_i \sum_{j=1}^{n} c_j K(X_i, X_j) \right) \\
(6.31b) & \quad \text{subject to } \sum_{i,j=1}^{n} c_i c_j K(X_i, X_j) \leq \lambda^2
\end{align*}
\]

Suppose the surrogate loss function \( \varphi \) is convex. Then the objective function in (6.31) is convex as well, and the decision variables \( c_1, \ldots, c_n \in \mathbb{R} \) are subject to a quadratic constraint. Thus, (6.31) is an instance of a \textit{quadratically constrained convex program} (QCCP). Moreover, when \( \varphi \) is such that the objective is \textit{quadratic} in \( c_1, \ldots, c_n \), then we have a \textit{quadratically constrained quadratic problem} (QCQP), which can be solved very efficiently using interior point methods. For detailed background see the text of Boyd and Vandenberghe [BV04]. Many popular machine learning algorithms can be cast in the form (6.31). For instance, if we let \( \varphi \) be the hinge loss \( \varphi(u) = (u+1)^+ \), then (6.31) corresponds to the \textit{Support Vector Machine} (SVM) algorithm — more precisely, the SVM is the \textit{scalarized} version of (6.31), i.e., it has the form
\[
\min_{c_1, \ldots, c_n \in \mathbb{R}} \left\{ \frac{1}{n} \sum_{i=1}^{n} \left( 1 - Y_i \sum_{j=1}^{n} c_j K(X_i, X_j) \right) \right\}_+ + \tau \sum_{i,j=1}^{n} c_i c_j K(X_i, X_j)
\]
for some regularization parameter \( \tau > 0 \).
5. Convex risk minimization

Choosing a convex surrogate loss function \( \varphi \) has many advantages in general. First of all, we may arrange things in such a way that the function \( f^* \) that minimizes the surrogate loss \( A_\varphi(f) \) over all measurable \( f : X \rightarrow \mathbb{R} \) induces the Bayes classifier:

\[
\operatorname{sgn} f^*(x) \equiv \begin{cases} 
1, & \text{if } \eta(x) > 1/2 \\
-1, & \text{otherwise}
\end{cases}
\]  

(6.32) 

\[ \eta(x) = \begin{cases} 
1, & \text{if } \eta(x) > 1/2 \\
1 - \eta(x), & \text{otherwise}
\end{cases} \]

Theorem 6.8. Let \( P = P_{XY} \) be the joint distribution of the feature \( X \in \mathbb{R}^d \) and the binary label \( Y \in \{-1, +1\} \), and let \( \eta(x) = \mathbb{P}[Y = 1|X = x] \) be the corresponding regression function. Consider a surrogate loss function \( \varphi \), which is strictly convex and differentiable. Then the unique minimizer of the surrogate loss \( A_\varphi(f) = E[\varphi(-Yf(X))] \) over all (measurable) functions \( f : X \rightarrow \mathbb{R} \) has the form

\[
f^*(x) = \arg \min_{u \in \mathbb{R}} h_{\eta(x)}(u),
\]

where for each \( \eta \in [0, 1] \) we have \( h_\eta(u) := \eta \varphi(-u) + (1 - \eta)\varphi(u) \). Moreover, \( f^*(x) \) is positive if and only if \( \eta(x) > 1/2 \), i.e., the induced sign classifier \( g_f(x) = \operatorname{sgn}(f^*(x)) \) is the Bayes classifier (1.2).

Proof. By the law of iterated expectation,

\[
A_\varphi(f) = E[\varphi(-Yf(X))] = E[E[\varphi(-Yf(X))|X]].
\]

Hence,

\[
\inf_f A_\varphi(f) = \inf_f E[E[\varphi(-Yf(X))|X]] = E\left[ \inf_{u \in \mathbb{R}} E[\varphi(-Yu)|X = x] \right].
\]

For every \( x \in X \), we have

\[
E[\varphi(-Yu)|X = x] = \mathbb{P}[Y = 1|X = x] \varphi(-u) + \mathbb{P}[Y = -1|X = x] \varphi(u)
= \eta(x) \varphi(-u) + (1 - \eta(x)) \varphi(u)
\equiv h_{\eta(x)}(u).
\]

Since \( \varphi \) is strictly convex and differentiable, so is \( h_\eta \) for every \( \eta \in [0, 1] \). Therefore, \( \inf_{u \in \mathbb{R}} h_\eta(u) \) exists, and is achieved by a unique \( u^* \); in particular,

\[
f^*(x) = \arg \min_{u \in \mathbb{R}} h_{\eta(x)}(u).
\]

To find the \( u^* \) minimizing \( h_\eta \), we differentiate \( h_\eta \) w.r.t. \( u \) and set the derivative to zero. Since

\[
h'_\eta(u) = -\eta \varphi'(-u) + (1 - \eta) \varphi'(u),
\]

the point of minimum \( u^* \) is the solution to the equation

\[
\frac{\varphi'(u)}{\varphi'(-u)} = \frac{\eta}{1 - \eta}.
\]
Suppose $\eta > 1/2$; then
\[
\frac{\varphi'(u)}{\varphi'(-u)} > 1.
\]
Since $\varphi$ is strictly convex, its derivative $\varphi'$ is strictly increasing. Hence, $u^* > -u^*$ which implies that $u^* > 0$. Conversely, if $u^* \leq 0$, then $u^* \leq -u^*$, so $\varphi'(u^*) \leq \varphi'(-u^*)$, which means that $\eta/(1 - \eta) \leq 1$, i.e., $\eta \leq 1/2$. Thus, we conclude that $f^*(x)$, which is the minimizer of $h_{\eta(x)}$, is positive if and only if $\eta(x) > 1/2$, i.e., $\text{sgn}(f^*(x))$ is the Bayes classifier. $\square$

Secondly, under some additional regularity conditions it is possible to relate the minimum surrogate loss
\[
A^*_\varphi := \inf_f A_\varphi(f)
\]
to the Bayes rate
\[
L^* = \inf_f \mathbb{P}(Y \neq \text{sgn} f(X)),
\]
where in both expressions the infimum is over all measurable functions $f : X \rightarrow \mathbb{R}$:

**Theorem 6.9.** Assume that the surrogate loss function $\varphi$ satisfies the conditions of our basic surrogate bound, and that there exist positive constants $s \geq 1$ and $c$, such that the inequality
\[
L(f) - L^* \leq c \left( A_\varphi(f) - A^*_\varphi \right)^{1/s}
\]
holds for any measurable function $f : X \rightarrow \mathbb{R}$. Consider the learning algorithm that minimizes empirical surrogate loss over some class $\mathcal{F}$:

\[
\hat{f}_n = \arg \min_{f \in \mathcal{F}} A_{\varphi,n}(f) = \arg \min_{f \in \mathcal{F}} \frac{1}{n} \sum_{i=1}^{n} \varphi(-Y_i f(X_i)).
\]

Then
\[
L(\hat{f}_n) - L^* \leq 2^{1/s} c \left( 4 M_\varphi \mathbb{E} R_n(\mathcal{F}(X_n)) + B \sqrt{\frac{\log(1/\delta)}{2n}} \right)^{1/s} + c \left( \inf_{f \in \mathcal{F}} A_\varphi(f) - A^*_\varphi \right)^{1/s}
\]
with probability at least $1 - \delta$. 78
Proof. We have the following:

(6.36) \[ L(\hat{f}_n) - L^* \leq c \left( A_\varphi(\hat{f}_n) - A_\varphi^* \right)^{1/s} \]

(6.37) \[
= c \left( A_\varphi(\hat{f}_n) - \inf_{f \in F} A_\varphi(f) + \inf_{f \in F} A_\varphi(f) - A_\varphi^* \right)^{1/s}
\]

(6.38) \[
\leq c \left( A_\varphi(\hat{f}_n) - \inf_{f \in F} A_\varphi(f) \right)^{1/s} + c \left( \inf_{f \in F} A_\varphi(f) - A_\varphi^* \right)^{1/s}
\]

(6.39) \[
\leq 2^{1/s} c \left( \sup_{f \in F} |A_{\varphi,n}(f) - A_\varphi(f)| \right)^{1/s} + c \left( \inf_{f \in F} A_\varphi(f) - A_\varphi^* \right)^{1/s}
\]

(6.40) \[
\leq 2^{1/s} c \left( 4M_{\varphi} ER_n(\mathcal{F}(X^n)) + B \sqrt{\frac{\log(1/\delta)}{2n}} \right)^{1/s} + c \left( \inf_{f \in F} A_\varphi(f) - A_\varphi^* \right)^{1/s} \quad \text{w.p.} \geq 1 - \delta,
\]

where:

- (6.36) follows from (6.33);
- (6.38) follows from the inequality \((a + b)^{1/s} \leq a^{1/s} + b^{1/s}\) that holds for all \(a, b \geq 0\) and all \(s \geq 1\);
- (6.39) and (6.40) follow from the same argument as the one used in the proof of the basic surrogate bound.

This completes the proof. \(\square\)

Remark 6.8. Condition (6.33) is often easy to check. For instance, Zhang [Zha04] proved that it is satisfied, provided the inequality

(6.41) \[
\left| \frac{1}{2} - \eta \right|^s \leq (2c)^s \left( 1 - \inf_u h(\eta) \right)
\]

holds for all \(\eta \in [0, 1]\). For instance, (6.41) holds for the exponential loss \(\varphi(u) = e^u\) and the logit loss \(\varphi(u) = \log_2(1 + e^u)\) with \(s = 2\) and \(c = 2\sqrt{2}\); for the hinge loss \(\varphi(u) = (u + 1)_+\), (6.41) holds with \(s = 1\) and \(c = 4\).

What Theorem 6.9 says is that, assuming the expected Rademacher average \(ER_n(\mathcal{F}(X^n)) = O(1/\sqrt{n})\), the difference between the generalization error of the Convex Risk Minimization algorithm (6.34) and the Bayes rate \(L^*\) is, with high probability, bounded by the combination of two terms: the \(O(n^{-1/2s})\) “estimation error” term and the \((\inf_{f \in F} A_\varphi(f) - A_\varphi^*)^{1/s}\) “approximation error” term. If the hypothesis space \(\mathcal{F}\) is rich enough, so that \(\inf_{f \in F} A_\varphi(f) = A_\varphi^*\), then the difference between \(L(\hat{f}_n)\) and \(L^*\) is, with high probability, bounded as \(O(1/n^{-2s})\), independently of the dimension \(d\) of the feature space.
Regression with quadratic loss

Regression with quadratic loss is another basic problem studied in statistical learning theory. We have a random couple \( Z = (X, Y) \), where, as before, \( X \) is an \( \mathbb{R}^d \)-valued feature vector (or input vector) and \( Y \) is the real-valued response (or output). We assume that the unknown joint distribution \( P = P_Z = P_{XY} \) of \((X, Y)\) belongs to some class \( P \) of probability distributions over \( \mathbb{R}^d \times \mathbb{R} \).

The learning problem, then, is to produce a predictor of \( Y \) given \( X \) on the basis of an i.i.d. training sample \( Z^n = (Z_1, \ldots, Z_n) = ((X_1, Y_1), \ldots, (X_n, Y_n)) \) from \( P \). A predictor is just a (measurable) function \( f : \mathbb{R}^d \to \mathbb{R} \), and we evaluate its performance by the expected quadratic loss

\[
L(f) := E[(Y - f(X))^2].
\]

As we have seen before, the smallest expected loss is achieved by the regression function \( f^* : \mathbb{R}^d \to \mathbb{R} \), i.e.,

\[
L^* := \inf_{f} L(f) = L(f^*) = E[(X - E[Y|X])^2].
\]

Moreover, for any other \( f \) we have

\[
L(f) = L^* + \| f - f^* \|^2_{L^2(P_X)},
\]

where

\[
\| f - f^* \|^2_{L^2(P_X)} := \int_{R^d} |f(x) - f^*(x)|^2 P_X(dx).
\]

Since we do not know \( P \), in general we cannot hope to learn \( f^* \), so, as before, instead we aim at finding a good approximation to the best predictor in some class \( F \) of functions \( f : \mathbb{R}^d \to \mathbb{R} \), i.e., to use the training data \( Z^n \) to construct a predictor \( \hat{f}_n \in F \), such that

\[
L(\hat{f}_n) \approx L^*(F) := \inf_{f \in F} L(f)
\]

with high probability.

We will assume that the marginal distribution \( P_X \) of the feature vector is supported on a closed subset \( X \subseteq \mathbb{R}^d \), and that the joint distribution \( P \) of \((X, Y)\) is such that, with probability one,

\[
|Y| \leq M \quad \text{and} \quad |f^*(X)| \leq M.
\]

for some constant \( 0 < M < \infty \). Thus we can assume that the training samples belong to the set \( Z = X \times [-M, M] \). We will also assume that the class \( F \) is a subset of a suitable reproducing kernel Hilbert space (RKHS) \( \mathcal{H}_K \) induced by some Mercer kernel \( K : X \times X \to \mathbb{R} \). It will be useful to define

\[
C_K := \sup_{x \in X} \sqrt{K(x,x)};
\]
we will assume that $C_K$ is finite. The following simple bound will come in handy:

**Lemma 7.1.** For any function $f : X \to \mathbb{R}$, define the sup norm
\begin{equation}
\|f\|_\infty := \sup_{x \in X} |f(x)|.
\end{equation}
Then for any $f \in \mathcal{H}_K$ we have
\begin{equation}
\|f\|_\infty \leq C_K \|f\|_K.
\end{equation}

**Proof.** For any $f \in \mathcal{H}_K$ and $x \in X$,
\[ |f(x)| = |\langle f, K_x \rangle_K| \leq \|f\|_K \|K_x\|_K = \|f\|_K \sqrt{K(x, x)}, \]
where the first step is by the reproducing kernel property, while the second step is by Cauchy–Schwarz. Taking the supremum of both sides over $X$, we get (7.3). \qed

1. **ERM over a ball in RKHS**

First, we will look at the simplest case: ERM over a ball in $\mathcal{H}_K$. Thus, we pick the radius $\lambda > 0$ and take
\[ \mathcal{F} = \mathcal{F}_\lambda = \{ f \in \mathcal{H}_K : \|f\|_K \leq \lambda \}. \]
The ERM algorithm outputs the predictor
\[ \hat{f}_n = \arg \min_{f \in \mathcal{F}_\lambda} L_n(f) \equiv \arg \min_{f \in \mathcal{F}_\lambda} \frac{1}{n} \sum_{i=1}^{n} (Y_i - f(X_i))^2, \]
where $L_n(f)$ denotes, as usual, the empirical loss (in this case, empirical quadratic loss) of $f$.

**Theorem 7.1.** With probability at least $1 - \delta$,
\begin{equation}
L(\hat{f}_n) \leq L^*(\mathcal{F}_\lambda) + \frac{16(M + C_K \lambda)^2}{\sqrt{n}} + (M^2 + C_K^2 \lambda^2) \sqrt{\frac{32 \log(1/\delta)}{n}}.
\end{equation}

**Proof.** First let us introduce some notation. Let us denote the quadratic loss function $(y, u) \mapsto (y - u)^2$ by $\ell(y, u)$, and for any $f : \mathbb{R}^d \to \mathbb{R}$ let
\[ \ell \cdot f(x, y) := \ell(y, f(x)) = (y - f(x))^2. \]
Let $\ell \cdot \mathcal{F}_\lambda$ denote the function class $\{ \ell \cdot f : f \in \mathcal{F}_\lambda \}$.
Let $f^*_\lambda$ denote any minimizer of $L(f)$ over $\mathcal{F}_\lambda$, i.e., $L(f^*_\lambda) = L^*(\mathcal{F}_\lambda)$. As usual, we write
\begin{align}
L(\hat{f}_n) - L^*(\mathcal{F}_\lambda) &= L(\hat{f}_n) - L^*(\mathcal{F}_\lambda) \\
&= L(\hat{f}_n) - L_n(\hat{f}_n) + L_n(\hat{f}_n) - L_n(f^*_\lambda) + L_n(f^*_\lambda) - L(f^*_\lambda) \\
&\leq 2 \sup_{f \in \mathcal{F}_\lambda} |L_n(f) - L(f)| \\
&= 2 \sup_{f \in \mathcal{F}_\lambda} |P_n(\ell \cdot f) - P(\ell \cdot f)|
\end{align}
(7.5)
where we have defined the uniform deviation
\[ \Delta_n(\ell \cdot \mathcal{F}) := \sup_{f \in \mathcal{F}} |P_n(\ell \cdot f) - P(\ell \cdot f)|. \]
Next we show that, as a function of the training sample $Z^n$, $g(Z^n) = \Delta_n(\ell \cdot F_\lambda)$ has bounded differences. Indeed, for any $1 \leq i \leq n$, any $z'^n \in Z^n$, and any $z'_i \in Z$, let $z^n_{(i)}$ denote $z^n$ with the $i$th coordinate replaced by $z'_i$. Then

$$|g(z^n) - g(z^n_{(i)})| \leq \frac{1}{n} \sup_{f \in F_\lambda} \left| (y_i - f(x_i))^2 - (y'_i - f(x'_i))^2 \right|$$

$$\leq \frac{2}{n} \sup_{x \in \mathcal{X}} \sup_{|y| \leq M} \sup_{f \in F_\lambda} |y - f(x)|^2$$

$$\leq \frac{4}{n} \left( M^2 + \sup_{f \in F_\lambda} \|f\|_\infty^2 \right)$$

$$\leq \frac{4}{n} \left( M^2 + C_K^2 \lambda^2 \right),$$

where the last line is by Lemma 7.1. Thus, $\Delta_n(\ell \cdot F_\lambda)$ has the bounded difference property with $c_1 = \ldots = c_n = 4(M^2 + C_K^2 \lambda^2)/n$, so McDiarmid’s inequality says that, for any $t > 0$,

$$\mathbb{P}(\Delta_n(\ell \cdot F_\lambda) \geq \mathbb{E}\Delta_n(\ell \cdot F_\lambda) + t) \leq \exp\left( -\frac{nt^2}{8(M^2 + C_K^2 \lambda^2)^2} \right).$$

Therefore, letting

$$t = 2(M^2 + C_K^2 \lambda^2)\sqrt{\frac{2 \log(1/\delta)}{n}},$$

we see that

$$\Delta_n(\ell \cdot F_\lambda) \leq \mathbb{E}\Delta_n(\ell \cdot F_\lambda) + 2(M^2 + C_K^2 \lambda^2)\sqrt{\frac{2 \log(1/\delta)}{n}},$$

with probability at least $1 - \delta$. Moreover, by symmetrization we have

$$\mathbb{E}\Delta_n(\ell \cdot F_\lambda) \leq 2\mathbb{E}R_n(\ell \cdot F_\lambda(Z^n)),$$

where

$$R_n(\ell \cdot F_\lambda(Z^n)) = \frac{1}{n} \mathbb{E}_\sigma^n \sup_{f \in F_\lambda} \left| \sum_{i=1}^n \sigma_i \ell \cdot f(Z_i) \right|$$

is the Rademacher average of the (random) set

$$\ell \cdot F_\lambda(Z^n) = \{(\ell \cdot f(Z_1), \ldots, \ell \cdot f(Z_n)) : f \in F_\lambda\}$$

$$= \{(Y_1 - f(X_1)^2, \ldots, (Y_n - f(X_n))^2) : f \in F_\lambda\}.$$

To bound the Rademacher average in (7.7), we will need to use the contraction principle. To that end, consider the function $\varphi(t) = t^2$. On the interval $[-A, A]$ for some $A > 0$, this function is Lipschitz with constant $2A$, i.e.,

$$|s^2 - t^2| \leq 2A|s - t|, \quad -A \leq s, t \leq A.$$ 

Thus, since $|Y_i| \leq M$ and $|f(X_i)| \leq C_K \lambda$ for all $1 \leq i \leq n$, by the contraction principle we can write

$$R_n(\ell \cdot F_\lambda(Z^n)) \leq \frac{4(M + C_K \lambda)}{n} \mathbb{E}_\sigma^n \sup_{f \in F_\lambda} \left| \sum_{i=1}^n \sigma_i (Y_i - f(X_i)) \right|.$$  

82
Moreover
\[ E_{\sigma_n} \sup_{f \in F_\lambda} \left[ \sum_{i=1}^n \sigma_i (Y_i - f(X_i)) \right] \leq E_{\sigma_n} \left[ \sum_{i=1}^n \sigma_i Y_i \right] + E_{\sigma_n} \sup_{f \in F_\lambda} \left[ \sum_{i=1}^n \sigma_i f(X_i) \right] \]
\[ \leq \sqrt{\sum_{i=1}^n Y_i^2 + nR_n(F_\lambda (Z^n))} \leq (M + C_K \lambda) \sqrt{n}, \]
(7.9)

where the first step uses the triangle inequality, the second step uses the result from previous lectures on the expected absolute value of Rademacher sums, and the third step uses (7.1) and the bound on the Rademacher average over a ball in an RKHS. Combining (7.6) through (7.9) (and overbounding (7.9) slightly), we conclude that

\[ \Delta_n(\ell \cdot F_\lambda) \leq 8(M + C_K \lambda)^2 \sqrt{n} + 2(M^2 + C_k^2 \lambda^2) \sqrt{\frac{2\log(1/\delta)}{n}} \]
(7.10)

with probability at least \( 1 - \delta \). Finally, combining this with (7.5), we get (7.4). \( \square \)

2. Regularized least squares in an RKHS

The observation we had made many times by now is that when the joint distribution of the input-output pair \((X, Y) \in X \times \mathbb{R}\) is unknown, there is no hope in general to learn the optimal predictor \(f^*\) from a finite training sample. Thus, restricting our attention to some hypothesis space \(F\), which is a proper subset of the class of all measurable functions \(f : X \to \mathbb{R}\), is a form of insurance: If we do not do this, then we can always find some function \(f\) that attains zero empirical loss, yet performs spectacularly badly on the inputs outside the training set. When this happens, we say that our learned predictor overfits.

On the other hand, if our hypothesis space \(F\) consists of well-behaved functions, then it is possible to learn a predictor that achieves a graceful balance between in-sample data fit and out-of-sample generalization. The price we pay is the approximation error

\[ L^*(F) - L^* \equiv \inf_{f \in F} L(f) - \inf_{f : X \to \mathbb{R}} L(f) \geq 0. \]

In the regression setting, the approximation error can be expressed as

\[ L^*(F) - L^* = \inf_{f \in F} \|f - f^*\|^2_{P_X}, \]

where \(f^*(x) = E[Y|X = x]\) is the regression function (the MMSE predictor of \(Y\) given \(X\)).

When seen from this perspective, the use of a restricted hypothesis space \(F\) is a form of regularization — a way of guaranteeing that the learned predictor performs well outside the training sample. However, this is not the only way to achieve regularization. In this section, we will analyze another way: complexity regularization. In a nutshell, complexity regularization is a modification of the ERM scheme that allows us to search over a fairly "rich" hypothesis space by adding a penalty term. Complexity regularization is a very general technique with wide applicability. We will look at a particular example of complexity regularization over an RKHS and derive a simple bound on its generalization performance.
To set things up, let $\gamma > 0$ be a regularization parameter. Introduce the regularized quadratic loss
\[ J_\gamma(f) := L(f) + \gamma \|f\|_K^2 \]
and its empirical counterpart
\[ J_{n,\gamma}(f) := L_n(f) + \gamma \|f\|_K^2. \]
Define the functions
\[ f_\gamma^* := \arg \min_{f \in \mathcal{H}_K} J_\gamma(f) \quad (7.11) \]
and
\[ \hat{f}_{n,\gamma} := \arg \min_{f \in \mathcal{H}_K} J_{n,\gamma}(f). \quad (7.12) \]
We will refer to (7.12) as the regularized kernel least squares (RKLS) algorithm.

Note that the minimization in (7.11) and (7.12) takes place in the entire RKHS $\mathcal{H}_K$, rather than a subset, say, a ball. However, the addition of the regularization term $\|f\|_K^2$ ensures that the RKLS algorithm does not just select any function $f \in \mathcal{H}_K$ that happens to fit the training data well — instead, it weighs the goodness-of-fit term $L_n(f)$ term against the “complexity” $\|f\|_K^2$, since a very large value of $\|f\|_K^2$ would indicate that $f$ might “wiggle around” a lot and, therefore, overfit the training sample. The regularization parameter $\gamma > 0$ controls the relative importance of the goodness-of-fit and the complexity terms.

We have the following basic bound on the generalization performance of RKLS:

**Theorem 7.2.** With probability at least $1 - \delta$,
\[ L(\hat{f}_{n,\gamma}) - L^* \leq A(\gamma) + \frac{16M^2 \left(1 + \frac{C_K}{\sqrt{n}}\right)^2}{\sqrt{n}} + 2 \left(2M^2 + \frac{C_K^2(M^2 + A(\gamma))}{\gamma}\right) \sqrt{\frac{2 \log(2/\delta)}{n}} \quad (7.13) \]
where
\[ A(\gamma) := \inf_{f \in \mathcal{H}_K} \left[ L(f) + \gamma \|f\|_K^2 \right] - L^* \]
is the regularized approximation error.

**Proof.** We start with the following lemma:

**Lemma 7.2.**
\[ L(\hat{f}_{n,\gamma}) - L^* \leq \delta_n(\hat{f}_{n,\gamma}) - \delta_n(f_\gamma^*) + A(\gamma), \quad (7.14) \]
where $\delta_n(f) := L(f) - L_n(f)$ for all $f$. 

84
Proof. First, an obvious overbounding gives \( L(\hat{f}_{n,\gamma}) - L^* \leq J_\gamma(\hat{f}_{n,\gamma}) - L^* \). Then
\[
J_\gamma(\hat{f}_{n,\gamma}) = L(\hat{f}_{n,\gamma}) + \gamma\|\hat{f}_{n,\gamma}\|_K^2 \\
= L(\hat{f}_{n,\gamma}) - L_n(\hat{f}_{n,\gamma}) + L_n(\hat{f}_{n,\gamma}) + \gamma\|\hat{f}_{n,\gamma}\|_K^2 \\
= L(\hat{f}_{n,\gamma}) - L_n(\hat{f}_{n,\gamma}) + J_{n,\gamma}(\hat{f}_{n,\gamma}) \\
\leq L(\hat{f}_{n,\gamma}) - L_n(\hat{f}_{n,\gamma}) + J_{n,\gamma}(f^*_\gamma) \\
= L(\hat{f}_{n,\gamma}) - L_n(\hat{f}_{n,\gamma}) + L_n(f^*_\gamma) + \gamma\|f^*_\gamma\|_K^2 \\
= L(\hat{f}_{n,\gamma}) - L_n(\hat{f}_{n,\gamma}) + L_n(f^*_\gamma) - L(f^*_\gamma) + L(f^*_\gamma) + \gamma\|f^*_\gamma\|_K^2 \\
= L(\hat{f}_{n,\gamma}) - L_n(\hat{f}_{n,\gamma}) + L_n(f^*_\gamma) - L(f^*_\gamma) + J_\gamma(f^*_\gamma).
\]
This gives
\[
L(\hat{f}_{n,\gamma}) - L^* \leq L(\hat{f}_{n,\gamma}) - L_n(\hat{f}_{n,\gamma}) + L_n(f^*_\gamma) - L(f^*_\gamma) + J_\gamma(f^*_\gamma) - L^* \\
= L(\hat{f}_{n,\gamma}) - L_n(\hat{f}_{n,\gamma}) + L_n(f^*_\gamma) - L(f^*_\gamma) + \inf_{f \in H} [L(f) + \gamma\|f\|_K^2] - L^* \\
= L(\hat{f}_{n,\gamma}) - L_n(\hat{f}_{n,\gamma}) + L_n(f^*_\gamma) - L(f^*_\gamma) + A(\gamma),
\]
and we are done. \( \square \)

Lemma 7.2 shows that the excess loss of the regularized empirical loss minimizer \( \hat{f}_{n,\gamma} \) is bounded from above by the sum of three terms: the deviation \( \delta_n(\hat{f}_{n,\gamma}) := L(\hat{f}_{n,\gamma}) - L(\hat{f}_{n,\gamma}) \) of \( \hat{f}_{n,\gamma} \) itself, the (negative) deviation \( -\delta_n(f^*_\gamma) := L_n(f^*_\gamma) - L(f^*_\gamma) \) of the best regularized predictor \( f^*_\gamma \), and the approximation error \( A(\gamma) \). To prove Theorem 7.2, we will need to obtain high-probability bounds on the two deviation terms. To that end, we need a lemma:

Lemma 7.3. The functions \( f^*_\gamma \) and \( \hat{f}_{n,\gamma} \) satisfy the bounds
\[
\|f^*_\gamma\|_\infty \leq C K \sqrt{\frac{A(\gamma)}{\gamma}} \tag{7.15}
\]
and
\[
\|\hat{f}_{n,\gamma}\|_K \leq \frac{M}{\sqrt{\gamma}} \quad \text{with probability one} \tag{7.16}
\]
respectively.

Proof. To prove (7.15), we use the fact that
\[
A(\gamma) = L(f^*_\gamma) - L^* + \gamma\|f^*_\gamma\|_K^2 \geq \gamma\|f^*_\gamma\|_K^2,
\]
which gives \( \|f^*_\gamma\|_K \leq \sqrt{A(\gamma)/\gamma} \). From this and from (7.3) we obtain (7.15).

For (7.16), we use the fact that \( \hat{f}_{n,\gamma} \) minimizes \( J_{n,\gamma}(f) \) over all \( f \). In particular,
\[
J_{n,\gamma}(\hat{f}_{n,\gamma}) = L_n(\hat{f}_{n,\gamma}) + \gamma\|\hat{f}_{n,\gamma}\|_K^2 \leq J_{n,\gamma}(0) = \frac{1}{n} \sum_{i=1}^{n} Y_i^2 \leq M^2 \quad \text{w.p. 1},
\]

85
where the last step follows from (7.1). Rearranging and using the fact that \( L_n(f) \geq 0 \) for all \( f \), we get (7.16).

Now we are ready to bound \( \delta_n(\hat{f}_{n,\gamma}) \). For any \( R \geq 0 \), let \( \mathcal{F}_R = \{ f \in \mathcal{H}_K : \| f \|_K \leq R \} \) denote the zero-centered ball of radius \( R \) in the RKHS \( \mathcal{H}_K \). Then Lemma 7.3 says that \( \hat{f}_{n,\gamma} \in \mathcal{F}_{M/\sqrt{n}} \) with probability one. Therefore, with probability one we have

\[
\delta_n(\hat{f}_{n,\gamma}) = \delta_n(\hat{f}_{n,\gamma}) \cdot 1_{\{\hat{f}_{n,\gamma} \in \mathcal{F}_{M/\sqrt{n}}\}} \\
\leq \delta_n(\hat{f}_{n,\gamma}) \cdot 1_{\{\hat{f}_{n,\gamma} \in \mathcal{F}_{M/\sqrt{n}}\}} \\
\leq \sup_{f \in \mathcal{F}_{M/\sqrt{n}}} |\delta_n(f)| \cdot 1_{\{\hat{f}_{n,\gamma} \in \mathcal{F}_{M/\sqrt{n}}\}} \\
\leq \Delta_n(\ell \cdot \mathcal{F}_{M/\sqrt{n}}).
\]

Consequently, we can carry out the same analysis as in the proof of Theorem 7.1. First of all, the function \( g(Z^n) = \Delta_n(\ell \cdot \mathcal{F}_{M/\sqrt{n}}) \) has bounded differences with

\[
c_1 = \ldots = c_n \leq \frac{4}{n} \left( M^2 + \sup_{f \in \mathcal{F}_{M/\sqrt{n}}} \| f \|_\infty^2 \right) \leq \frac{4M^2}{n} \left( 1 + \frac{C_K^2}{\gamma} \right)
\]

where the last step uses (7.16) and Lemma 7.1. Therefore, with probability at least \( 1 - \delta/2 \),

\[
(7.17) \quad \delta_n(\hat{f}_{n,\gamma}) \leq \Delta_n(\ell \cdot \mathcal{F}_{M/\sqrt{n}}) \leq \frac{8M^2 \left( 1 + \frac{C_K^2}{\gamma} \right)^2}{\sqrt{n}} + 2M^2 \left( 1 + \frac{C_K^2}{\gamma} \right) \sqrt{\frac{2 \log(2/\delta)}{n}},
\]

where the second step follows from (7.10) with \( \delta \) replaced by \( \delta/2 \) and with \( \lambda = M/\sqrt{n} \).

It remains to bound \( \delta_n(f^*_\gamma) \). This is, actually, much easier, since we are dealing with a single data-independent function. In particular, note that we can write

\[
\delta_n(f^*_\gamma) = \frac{1}{n} \sum_{i=1}^n (Y_i - f^*_\gamma(X_i))^2 - \mathbb{E} [(Y - f^*_\gamma(X))^2] = \frac{1}{n} \sum_{i=1}^n U_i,
\]

where \( U_i := (Y_i - f^*_\gamma(X_i))^2 - \mathbb{E} [(Y - f^*_\gamma(X))^2], 1 \leq i \leq n \), are i.i.d. random variables with \( \mathbb{E} U_i = 0 \) and

\[
|U_i| \leq \sup_{y \in [-M,M]} \sup_{x \in \mathbb{X}} (y - f^*_\gamma(x))^2 \leq 2(M^2 + \| f^*_\gamma \|_\infty^2) \leq 2 \left( M^2 + \frac{C_K^2 A(\gamma)}{\gamma} \right)
\]

with probability one, where we have used (7.1) and (7.15). We can therefore use Hoeffding’s inequality to write, for any \( t \geq 0 \),

\[
\mathbb{P} \left( -\delta_n(f^*_\gamma) \geq t \right) = \mathbb{P} \left( \frac{1}{n} \sum_{i=1}^n U_i \leq -t \right) \leq \exp \left( -\frac{nt^2}{8(M^2 + C_K^2 A(\gamma)/\gamma)^2} \right)
\]

This implies that

\[
(7.18) \quad -\delta_n(f^*_\gamma) \leq 2 \left( M^2 + \frac{C_K^2 A(\gamma)}{\gamma} \right) \sqrt{\frac{2 \log(2/\delta)}{n}}
\]

86
with probability at least $1 - \delta/2$. Combining (7.17) and (7.18) with (7.14), we get (7.13).
Part 3

Some Applications
CHAPTER 8

Empirical vector quantization

Now that we have safely made our way through the combinatorial forests of Vapnik–Chervonenkis classes, we will look at an interesting application of the VC theory to a problem in communications engineering: empirical design of vector quantizers. Vector quantization is a technique for lossy data compression (or source coding), so we will first review, at a very brisk pace, the basics of source coding, and then get to business. The presentation will closely follow an excellent survey by Tamás Linder [Lin01].

1. A brief introduction to source coding

It’s trite but true: we live in a digital world. We store, exchange, and manipulate vast quantities of binary data. While a lot of the data are inherently discrete (e.g., text), most are compressed representations of continuous-valued (analog) sources, such as audio, speech, images, or video. The process of mapping source data from their “native” format to binary representations and back is known in the information theory and the communications engineering communities as source coding.

There are two types of source coding: lossless and lossy. The former pertains to constructing compact binary representations of discrete data, such as text, and the objective is to map any sequence of symbols emitted by the source of interest into a binary file which is as short as possible and which will permit exact (i.e., error-free) reconstruction (decompression) of the data. The latter, on the other hand, deals with continuous-valued sources (such as images), and the objective is to map any source realization to a compact binary representation that would, upon decompression, differ from the original source as little as possible. We will focus on lossy source coding. Needless to say, we will only be able to give a very superficial overview of this rich subject. A survey article by Gray and Neuhoff [GN98] does a wonderful job of tracing both the historical development and the state of the art in lossy source coding; for an encyclopedic treatment I recommend the book by Gersho and Gray [GG92].

One of the simpler models of an analog source is a stationary stochastic process \( Z_1, Z_2, \ldots \) with values in \( \mathbb{R}^d \). For example, if \( d \) is a perfect square, then each \( Z_i \) could represent a \( \sqrt{d} \times \sqrt{d} \) image patch. The compression process consists of two stages. First, each \( Z_i \) is mapped to a binary string \( b_i \). Thus, the entire data stream \( \{Z_i\}_{i=1}^\infty \) is represented by the sequence of binary strings \( \{b_i\}_{i=1}^\infty \). The source data are reconstructed by mapping each \( b_i \) into a vector \( \hat{Z}_i \in \mathbb{R}^d \). Since each \( Z_i \) takes on a continuum of values, the mapping \( Z_i \mapsto b_i \) is inherently many-to-one, i.e., noninvertible. This is the reason why this process is called lossy source coding — in going from the analog data \( \{Z_i\} \) to the digital representation \( \{b_i\} \) and then to the reconstruction \( \hat{Z}_i \), we lose information needed to recover each \( Z_i \) exactly. The overall mapping \( Z_i \mapsto b_i \mapsto \hat{Z}_i \) is called a vector quantizer, where the term “vector” refers to the
vector-valued nature of the source \( \{ Z_i \} \), while the term “quantizer” indicates the process of representing a continuum by a discrete set. We assume that the mappings comprising the quantizer are time-invariant, i.e., do not depend on the time index \( i \in \mathbb{N} \).

There are two figures of merit for a given quantizer: the compactness of the binary representation \( Z_i \mapsto b_i \) and the accuracy of the reconstruction \( b_i \mapsto \hat{Z}_i \). The former is given by the rate of the quantizer, i.e., the expected length of \( b_i \) in bits. Since the source \( \{ Z_i \} \) is assumed to be stationary and the quantizer is assumed to be time-invariant, we have

\[
\mathbf{E}[\text{len}(b_i)] = \mathbf{E}[\text{len}(b_1)], \quad \forall i \in \mathbb{N},
\]

where, for a binary string \( b \), \( \text{len}(b) \) denotes its length in bits. If the length of \( b_i \equiv b_i(Z_i) \) depends on \( Z_i \), then we say that the quantizer is \textit{variable-rate}; otherwise, we say that the quantizer is \textit{fixed-rate}. The latter measures how well the reconstruction \( \hat{Z}_i \) approximates the source \( Z_i \) on average. In order to do that, we pick a nonnegative distortion measure \( d : \mathbb{R}^d \times \mathbb{R}^d \rightarrow [0, \infty) \), so that \( d(z, \hat{z}) \geq 0 \) quantifies how well one vector \( z \in \mathbb{R}^d \) is approximated by another \( \hat{z} \in \mathbb{R}^d \). Then we look at the expected value \( \mathbf{E}[d(Z_i, \hat{Z}_i)] \), which is the same for all \( i \), again owing to the stationarity of \( \{ Z_i \} \) and the time invariance of the quantizer. A typical distortion measure is the squared Euclidean norm

\[
d(z, \hat{z}) = \| z - \hat{z} \|^2 = \sum_{j=1}^{d} |z(j) - \hat{z}(j)|^2,
\]

where \( z(j) \) denotes the \( j \)th coordinate of \( z \). We will focus only on this distortion measure from now on.

Now, using the fact that the rate and the expected distortion of a quantizer do not depend on the time index \( i \), we can just consider the problem of quantizing a single \( \mathbb{R}^d \)-valued random variable \( Z \) with the same distribution as that of \( Z_1 \). From now on, we will refer to such a \( Z \) as the source. Thus, the rate of a given quantizer \( Z \mapsto b \mapsto \hat{Z} \) is given by \( \mathbf{E}[\text{len}(b)] \) and the expected distortion \( \mathbf{E}\| Z - \hat{Z} \|^2 \). Naturally, one would like to keep both of these as low as possible: low rate means that it will take less memory space to store the compressed data and that it will be possible to transmit the compressed data over low-fidelity (i.e., low-capacity) digital channels; low expected distortion means that the reconstructed source will be a very accurate approximation of the true source. However, these two quantities are in conflict: if we make the rate too low, we will be certain to incur a lot of loss in reconstructing the data; on the other hand, insisting on very accurate reconstruction will mean that the binary representation must use a large number of bits. For this reason, the natural question is as follows: what is the smallest distortion achievable on a given source by any quantizer with a given rate?

2. Fixed-rate vector quantization

Let \( Z = \mathbb{R}^d \).

**Definition 8.1.** Let \( k \in \mathbb{N} \). A \( (d \text{-dimensional}) \) \( k \)-point vector quantizer is a (measurable) mapping \( q : Z \rightarrow \mathcal{C} = \{ y_1, \ldots, y_k \} \subset Z \), where the set \( \mathcal{C} \) is called the codebook and its elements are called the codevectors.
The source is a random vector \( Z \in \mathbb{R}^d \) with some probability distribution \( P_Z \). A given \( k \)-point quantizer \( q \) represents \( Z \) by the quantized output \( \hat{Z} = q(Z) \). Since \( q(Z) \) can take only \( k \) possible values, it is possible to represent it uniquely by a binary string of \( \lceil \log_2 k \rceil \) bits. The number

\[
R(q) := \lceil \log_2 k \rceil
\]

is called the rate of \( q \) (in bits), where we follow standard practice and ignore the integer constraint on the length of the binary representation. The rate is often normalized by the dimension \( d \) to give \( r(q) = d^{-1} R(q) \) (measured in bits per coordinate); however, since we assume \( d \) fixed, there is no need to worry about the normalization. The fidelity of \( q \) in representing \( Z \sim P_Z \) is measured by the expected distortion

\[
D(P_Z, q) := \mathbb{E} \| Z - q(Z) \|^2 = \int_{\mathbb{R}^d} \| z - q(z) \|^2 P_Z(dz).
\]

We will assume throughout that \( Z \) has finite second moment, \( \mathbb{E} \| Z \|^2 < \infty \), so that \( D(P_Z, q) < \infty \).

The main objective in vector quantization is to minimize the expected distortion subject to a constraint on the rate (or, equivalently, on the codebook size). Thus, if we denote by \( Q_k \) the set of all \( k \)-point vector quantizers, then the optimal performance on a given source distribution \( P_Z \) is defined by

\[
D^*_k(P_Z) := \inf_{q \in Q_k} D(P_Z, q) \equiv \inf_{q \in Q_k} \mathbb{E} \| Z - q(Z) \|^2.
\]

**Definition 8.2.** We say that a quantizer \( q^* \in Q_k \) is optimal for \( P_Z \) if

\[
D(P_Z, q^*) = D^*_k(P_Z).
\]

As we will soon see, it turns out that an optimal quantizer always exists — in other words, the infimum in (8.1) is actually a minimum — and it can always be chosen to have a particularly useful structural property:

**Definition 8.3.** A quantizer \( q \in Q_k \) with codebook \( C = \{ y_1, \ldots, y_k \} \) is called nearest-neighbor if, for all \( z \in \mathcal{Z} \),

\[
\| z - q(z) \|^2 = \min_{1 \leq j \leq k} \| z - y_j \|^2.
\]

Let \( Q^\text{NN}_k \) denote the set of all \( k \)-point nearest-neighbor quantizers. We have the following simple but important result:

**Lemma 8.1.** For any \( q \in Q_k \) we can always find some \( q' \in Q^\text{NN}_k \), such that \( D(P_Z, q') \leq D(P_Z, q) \).

**Proof.** Given a quantizer \( q \in Q_k \) with codebook \( C = \{ y_1, \ldots, y_k \} \), define \( q' \) by

\[
q'(z) := \arg \min_{y_j \in C} \| z - y_j \|^2.
\]
where ties are broken by going with the lowest index. Then $q'$ is clearly a nearest-neighbor quantizer, and

$$D(P_Z, q') = E\|Z - q'(Z)\|^2 = E\left[\min_{1 \leq j \leq k} \|Z - y_j\|^2\right] \leq E\|Z - q(Z)\|^2 \equiv D(P_Z, q).$$

The lemma is proved. $\blacksquare$

In light of this lemma, we can rewrite (8.1) as

$$D^*_k(P_Z) = \inf_{q \in \mathcal{Q}^\text{NN}_k} E\|Z - q(Z)\|^2 = \inf_{c = \{y_1, \ldots, y_k\} \subset Z} E\left[\min_{1 \leq j \leq k} \|Z - y_j\|^2\right].$$

An important result due to Pollard [Pol82], which we state here without proof, then says the following:

**Theorem 8.1.** If $Z$ has a finite second moment, $E\|Z\|^2 < \infty$, then there exists a nearest-neighbor quantizer $q^* \in \mathcal{Q}^\text{NN}_k$ such that $D(P_Z, q^*) = D^*_k(P_Z)$.

### 3. Learning an optimal quantizer

Unfortunately, finding an optimal $q^*$ is a very difficult problem. Indeed, the optimization problem in (8.2) has a combinatorial search component to it, since we have to optimize over all $k$-point sets $C$ in $\mathbb{R}^d$. Moreover, the source distribution $P_Z$ is often not known exactly, especially for very complex sources, such as natural images. For these reasons, we have to resort to empirical methods for quantizer design, which rely on the availability of a large number of independent samples from the source distribution of interest.

Assuming that such samples are easily available, we can formulate the empirical quantizer design problem as follows. Let us fix the desired codebook size $k$. For each $n \in \mathbb{N}$, let $Z^n = (Z_1, \ldots, Z_n)$ be an i.i.d. sample from $P_Z$. We seek an algorithm that would take $Z^n$ and produce a quantizer $\hat{q}_n \in \mathcal{Q}_k$ that would approximate, as closely as possible, an optimal quantizer $q^* \in \mathcal{Q}_k$ that achieves $D^*_k(P_Z)$. In other words, we hope to learn an (approximately) optimal quantizer for $P_Z$ based on a sufficiently long training sample.

The first thing to note is that the theory of quantization outlined in the preceding section applies to the empirical distribution of the training sample $Z^n$,

$$P_n = \frac{1}{n} \sum_{i=1}^n \delta_{Z_i}.$$ 

In particular, given a quantizer $q \in \mathcal{Q}_k$, we can compute its expected distortion

$$D(P_n, q) = E_{P_n} \|Z - q(Z)\|^2 = \frac{1}{n} \sum_{i=1}^n \|Z_i - q(Z_i)\|^2.$$
Moreover, the minimum achievable distortion is given by
\[
D^*_k(P_n) = \min_{q \in \mathcal{Q}_k^n} \frac{1}{n} \sum_{i=1}^{n} \| Z_i - q(Z_i) \|^2 = \min_{q \in \mathcal{Q}_k^n} \| Z_i - q(Z_i) \|^2.
\]

Note that we have replaced the infimum with the minimum, since an optimal quantizer always exists and can be assumed to have the nearest-neighbor property. Moreover, since \( P_n \) is a discrete distribution, the existence of an optimal nearest-neighbor quantizer can be proved directly, without recourse to Pollard’s theorem. Thus, we can restrict our attention to nearest-neighbor \( k \)-point quantizers.

**Definition 8.4.** We say that a quantizer \( \hat{q}_n \in \mathcal{Q}_k^n \) is **empirically optimal** for \( Z^n \) if
\[
D(P_n, \hat{q}_n) = D^*_k(P_n) = \min_{q \in \mathcal{Q}_k^n} D(P_n, q) = \min_{q \in \mathcal{Q}_k^n} \frac{1}{n} \sum_{i=1}^{n} \| Z_i - q(Z_i) \|^2.
\]

Note that, by the nearest-neighbor property,
\[
D^*_k(P_n) = \min_{C = \{y_1, \ldots, y_k\} \subseteq Z^n} \frac{1}{n} \sum_{i=1}^{n} \min_{1 \leq j \leq k} \| Z_i - y_j \|^2.
\]

Thus, let \( \hat{q}_n \in \mathcal{Q}_k^n \) be an empirically optimal nearest-neighbor quantizer. Let \( Z \sim P_Z \) be a new source realization, independent of the training data \( Z^n \). If we apply \( \hat{q}_n \) to \( Z \), the resulting quantized output \( \hat{Z} = \hat{q}_n(Z) \) will depend on both the input \( Z \) and on the training data \( Z^n \). Moreover, the expected distortion of \( \hat{q}_n \), given by
\[
E \left[ D(P_Z, \hat{q}_n) \left| Z^n \right. \right] = \int \| z - \hat{q}_n(z) \|^2 P_Z(dz),
\]
is a random variable, since it depends (through \( \hat{q}_n \)) on the training data \( Z^n \). In the next section we will show that, under certain assumptions on the source \( P_Z \), the empirically optimal quantizer \( \hat{q}_n \) is nearly optimal on \( P_Z \) as well, in the sense that
\[
E \left[ D(P_Z, \hat{f}_n) - D^*_k(P_Z) \right] \leq \frac{C}{\sqrt{n}},
\]
where the expectation is w.r.t. the distribution \( Z^n \) and \( C > 0 \) is some constant that depends on \( d, k \), and a certain characteristic of \( P_Z \). More generally, it is possible to show that empirically optimal quantizers are strongly consistent in the sense that
\[
D(P_Z, \hat{q}_n) - D^*_k(P_Z) \xrightarrow{n \to \infty} 0 \quad \text{almost surely}
\]
provided the source \( P_Z \) has a finite second moment (see Linder’s survey [Lin01] for details).

**Remark 8.1.** It should be pointed out that the problem of finding an exact minimizer of \( D(P_n, q) \) over \( q \in \mathcal{Q}_k^n \) is NP-complete. Instead, various approximation techniques are used. The most popular one is the Lloyd algorithm, known in the computer science community as the method of \( k \)-means. There, one starts with an initial codebook \( C^{(0)} = \{y_1^{(0)}, \ldots, y_k^{(0)}\} \) and then iteratively recomputes the quantizer partition and the new codevectors until convergence.
4. Finite sample bound for empirically optimal quantizers

In this section, we will show how the VC theory can be used to establish (8.3) for any source supported on a ball of finite radius. This result was proved by Linder, Lugosi and Zeger [LLZ94], and since then refined and extended by multiple authors. Some recent works even remove the requirement that $Z$ be finite-dimensional and consider more general coding schemes in Hilbert spaces [MP10].

For a given $r > 0$ and $z \in \mathbb{R}^d$, let $B_r(z)$ denote the $\ell_2$ ball of radius $r$ centered at $z$:

$B_r(z) := \{ y \in \mathbb{R}^d : \| y - z \| \leq r \}.$

Let $P(r)$ denote the set of all probability distributions $P_Z$ on $Z = \mathbb{R}^d$, such that

$P_Z(B_r(0)) = 1.$

Here is the main result we will prove in this section:

THEOREM 8.2. There exists some absolute constant $C > 0$, such that

$$\sup_{P_Z \in P(r)} \mathbb{E} [D(P_Z, \hat{q}_n) - D_k^*(P_Z)] \leq C r^2 \sqrt{\frac{k(d+1) \log(k(d+1))}{n}}.$$  

Here, as before, $\hat{q}_n$ denotes an empirically optimal quantizer based on an i.i.d. sample $Z^n$.

Before launching into the proof, we state and prove a useful lemma:

LEMMA 8.2. Let $Q_k^{\text{NN}}(r)$ denote the set of all nearest-neighbor $k$-point quantizers whose codewords lie in $B_r(0)$. Then for any $P_Z \in P(r)$,

$$D(P_Z, \hat{q}_n) - D_k^*(P_Z) \leq 2 \sup_{q \in Q_k^{\text{NN}}(r)} |D(P_n, q) - D(P_Z, q)|.$$  

PROOF. Fix $P_Z$ and let $q^* \in Q_k^{\text{NN}}$ denote an optimal quantizer, i.e., $D(P_Z, q^*) = D_k^*(P_Z)$. Then, using our old trick of adding and subtracting the right empirical quantities, we can write

$$D(P_Z, \hat{q}_n) - D_k^*(P_Z) = D(P_Z, \hat{q}_n) - D(P_n, \hat{q}_n) + D(P_n, \hat{q}_n) - D(P_n, q^*) + D(P_n, q^*) - D(P_Z, q^*).$$

Since $\hat{q}_n$ minimizes the empirical distortion $D(P_n, q)$ over all $q \in Q_k^{\text{NN}}$, we have $D(P_n, \hat{q}_n) \leq D(P_n, q^*)$, which leads to

$$D(P_Z, \hat{q}_n) - D_k^*(P_Z) \leq D(P_Z, \hat{q}_n) - D(P_n, \hat{q}_n) + D(P_n, q^*) - D(P_Z, q^*).$$

Now, since $B_r(0)$ is a convex set, for any point $y \notin B_r(0)$ we can compute its projection $y'$ onto $B_r(0)$, namely $y' = ry/\|y\|$. Then $y'$ is strictly closer to all $z \in B_r(0)$ than $y$, i.e.,

$$\|z - y'\| < \|z - y\|, \quad \forall z \in B_r(0).$$

Thus, if we take an arbitrary quantizer $q \in Q_k$ and replace all of its codevectors outside $B_r(0)$ by their projections, we will obtain another quantizer $q'$, such that $\|z - q'(z)\| \leq \|z - q(z)\|$ for all $z \in B_r(0)$. (The $\leq$ sign is due to the fact that some of the codevectors of $q$ may already be in $B_r(0)$, so the projection will not affect them). But then for any $P_Z \in P(r)$ we will have $D(P_Z, q') \leq D(P_Z, q)$. Moreover, if $Z^n$ is an i.i.d. sample from $P_Z$ and $P_n$ is the corresponding empirical distribution, then $P_n \in P(r)$ with probability one. Hence, we can
assume that both $\hat{q}_n$ and $q^*$ have all their codevectors in $B_r(0)$, and therefore from (8.4) we obtain
\[
D(P_Z, \hat{q}_n) - D'_k(P_Z) \leq D(P_Z, \hat{q}_n) - D(P_n, \hat{q}_n) + D(P_n, q^*) - D(P_Z, q^*) \\
\leq |D(P_n, \hat{q}_n) - D(P_Z, \hat{q}_n)| + |D(P_Z, q^*) - D(P_n, q^*)| \\
\leq 2 \sup_{q \in Q_k(r)} |D(P_n, q) - D(P_Z, q)|. 
\]
This finishes the proof. \hfill \Box

Now we can get down to business:

**Proof (of Theorem 8.2).** For a given quantizer $q \in Q_k(r)$, define the function
\[
f_q(z) := \|z - q(z)\|^2,
\]
which is just the squared Euclidean distortion between $z$ and $q(z)$. In particular, for any $P \in \mathcal{P}(r)$ the expected distortion $D(P, q)$ is equal to $P(f_q)$. Since $q \in Q_k(r)$, we have $\|q(z)\| \leq r$ for all $z$. Therefore, for any $z \in B_r(0)$ we will have
\[
0 \leq f_q(z) \leq 2\|z\|^2 + 2\|q(z)\|^2 \leq 4r^2.
\]
Therefore, using the fact that the expectation of any nonnegative random variable $U$ can be written as
\[
\mathbf{E}U = \int_0^\infty \mathbf{P}(U > u)du,
\]
we can write
\[
D(P_Z, q) = P_Z(f_q) = \int_0^{4r^2} P_Z(f_q(Z) > u)du
\]
and
\[
D(P_n, q) = P_n(f_q) = \int_0^{4r^2} P_n(f_q(Z) > u)du = \int_0^{4r^2} \frac{1}{n} \sum_{i=1}^n 1\{f_q(Z_i) > u\}du \quad \text{a.s.}
\]
Therefore
\[
\sup_{q \in Q_k(r)} |D(P_n, q) - D(P_Z, q)| \\
= \sup_{q \in Q_k(r)} |P_n(q) - P_Z(q)| \\
= \sup_{q \in Q_k(r)} \left| \int_0^{4r^2} \left( \frac{1}{n} \sum_{i=1}^n 1\{f_q(Z_i) > u\} - P_Z(f_q(Z) > u) \right) du \right| \\
\leq 4r^2 \sup_{q \in Q_k(r)} \sup_{0 \leq u \leq 4r^2} \left| \frac{1}{n} \sum_{i=1}^n 1\{f_q(Z_i) > u\} - P_Z(f_q(Z) > u) \right| \quad \text{a.s.} 
\]
where the last step uses the fact that
\[
\int_a^b h(u)du \leq |b - a| \sup_{a \leq u \leq b} |h(u)|.
\]
Now, for a given \( q \in \mathcal{Q}_k^{\text{NN}}(r) \) and a given \( u > 0 \) let us define the set
\[
A_{u,q} := \left\{ z \in \mathbb{R}^d : f_q(z) > u \right\},
\]
and let \( \mathcal{A} \) denote the class of all such sets: \( \mathcal{A} := \{ A_{u,q} : u > 0, q \in \mathcal{Q}_k^{\text{NN}}(r) \} \). Then \( 1_{\{f_q(z) > u\}} = 1_{\{z \in A_{u,q}\}} \), so from (8.5) we can write
\[
(8.6) \quad \sup_{q \in \mathcal{Q}_k^{\text{NN}}(r)} |D(P_n, q) - D(P_Z, q)| \leq 4r^2 \sup_{A \in \mathcal{A}} |P_n(A) - P_Z(A)|.
\]

Therefore,
\[
\mathbb{E}[D(P_Z, \hat{q}_n) - D^*(P_Z)] \leq 2\mathbb{E}\left[ \sup_{q \in \mathcal{Q}_k^{\text{NN}}(r)} |D(P_n, q) - D(P_Z, q)| \right] \leq 8r^2 \mathbb{E}\left[ \sup_{A \in \mathcal{A}} |P_n(A) - P_Z(A)| \right],
\]
where the first step follows from Lemma 8.2 and the second step follows from (8.6). To finish the proof, we will show that \( \mathcal{A} \) is a VC class with \( V(\mathcal{A}) \leq 4k(d + 1) \log(k(d + 1)) \), so that
\[
\mathbb{E}\left[ \sup_{A \in \mathcal{A}} |P_n(A) - P_Z(A)| \right] \leq C \sqrt{\frac{V(\mathcal{A})}{n}} \leq 2C \sqrt{\frac{k(d + 1) \log(k(d + 1))}{n}}.
\]

In order to bound the VC dimension of \( \mathcal{A} \), let us consider a typical set \( A_{u,q} \). Let \( \{y_1, \ldots, y_k\} \) denote the codevectors of \( q \). Since \( q \) is a nearest-neighbor quantizer, a point \( z \) will be in \( A_{u,q} \) if and only if
\[
f_q(z) = \min_{1 \leq j \leq k} \|z - y_j\|^2 > u,
\]
which is equivalent to
\[
\|z - y_j\| > \sqrt{u}, \quad \forall 1 \leq j \leq k.
\]
In other words, we can write
\[
A_{u,q} = \bigcap_{j=1}^k B_{\sqrt{u}}(y_j)^c.
\]
Since this can be done for every \( u > 0 \) and every \( q \in \mathcal{Q}_k^{\text{NN}}(r) \), we conclude that the class \( \mathcal{A} \) is contained in another class \( \tilde{\mathcal{A}} \), defined by
\[
\tilde{\mathcal{A}} := \left\{ \bigcap_{j=1}^k B_{\sqrt{u}}(y_j)^c : B_j \in \mathcal{B}, \forall j \right\},
\]
where \( \mathcal{B} \) denotes the class of all closed balls in \( \mathbb{R}^d \). Therefore, \( V(\mathcal{A}) \leq V(\tilde{\mathcal{A}}) \). To bound \( V(\tilde{\mathcal{A}}) \), we must examine its shatter coefficients. We will need the following facts\(^1\):

1. For any class of sets \( \mathcal{M} \), let \( \overline{\mathcal{M}} \) denote the class \( \{M^c : M \in \mathcal{M}\} \) formed by taking the complements of all sets in \( \mathcal{M} \). Then for any \( n \)
\[
\mathcal{S}_n(\overline{\mathcal{M}}) = \mathcal{S}_n(\mathcal{M}).
\]

\(^1\)Exercise: prove them!
(2) For any class of sets $\mathcal{N}$, let $\mathcal{N}_k$ denote the class $\{N_1 \cap N_2 \cap \ldots \cap N_k : N_j \in \mathcal{N}, 1 \leq j \leq k\}$, formed by taking intersections of all possible choices of $k$ sets from $\mathcal{N}$. Then

$$S_n(\mathcal{N}_k) \leq S_n^k(\mathcal{N}).$$

In the above notation, $\tilde{A} = (\mathcal{B})_k$, so

$$S_n(\tilde{A}) \leq S_n^k(\mathcal{B}),$$

where $\mathcal{B}$ is the class of all closed balls in $\mathbb{R}^d$. From the previous lecture we know that $V(\mathcal{B}) = d + 1$, and so the Sauer–Shelah lemma gives

$$S_n(\tilde{A}) \leq \left(\frac{ne}{d+1}\right)^{k(d+1)}, \quad \text{for } n \geq d + 1. \tag{8.7}$$

We can now upper-bound $V(\tilde{A})$ by finding an $n$ for which the right-hand side of (8.7) is less than $2^n$. It is easy to check that, for $d \geq 2$, $n = 4k(d + 1) \log(k(d + 1))$ does the job; for $d = 1$ it’s clear that $V(\tilde{A}) \leq 2k$. Thus,

$$V(A) \leq V(\tilde{A}) \leq 4k(d + 1) \log(k(d + 1)),$$

as claimed. The proof is finished. \qed
Dimensionality reduction in Hilbert spaces

Dimensionality reduction is a generic name for any procedure that takes a complicated object living in a high-dimensional (or possibly even infinite-dimensional) space and approximates it in some sense by a finite-dimensional vector. We are interested in a particular class of dimensionality reduction methods. Consider a data source that generates vectors in some Hilbert space $\mathcal{H}$, which is either infinite-dimensional or has a finite but extremely large dimension (think $\mathbb{R}^d$ with the usual Euclidean norm, where $d$ is huge). We will assume that the vectors of interest lie in the unit ball of $\mathcal{H}$,

$$B(\mathcal{H}) := \{ x \in \mathcal{H} : \|x\| \leq 1 \},$$

where $\|x\| = \sqrt{\langle x, x \rangle}$ is the norm on $\mathcal{H}$. We wish to represent each $x \in B(\mathcal{H})$ by a vector $\hat{y} \in \mathbb{R}^k$ for some fixed $k$ (if $\mathcal{H}$ is $d$-dimensional, then of course we must have $d \gg k$). For instance, $k$ may represent some storage limitation, such as a device that can store no more than $k$ real numbers (or, more realistically, $k$ double-precision floating-point numbers, which for all practical purposes can be thought of as real numbers). The mapping $x \mapsto \hat{y}$ can be thought of as an encoding rule. In addition, given $\hat{y} \in \mathbb{R}^k$, we need a decoding rule that takes $\hat{y}$ and outputs a vector $\hat{x} \in \mathcal{H}$ that will serve as an approximation of $x$. In general, the cascade of mappings

$$x \xrightarrow{\text{encoding}} \hat{y} \xrightarrow{\text{decoding}} \hat{x}$$

will be lossy, i.e., $x \neq \hat{x}$. So, the goal is to ensure that the squared norm error $\|x - \hat{x}\|^2$ is as small as possible. In this lecture, we will see how Rademacher complexity techniques can be used to characterize the performance of a particular fairly broad class of dimensionality reduction schemes in Hilbert spaces. Our exposition here is based on a beautiful recent paper of Maurer and Pontil [MP10].

We will consider a particular type of dimensionality reduction schemes, where the encoder is a (nonlinear) projection, whereas the decoder is a linear operator from $\mathbb{R}^k$ into $\mathcal{H}$ (the Appendix contains some basic facts pertaining to linear operators between Hilbert spaces). To specify such a scheme, we fix a pair $(\mathcal{Y}, T)$ consisting of a closed set $\mathcal{Y} \subseteq \mathbb{R}^k$ and a linear operator $T : \mathbb{R}^k \to \mathcal{H}$. We call $\mathcal{Y}$ the codebook and use the encoding rule

$$\hat{y} = \arg\min_{y \in \mathcal{Y}} \|x - Ty\|^2. \tag{9.1}$$

Unless $\mathcal{Y}$ is a closed subspace of $\mathbb{R}^k$, this encoding map will be nonlinear. The decoding, on the other hand, is linear: $\hat{x} = T\hat{y}$. With these definitions, the reconstruction error is given by

$$\|x - \hat{x}\|^2 = f_T(x) := \min_{y \in \mathcal{Y}} \|x - Ty\|^2.$$
Now suppose that the input to our dimensionality reduction scheme is a random vector $X \in B(\mathcal{H})$ with some unknown distribution $P$. Then we measure the performance of the coding scheme $(Y, T)$ by its expected reconstruction error

$$L(T) := \mathbb{E}_P[f_T(X)] \equiv \mathbb{E}_P \left[ \min_{y \in Y} \|X - Ty\|^2 \right]$$

(note that, even though the reconstruction error depends on the codebook $Y$, we do not explicitly indicate this dependence, since the choice of $Y$ will be fixed by a particular application). Now let $\mathcal{T}$ be some fixed class of admissible linear decoding maps $\mathcal{T} : \mathbb{R}^k \to \mathcal{H}$. So, if we knew $P$, we could find the best decoder $\tilde{T} \in \mathcal{T}$ that achieves

$$L^*(\mathcal{T}) := \inf_{T \in \mathcal{T}} L(T)$$

(assuming, of course, that the infimum exists and is achieved by at least one $T \in \mathcal{T}$).

By now, you know the drill: We don’t know $P$, but we have access to a large set of samples $X_1, \ldots, X_n$ drawn i.i.d. from $P$. So we attempt to learn $\tilde{T}$ via ERM:

$$\hat{T}_n := \arg \min_{T \in \mathcal{T}} \frac{1}{n} \sum_{i=1}^n f_T(X_i) = \arg \min_{T \in \mathcal{T}} \frac{1}{n} \sum_{i=1}^n \min_{y \in Y} \|X_i - Ty\|^2.$$

Our goal is to establish the following result:

**Theorem 9.1.** Assume that $Y$ is a closed subset of the unit ball $B_2^k = \{y \in \mathbb{R}^k : \|y\|_2 \leq 1\}$, and that every $T \in \mathcal{T}$ satisfies

$$\|Te_j\| \leq \alpha, \quad 1 \leq j \leq k$$

$$\|T\|_Y := \sup_{y \in Y, y \neq 0} \|Ty\| \leq \alpha$$

for some finite $\alpha \geq 1$, where $e_1, \ldots, e_k$ is the standard basis of $\mathbb{R}^k$. Then

$$(9.2) \quad L(\hat{T}_n) \leq L^*(\mathcal{T}) + \frac{60\alpha^2 k^2}{\sqrt{n}} + 4\alpha^2 \sqrt{\frac{2 \log(1/\delta)}{n}}$$

with probability at least $1 - \delta$. In the special case when $Y = \{e_1, \ldots, e_k\}$, the standard basis in $\mathbb{R}^k$, the event

$$(9.3) \quad L(\hat{T}_n) \leq L^*(\mathcal{T}) + \frac{40\alpha^2 k}{\sqrt{n}} + 4\alpha^2 \sqrt{\frac{2 \log(1/\delta)}{n}}$$

holds with probability at least $1 - \delta$.

**Remark 9.1.** The above result is slightly weaker than the one from [MP10]; as a consequence, the constants in Eqs. (9.2) and (9.3) are slightly worse than they could otherwise be.

1. **Examples**

Before we get down to business and prove the theorem, let’s look at a few examples.
1.1. Principal component analysis (PCA). The objective of PCA is, given \( k \), construct a projection \( \Pi \) onto a \( k \)-dimensional closed subspace of \( \mathcal{H} \) to maximize the average “energy content” of the projected vector:

\[
\text{maximize } \mathbb{E} \| \Pi X \|^2
\]

subject to \( \dim \Pi(\mathcal{H}) = k \)

\( \Pi^2 = \Pi \)  

(9.4)

For any \( x \in \mathcal{H} \),

\[
\| \Pi x \|^2 = \| x \|^2 - \| (I - \Pi) x \|^2,
\]

where \( I \) is the identity operator on \( \mathcal{H} \). To prove (9.5), expand the right-hand side:

\[
\| x \|^2 - \| (I - \Pi) x \|^2 = \| x \|^2 - \| x - \Pi x \|^2 = 2\langle x, \Pi x \rangle - \| \Pi x \|^2 = \| \Pi x \|^2,
\]

where the last step is by the properties of projections. Thus,

\[
\| \Pi x \|^2 = \| x \|^2 - \| x - \Pi x \|^2 = \| x \|^2 - \min_{x' \in \mathcal{K}} \| x - x' \|^2,
\]

(9.6)

where \( \mathcal{K} \) is the range of \( \Pi \) (the closure of the linear span of all vectors of the form \( \Pi x, x \in \mathcal{H} \)). Moreover, any projection operator \( \Pi : \mathcal{H} \rightarrow \mathcal{K} \) with \( \dim(\mathcal{H}) = k \) can be factored as \( TT^* \), where \( T : \mathbb{R}^k \rightarrow \mathcal{H} \) is an isometry (see Appendix for definitions and the proof of this fact). Using this fact, we can write

\[
\mathcal{K} = \Pi(\mathcal{H}) = \{ Ty : y \in \mathbb{R}^k \}.
\]

Using this in (9.6), we get

\[
\| \Pi x \|^2 = \| x \|^2 - \min_{y \in \mathbb{R}^k} \| x - Ty \|^2.
\]

Hence, solving the optimization problem (9.4) is equivalent to finding the best linear decoding map \( \hat{T} \) for the pair \( (Y, T) \), where \( Y = \mathbb{R}^k \) and \( T \) is the collection of all isometries \( T : \mathbb{R}^k \rightarrow \mathcal{H} \). Moreover, if we recall our assumption that \( X \in B(\mathcal{H}) \) with probability one, then we see that there is no loss of generality if we take

\[
\mathcal{Y} = B^k_2 := \{ y \in \mathbb{R}^k : \| y \|_2 \leq 1 \},
\]

i.e., the unit ball in \( (\mathbb{R}^k, \| \cdot \|_2) \). This follows from the fact that \( \| \Pi x \| \leq \| x \| \) for any projection \( \Pi \), so, in particular, for \( \Pi = TT^* \) the encoding \( \hat{y} \) in (9.1) can be written as \( \hat{y} = T^* x \), and

\[
\| \hat{y} \|_2 = \| T \hat{y} \| = \| TT^* x \| = \| \Pi x \| \leq \| x \| \leq 1.
\]

Thus, Theorem 9.1 applies with \( \alpha = 1 \). That said, there are much tighter bounds for PCA that rely on deeper structural results pertaining to finite-dimensional subspaces of Hilbert spaces, but that is beside the point. The key idea here is that we can already get nice bounds using the tools already at our fingertips.
1.2. Vector quantization or \( k \)-means clustering. Vector quantization (or \( k \)-means clustering) is a procedure that takes a vector \( x \in \mathcal{H} \) and maps it to its nearest neighbor in a finite set \( \mathcal{C} = \{\xi_1, \ldots, \xi_k\} \subset \mathcal{H} \), where \( k \) is a given positive integer:

\[
\hat{x} = \arg \min_{\xi \in \mathcal{C}} \|x - \xi\|^2.
\]

If \( X \) is random with distribution \( P \), then the optimal \( k \)-point quantizer is given a size-\( k \) set \( \mathcal{C} = \{\xi_1, \ldots, \xi_k\} \) that minimizes the reconstruction error

\[
\mathbb{E}_P \left[ \min_{\xi \in \mathcal{C}} \|X - \xi\|^2 \right]
\]

over all \( \mathcal{C} \subset \mathcal{H} \) with \( |\mathcal{C}| = k \). We can cast the problem of finding \( \mathcal{C} \) in our framework by taking \( Y = \{e_1, \ldots, e_k\} \) (the standard basis in \( \mathbb{R}^k \)) and letting \( T \) be the set of all linear operators \( T : \mathbb{R}^k \to \mathcal{H} \). It is easy to see that any \( \mathcal{C} \subset \mathcal{H} \) with \( |\mathcal{C}| = k \) can be obtained as an image of the standard basis \( \{e_1, \ldots, e_k\} \) under some linear operator \( T : \mathbb{R}^k \to \mathcal{H} \). Indeed, for any \( \mathcal{C} = \{\xi_1, \ldots, \xi_k\} \), we can just define a linear operator \( T : \mathbb{R}^k \to \mathcal{H} \) by

\[
Te_j := \xi_j, \quad 1 \leq j \leq k
\]

and then extending it to all of \( \mathbb{R}^k \) by linearity:

\[
T \left( \sum_{j=1}^k y_j e_j \right) = \sum_{j=1}^k y_j Te_j = \sum_{j=1}^k y_j \xi_j.
\]

So, another way to interpret the objective of vector quantization is as follows: given a distribution \( P \) supported on \( B(\mathcal{H}) \), we seek a \( k \)-element set \( \mathcal{C} = \{\xi_1, \ldots, \xi_k\} \subset \mathcal{H} \), such that the random vector \( X \sim P \) can be well-approximated on average by linear combinations of the form

\[
\sum_{j=1}^k y_j \xi_j,
\]

where the vector of coefficients \( y = (y_1, \ldots, y_k) \) can have only one nonzero component, which is furthermore required to be equal to 1. In fact, there is no loss of generality in assuming that \( \mathcal{C} \subset B(\mathcal{H}) \) as well. This is a consequence of the fact that, for any \( x \in B(\mathcal{H}) \) and any \( x' \in \mathcal{H} \), we can always find some \( x'' \in B(\mathcal{H}) \) such that

\[
\|x - x''\| \leq \|x - x'\|.
\]

Indeed, it suffices to take \( x'' = \arg \min_{z \in B(\mathcal{H})} \|x' - z\|^2 \), and it is not hard to show that \( x'' = x'/\|x'\| \).

Thus, Theorem 9.1 applies with \( \alpha = 1 \). Moreover, the excess risk grows linearly with dimension \( k \), cf. Eq. (9.3). It is not known whether this linear dependence on \( k \) is optimal — there are \( \Omega(\sqrt{k/n}) \) lower bounds for vector quantization, but it is still an open question whether these lower bounds are tight [MP10].
1.3. **Nonnegative matrix factorization.** Consider approximating the random vector  
\[ X \sim P, \]  
where \( P \) is supported on the unit ball \( B(\mathcal{H}) \), by linear combinations of the form  
\[ \sum_{j=1}^{k} y_j \xi_j, \]  
where the real vector \( y = (y_1, \ldots, y_k) \) is constrained to lie in the nonnegative orthant  
\[ \mathbb{R}_+^k := \{ y = (y_1, \ldots, y_k) \in \mathbb{R}^k : y_j \geq 0, 1 \leq j \leq k \}, \]  
while the unit vectors \( \xi_1, \ldots, \xi_k \in B(\mathcal{H}) \) are constrained by the positivity condition  
\[ \langle \xi_j, \xi_\ell \rangle_{\mathcal{H}} \geq 0, \quad 1 \leq j, \ell \leq k. \]  
This is a generalization of the nonnegative matrix factorization (NMF) problem, originally posed by Lee and Seung \[LS99\].

To cast NMF in our framework, let \( Y = \mathbb{R}_+^k \), and let \( T \) be the set of all linear operators \( T : \mathbb{R}^k \rightarrow \mathcal{H} \) such that (i) \( \| Te_j \| = 1 \) for all \( 1 \leq j \leq k \) and (ii) \( \langle Te_j, Te_\ell \rangle \geq 0 \) for all \( 1 \leq j, \ell \leq k \). Then the choice of \( T \) is equivalent to the choice of \( \xi_1, \ldots, \xi_k \in B(\mathcal{H}) \), as above. Moreover, it can be shown that, for any \( x \in B(\mathcal{H}) \) and any \( T \in T \), the minimum of \( \| x - Ty \|_2^2 \) over all \( y \in \mathbb{R}_+^k \) is achieved at some \( \hat{y} \in \mathbb{R}_+^k \) with \( \| \hat{y} \|_2 \leq 1 \). Thus, there is no loss of generality if we take \( Y = \mathbb{R}_+^k \cap B_2^k \). In this case, the conditions of Theorem 9.1 are satisfied with \( \alpha = 1 \).

1.4. **Sparse coding.** Take \( Y \) to be the \( \ell_1 \) unit ball  
\[ B_1^k := \left\{ y = (y_1, \ldots, y_k) \in \mathbb{R}^k : \| y \|_1 = \sum_{j=1}^{k} |y_j| \leq 1 \right\}, \]  
and let \( T \) be the collection of all linear operators \( T : \mathbb{R}^k \rightarrow \mathcal{H} \) with \( \| Te_j \| \leq 1 \) for all \( 1 \leq j \leq k \). In this case, the dimensionality reduction problem is to approximate a random \( X \in B(\mathcal{H}) \) by a linear combination of the form  
\[ \sum_{j=1}^{k} y_j \xi_j, \]  
where \( y = (y_1, \ldots, y_k) \in \mathbb{R}^k \) satisfies the constraint \( \| y \|_1 \leq 1 \), while the vectors \( \xi_1, \ldots, \xi_k \) belong to the unit ball \( B(\mathcal{H}) \). Then for any \( y = \sum_{j=1}^{k} y_j e_j \in Y \) we have  
\[ \| Ty \| = \left\| \sum_{j=1}^{k} y_j Te_j \right\| \leq \sum_{j=1}^{k} |y_j| \| Te_j \| \leq \| y \|_1 \cdot \max_{1 \leq j \leq k} \| Te_j \| \leq 1, \]  
where the third line is by Hölder’s inequality. Then the conditions of Theorem 9.1 are satisfied with \( \alpha = 1 \).
2. Proof of Theorem 9.1

Now we turn to the proof of Theorem 9.1. The format of the proof is the familiar one: if we consider the empirical reconstruction error

\[ L_n(T) := \frac{1}{n} \sum_{i=1}^{n} f_T(X_i) \]

for every \( T \in \mathcal{T} \) and define the uniform deviation

\[ \Delta_n(X^n) := \sup_{T \in \mathcal{T}} |L_n(T) - L(T)|, \]

(9.7) then

\[ L(\hat{T}_n) \leq L^*(\mathcal{T}) + 2\Delta_n(X^n). \]

Now, for any \( x \in B(\mathcal{H}) \), any \( y \in \mathcal{Y} \), and any \( T \in \mathcal{T} \), we have

\[ 0 \leq \|x - Ty\| \leq 2\|x\| + 2\|Ty\| \leq 4\alpha^2. \]

Thus, the uniform deviation \( \Delta_n(X^n) \) has bounded differences with \( c_1 = \ldots = c_n = 4\alpha^2/n \), so by McDiarmid’s inequality,

\[ L(\hat{T}_n) \leq L^*(\mathcal{T}) + 2E\Delta_n(X^n) + 4\alpha^2 \sqrt{\frac{2\log(1/\delta)}{n}}, \]

(9.8) with probability at least \( 1 - \delta \). By the usual symmetrization argument, we obtain the bound \( E\Delta_n(X^n) \leq 2E R_n(\mathcal{F}(X^n)) \), where \( \mathcal{F} \) is the class of functions \( f_T \) for all \( T \in \mathcal{T} \). Now, the whole affair hinges on getting a good upper bound on the Rademacher averages \( R_n(\mathcal{F}(X^n)) \). We will do this in several steps, and we need to introduce some additional machinery along the way.

2.1. Gaussian averages. Let \( \gamma_1, \ldots, \gamma_n \) be i.i.d. standard normal random variables. In analogy to the Rademacher average of a bounded set \( A \subset \mathbb{R}^n \), we can define the Gaussian average of \( A \) [BM02] as

\[ G_n(A) := E_{\gamma^n} \sup_{a \in A} \left| \frac{1}{n} \sum_{i=1}^{n} \gamma_i a_i \right|. \]

**Lemma 9.1** (Gaussian averages vs. Rademacher averages).

\[ R_n(A) \leq \sqrt{\frac{\pi}{2}} G_n(A). \]

**Proof.** Let \( \sigma^n = (\sigma_1, \ldots, \sigma_n) \) be an \( n \)-tuple of i.i.d. Rademacher random variables independent of \( \gamma^n \). Since each \( \gamma_i \) is a symmetric random variable, it has the same distribution
as $\sigma_i|\gamma_i|$. Therefore,

$$G_n(A) = \frac{1}{n} \mathbb{E}_{\gamma} \sup_{a \in A} \left| \sum_{i=1}^{n} \gamma_i a_i \right|$$

$$= \frac{1}{n} \mathbb{E}_{\sigma} \mathbb{E}_{\gamma} \sup_{a \in A} \left| \sum_{i=1}^{n} \sigma_i |\gamma_i| a_i \right|$$

$$\geq \frac{1}{n} \mathbb{E}_{\sigma} \sup_{a \in A} \left| \sum_{i=1}^{n} \sigma_i a_i \mathbb{E}_{\gamma} |\gamma_i| \right|$$

$$= \mathbb{E} |\gamma_1| \cdot \frac{1}{n} \mathbb{E}_{\sigma} \sup_{a \in A} \left| \sum_{i=1}^{n} \sigma_i a_i \right|$$

$$= \mathbb{E} |\gamma_1| R_n(A),$$

where the second step is by convexity, while in the last step we have used the fact that $\gamma_1, \ldots, \gamma_n$ are i.i.d. random variables. Now, if $\gamma$ is a standard normal random variable, then

$$\mathbb{E} |\gamma| = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{\infty} |t| e^{-t^2/2} dt$$

$$= \frac{1}{\sqrt{2\pi}} \int_{0}^{\infty} t e^{-t^2/2} dt - \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{0} t e^{-t^2/2} dt$$

$$= \sqrt{\frac{2}{\pi}} \int_{0}^{\infty} t e^{-t^2/2} dt$$

$$= \sqrt{\frac{2}{\pi}}.$$

Rearranging, we get (9.9). \qed

Gaussian averages are often easier to work with than Rademacher averages. The reason for this is that, for any $n$ real constants $a_1, \ldots, a_n$, the sum $W_a := a_1 \gamma_1 + \ldots + a_n \gamma_n$ is a Gaussian random variable with mean 0 and variance $a_1^2 + \ldots + a_n^2$. Moreover, for any finite collection of vectors $a^{(1)}, \ldots, a^{(m)} \in \mathcal{A}$, the random variables $W_{a^{(1)}}, \ldots, W_{a^{(m)}}$ are jointly Gaussian. Thus, the collection of random variables $(W_a)_{a \in \mathcal{A}}$ is a zero-mean Gaussian process, where we say that a collection of real-valued random variables $(W_a)_{a \in \mathcal{A}}$ is a Gaussian process if all finite linear combinations of the $W_a$'s are Gaussian random variables. In particular, we
can compute covariances: for any \(a, a' \in \mathcal{A}\),
\[
\mathbb{E}[W_a W_{a'}] = \mathbb{E} \left[ \sum_{i=1}^{n} \sum_{j=1}^{n} \gamma_i \gamma_j a_i a'_j \right]
= \sum_{i=1}^{n} \sum_{j=1}^{n} \mathbb{E}[\gamma_i \gamma_j] a_i a'_j
= \sum_{i=1}^{n} a_i a'_i
= \langle a, a' \rangle
\]
and things like
\[
\mathbb{E}[ (W_a - W_{a'})^2 ] = \mathbb{E} \left[ \sum_{i=1}^{n} \sum_{j=1}^{n} \gamma_i \gamma_j (a_i - a'_i)(a_j - a'_j) \right]
= \sum_{i=1}^{n} \sum_{j=1}^{n} \mathbb{E}[\gamma_i \gamma_j] (a_i - a'_i)(a_j - a'_j)
= \sum_{i=1}^{n} (a_i - a'_i)^2
= \|a - a'|^2.
\]
The latter quantities are handy because of a very useful result called Slepian’s lemma [Sle62, LT91]:

**Lemma 9.2.** Let \((W_a)_{a \in \mathcal{A}}\) and \((V_a)_{a \in \mathcal{A}}\) be two zero-mean Gaussian processes with some index set \(\mathcal{A}\) (not necessarily a subset of \(\mathbb{R}^n\)), such that
\[
\mathbb{E}[ (W_a - W_{a'})^2 ] \leq \mathbb{E}[ (V_a - V_{a'})^2 ], \quad \forall a, a' \in \mathcal{A}.
\]
Then
\[
\mathbb{E} \sup_{a \in \mathcal{A}} W_a \leq \mathbb{E} \sup_{a \in \mathcal{A}} V_a.
\]

**Remark 9.2.** The Gaussian processes \((W_a), (V_a)\) that appear in Slepian’s lemma are not necessarily of the form \(W_a = \langle a, \gamma^n \rangle\) with \(\gamma^n = (\gamma_1, \ldots, \gamma_n)\) a vector of independent Gaussians. They can be arbitrarily collections of random variables indexed by the elements of \(\mathcal{A}\), such that any finite linear combination of \(W_a\’s\) or of \(V_a\’s\) is Gaussian.

Slepian’s lemma is typically used to obtain upper bounds on the expected supremum of one Gaussian process in terms of another, which is hopefully easier to handle. The only wrinkle is that we can’t apply Slepian’s lemma to the problem of estimating the Gaussian average \(G_n(\mathcal{A})\) because of the absolute value. However, if all \(a \in \mathcal{A}\) are uniformly bounded in norm, the absolute value makes little difference:
Lemma 9.3. Let $\mathcal{A} \subset \mathbb{R}^n$ be a set of vectors uniformly bounded in norm, i.e., there exists some $L < \infty$ such that $\|a\| \leq L$ for all $a \in \mathcal{A}$. Let

$$
\tilde{G}_n(A) := \frac{1}{n} \mathbb{E} \left[ \sup_{a \in A} \sum_{i=1}^{n} \gamma_i a_i \right].
$$

Then

$$
\tilde{G}_n(A) \leq G_n(A) \leq 2\tilde{G}_n(A) + \sqrt{\frac{2 L}{\pi n}}.
$$

Proof. The first inequality in (9.13) is obvious. For the second inequality, pick an arbitrary $a' \in \mathcal{A}$, let $W_a = \sum_{i=1}^{n} \gamma_i a_i$ for any $a \in \mathcal{A}$, and write

$$
G_n(A) = \frac{1}{n} \mathbb{E} \left[ \sup_{a \in \mathcal{A}} |W_a| \right] 
= \frac{1}{n} \mathbb{E} \left[ \sup_{a \in \mathcal{A}} |W_a - W_{a'}| \right] + \frac{1}{n} \mathbb{E} |W_{a'}|.
$$

Since $a'$ was arbitrary, this gives

$$
G_n(A) \leq \sup_{a' \in \mathcal{A}} \left\{ \frac{1}{n} \mathbb{E} \left[ \sup_{a \in \mathcal{A}} |W_a - W_{a'}| \right] + \frac{1}{n} \mathbb{E} |W_{a'}| \right\}
\leq \frac{1}{n} \mathbb{E} \left[ \sup_{a,a' \in \mathcal{A}} |W_a - W_{a'}| \right] + \frac{1}{n} \sup_{a' \in \mathcal{A}} \mathbb{E} |W_{a'}|.
$$

For any two $a, a'$, the random variable $W_a - W_{a'}$ is symmetric, so

$$
\mathbb{E} \left[ \sup_{a,a' \in \mathcal{A}} |W_a - W_{a'}| \right] = 2 \mathbb{E} \left[ \sup_{a \in \mathcal{A}} W_a \right].
$$

Moreover, for any $a' \in \mathcal{A}$, $W_{a'}$ is Gaussian with zero mean and variance $\|a'\|^2 \leq L^2$. Thus,

$$
\sup_{a' \in \mathcal{A}} \mathbb{E} |W_{a'}| \leq L \mathbb{E} |\gamma| = \sqrt{\frac{2}{\pi}} L.
$$

Using the two above formulas in (9.14), we get the second inequality in (9.13), and the lemma is proved.

Armed with this lemma, we can work with the quantity $\tilde{G}_n(A)$ instead of the Gaussian average $G_n(A)$. The advantage is that now we can rely on tools like Slepian’s lemma.

2.2. Bounding the Rademacher average. Now everything hinges on bounding the Gaussian average $G_n(F(x^n))$ for a fixed sample $x^n = (x_1, \ldots, x_n)$, which in turn will give us a bound on the Rademacher average $R_n(F(x^n))$, by Lemmas 9.1 and 9.3. Let $(\gamma_i)_{1 \leq i \leq n}$, $(\gamma_{ij})_{1 \leq i \leq n, 1 \leq j \leq k}$, and $(\gamma_{ijk})_{1 \leq i \leq n, 1 \leq j \leq k, 1 \leq \ell \leq k}$ be mutually independent sequences of i.i.d. standard Gaussian random variables. Define the following zero-mean Gaussian processes, indexed by
$T \in \mathcal{T}$:

\[ W_T := \sum_{i=1}^{n} \gamma_i f_T(x_i), \]

\[ V_T := \sum_{i=1}^{n} \sum_{j=1}^{k} \gamma_{ij} \langle x_i, Te_j \rangle, \]

\[ U_T := \sum_{i=1}^{n} \sum_{j=1}^{k} \sum_{\ell=1}^{k} \gamma_{ij\ell} \langle Te_j, Te_\ell \rangle, \]

\[ \Upsilon_T := \sqrt{8V_T + 2U_T}. \]

By definition,

\[ G_n(F(x^n)) = \mathbf{E} \sup_{T \in \mathcal{T}} \left| \frac{1}{n} \sum_{i=1}^{n} \gamma_i f_T(x_i) \right| \]

\[ = \frac{1}{n} \mathbf{E} \sup_{T \in \mathcal{T}} |W_T|, \]

and we define $\tilde{G}_n(F(x^n))$ similarly. We will use Slepian’s lemma to upper-bound $\tilde{G}_n(F(x^n))$ in terms of expected suprema of $(V_T)_{T \in \mathcal{T}}$ and $(U_T)_{T \in \mathcal{T}}$. To that end, we start with

\[ \mathbf{E} \left[ (W_T - W_{T'})^2 \right] = \sum_{i=1}^{n} (f_T(x_i) - f_{T'}(x_i))^2 \]

\[ = \sum_{i=1}^{n} \left( \min_{y \in \mathcal{Y}} \|x_i - Ty\|^2 - \min_{y \in \mathcal{Y}} \|x_i - T'y\|^2 \right)^2 \]

\[ \leq \sum_{i=1}^{n} \left( \max_{y \in \mathcal{Y}} \|x_i - Ty\|^2 - \|x_i - T'y\|^2 \right)^2 \]

\[ = \sum_{i=1}^{n} \left( \max_{y \in \mathcal{Y}} 2\langle x_i, Ty - T'y \rangle + \|Ty\|^2 - \|T'y\|^2 \right)^2 \]

\[ \leq 8 \sum_{i=1}^{n} \max_{y \in \mathcal{Y}} |\langle x_i, Ty - T'y \rangle|^2 + 2 \sum_{i=1}^{n} \max_{y \in \mathcal{Y}} (\|Ty\|^2 - \|T'y\|^2)^2, \]

(9.15)
where in the third line we have used properties of inner products, and the last line is by the inequality \((a + b)^2 \leq 2a^2 + 2b^2\). Now, for each \(i\),

\[
\max_{y \in Y} |\langle x_i, Ty - T'y \rangle|^2 = \max_{y \in Y} \left| \sum_{j=1}^{k} y_j \langle x_i, Te_j - T'e_j \rangle \right|^2
\]

\[
\leq \max_{y \in Y} \|y\|^2 \sum_{j=1}^{k} |\langle x_i, Te_j - T'e_j \rangle|^2
\]

\[
\leq \sum_{j=1}^{k} \|\langle x_i, Te_j - T'e_j \rangle\|^2,
\]

where in the second step we have used Cauchy–Schwarz. Summing over \(1 \leq i \leq n\), we see that

\[
\sum_{i=1}^{n} \max_{y \in Y} |\langle x_i, Ty - T'y \rangle|^2 \leq \sum_{i=1}^{n} \sum_{j=1}^{k} |\langle x_i, Te_j - T'e_j \rangle|^2
\]

(9.16)

\[
= E \left[ (V_T - V'_T)^2 \right].
\]

Similarly,

\[
\max_{y \in Y} (\|Ty\|^2 - \|T'y\|^2)^2 = \max_{y \in Y} \left( \sum_{j=1}^{k} \sum_{\ell=1}^{k} y_j y_{\ell} \langle Te_j, Te_{\ell} \rangle - \langle T'e_j, T'e_{\ell} \rangle \right)^2
\]

\[
\leq \max_{y \in Y} \|y\|^4 \cdot \sum_{j=1}^{k} \sum_{\ell=1}^{k} \|\langle Te_j, Te_{\ell} \rangle - \langle T'e_j, T'e_{\ell} \rangle\|^2
\]

\[
= \max_{y \in Y} \parallel y \parallel^4 \sum_{j=1}^{k} \sum_{\ell=1}^{k} (\langle Te_j, Te_{\ell} \rangle - \langle T'e_j, T'e_{\ell} \rangle)^2,
\]

\[
\leq \sum_{j=1}^{k} \sum_{\ell=1}^{k} (\langle Te_j, Te_{\ell} \rangle - \langle T'e_j, T'e_{\ell} \rangle)^2.
\]

Therefore,

(9.17)

\[
\sum_{i=1}^{n} \max_{y \in Y} (\|Ty\|^2 - \|T'y\|^2) \leq E \left[ (U_T - U'_T)^2 \right].
\]

Using (9.16) and (9.17) in (9.15), we have

\[
E \left[ (W_T - W'_T)^2 \right] \leq 8E \left[ (V_T - V'_T)^2 \right] + 2E \left[ (U_T - U'_T)^2 \right]
\]

\[
= E \left[ (\Upsilon_T - \Upsilon'_T)^2 \right].
\]

109
We can therefore apply Slepian’s lemma (Lemma 9.2) to \((W_T)_{T \in \mathcal{T}}\) and \((\Upsilon_T)_{T \in \mathcal{T}}\) to write

\[
\tilde{G}_n(\mathcal{F}(x^n)) = \frac{1}{n} \mathbb{E} \sup_{T \in \mathcal{T}} W_T \\
\leq \frac{1}{n} \mathbb{E} \sup_{T \in \mathcal{T}} \Upsilon_T \\
\leq \frac{\sqrt{8}}{n} \mathbb{E} \sup_{T \in \mathcal{T}} V_T + \frac{\sqrt{2}}{n} \mathbb{E} \sup_{T \in \mathcal{T}} U_T. 
\]

(9.18)

We now upper-bound the expected suprema of \(V_T\) and \(U_T\). For the former,

\[
\mathbb{E} \sup_{T \in \mathcal{T}} V_T = \mathbb{E} \sup_{T \in \mathcal{T}} \sum_{i=1}^{n} \sum_{j=1}^{k} \gamma_{ij} \langle x_i, T e_j \rangle \\
= \mathbb{E} \sup_{T \in \mathcal{T}} \sum_{j=1}^{k} \left( \sum_{i=1}^{n} \gamma_{ij} x_i, T e_j \right) \\
\leq \mathbb{E} \sup_{T \in \mathcal{T}} \sum_{j=1}^{k} \left\| \sum_{i=1}^{n} \gamma_{ij} x_i \right\| \| T e_j \| \\
\leq \mathbb{E} \sum_{j=1}^{k} \left\| \sum_{i=1}^{n} \gamma_{ij} x_i \right\| \sup_{T \in \mathcal{T}} \| T e_j \| \\
\leq \alpha \sum_{j=1}^{k} \mathbb{E} \left\| \sum_{i=1}^{n} \gamma_{ij} x_i \right\| \\
\leq \alpha \sum_{j=1}^{k} \mathbb{E} \sqrt{\sum_{i=1}^{n} \sum_{i' = 1}^{n} \gamma_{ij} \gamma_{i'j} \langle x_i, x_{i'} \rangle} \\
\leq \alpha \sum_{j=1}^{k} \sqrt{\sum_{i=1}^{n} \sum_{i' = 1}^{n} \mathbb{E} \left[ \gamma_{ij} \gamma_{i'j} \right] \langle x_i, x_{i'} \rangle} \\
= \alpha \sum_{j=1}^{k} \sqrt{\sum_{i=1}^{n} \| x_i \|^2} \\
\leq \alpha k \sqrt{n}. 
\]

\((x_i \in B(\mathcal{H})\text{ for all } i)\)
Similarly, for the latter,

\[
E \sup_{T \in \mathcal{T}} U_T = E \sup_{T \in \mathcal{T}} \sum_{i=1}^{n} \sum_{j=1}^{k} \sum_{\ell=1}^{k} \gamma_{ij\ell} \langle Te_j, Te_\ell \rangle \\
\leq \sum_{j=1}^{k} \sum_{\ell=1}^{k} E \sup_{T \in \mathcal{T}} \sum_{i=1}^{n} \gamma_{ij\ell} \langle Te_j, Te_\ell \rangle \\
\leq \sum_{j=1}^{k} \sum_{\ell=1}^{k} E \left| \sum_{i=1}^{n} \gamma_{ij\ell} \right| \sup_{T \in \mathcal{T}} \|Te_j\| \|Te_\ell\| \\
\leq \alpha^2 k^2 \sqrt{\frac{2n}{\pi}}.
\]

Substituting these bounds into (9.18), we have

\[
\tilde{G}_n(\mathcal{F}(x^n)) \leq \frac{1}{n} \left( \alpha k \sqrt{8n} + \alpha^2 k^2 \frac{2\sqrt{n}}{\sqrt{\pi}} \right) \leq \frac{5\alpha^2 k^2}{\sqrt{n}}.
\]

Thus, applying Lemmas 9.1 and 9.3, we have

\[
R_n(\mathcal{F}(x^n)) \leq \sqrt{\frac{\pi}{2}} G_n(\mathcal{F}(x^n)) \\
\leq \sqrt{\frac{\pi}{2}} \left[ 2\tilde{G}_n(\mathcal{F}(x^n)) + \frac{2}{\pi} \max_{T \in \mathcal{T}} \sqrt{\sum_{i=1}^{n} |f_T(x_i)|^2} \right] \\
\leq \sqrt{\frac{\pi}{2}} \left[ \frac{10\alpha^2 k^2}{\sqrt{n}} + \sqrt{\frac{2}{\pi}} \frac{2\alpha}{\sqrt{n}} \right] \\
\leq \frac{15\alpha^2 k^2}{\sqrt{n}}
\]

Recalling (9.8), we see that the event (9.2) holds with probability at least \(1 - \delta\).

For the special case of \(k\)-means clustering, i.e., when \(Y = \{e_1, \ldots, e_k\}\), we follow a slightly different strategy. Define a zero-mean Gaussian process

\[
\Xi_T := \sum_{i=1}^{n} \sum_{j=1}^{k} \gamma_{ij} \|x_i - Te_j\|^2, \quad T \in \mathcal{T}.
\]
Then
\[
\mathbb{E} \left[ (W_T - W_{T'})^2 \right] = \sum_{i=1}^{n} \left( \min_{1 \leq j \leq k} \|x_i - T e_j\|^2 - \min_{1 \leq j \leq k} \|x_i - T' e_j\|^2 \right)^2 \\
\leq \sum_{i=1}^{n} \max_{1 \leq j \leq k} \left( \|x_i - T e_j\|^2 - \|x_i - T' e_j\|^2 \right)^2 \\
\leq \sum_{i=1}^{n} \sum_{j=1}^{k} \left( \|x_i - T e_j\|^2 - \|x_i - T' e_j\|^2 \right)^2 \\
= \mathbb{E} \left[ (\Xi - \Xi_{T'})^2 \right].
\]

For the process \((\Xi_T)\), we have
\[
\mathbb{E} \sup_{T \in T} \Xi_T = \mathbb{E} \sup_{T \in T} \sum_{i=1}^{n} \sum_{j=1}^{k} \gamma_{ij} \|x_i - T e_j\|^2 \\
= \mathbb{E} \sup_{T \in T} \sum_{i=1}^{n} \sum_{j=1}^{k} \gamma_{ij} \left\{ \|x_i\|^2 - 2\langle x_i, T e_j \rangle + \|T e_j\|^2 \right\} \\
\leq \sum_{j=1}^{k} \mathbb{E} \sup_{T \in T} \left\{ 2 \sum_{i=1}^{n} \gamma_{ij} |\langle x_i, T e_j \rangle| + \sum_{i=1}^{n} \gamma_{ij} \|T e_j\|^2 \right\} \\
\leq 3k\alpha^2 \sqrt{n},
\]
where the methods used to obtain this bound are similar to what we did for \((V_T)\) and \((U_T)\).

Using Lemmas 9.1–9.3, we have
\[
R_n(\mathcal{F}(x^n)) \leq \sqrt{\frac{\pi}{2}} G_n(\mathcal{F}(x^n)) \\
\leq \sqrt{\frac{\pi}{2}} \left[ 2\tilde{G}_n(\mathcal{F}(x^n)) + \sqrt{\frac{2}{\pi}} \max_{T \in T} \sqrt{\sum_{i=1}^{n} |f_T(x_i)|^2} \right] \\
\leq \sqrt{\frac{\pi}{2}} \left[ \frac{6\alpha^2 k}{\sqrt{n}} + \sqrt{\frac{2}{\pi}} \frac{2\alpha}{\sqrt{n}} \right] \\
\leq \frac{10\alpha^2 k}{\sqrt{n}}.
\]

Again, recalling (9.8), we see that the event (9.3) occurs with probability at least \(1 - \delta\). The proof of Theorem 9.1 is complete.

### 3. Linear operators between Hilbert spaces

We assume, for simplicity, that all Hilbert spaces \(\mathcal{H}\) of interest are separable. By definition, a Hilbert space \(\mathcal{H}\) is separable if it has a countable dense subset: there exists a countable set \(\{h_1, h_2, \ldots\} \subset \mathcal{H}\), such that for any \(h \in \mathcal{H}\) and any \(\varepsilon > 0\) there exists some \(j \in \mathbb{N}\), for which \(||h - h_j||_{\mathcal{H}} < \varepsilon\). Any separable Hilbert space \(\mathcal{H}\) has a countable complete and orthonormal basis, i.e., a countable set \(\{\varphi_1, \varphi_2, \ldots\} \subset \mathcal{H}\) with the following properties:
(1) **Orthonormality** — $\langle \varphi_i, \varphi_j \rangle_\mathcal{H} = \delta_{ij}$;

(2) **Completeness** — if there exists some $h \in \mathcal{H}$ which is orthogonal to all $\varphi_j$’s, i.e., $\langle h, \varphi_j \rangle = 0$ for all $j$, then $h = 0$.

As a consequence, any $h \in \mathcal{H}$ can be uniquely represented as an infinite linear combination

$$h = \sum_{j=1}^{\infty} c_j \varphi_j,$$

where $c_j = \langle h, \varphi_j \rangle_\mathcal{H}$,

where the infinite series converges in norm, i.e., for any $\varepsilon > 0$ there exists some $n \in \mathbb{N}$, such that

$$\left\| \varphi - \sum_{j=1}^{n} c_j \varphi_j \right\|_\mathcal{H} < \varepsilon.$$

Moreover, $\|h\|_\mathcal{H}^2 = \sum_{j=1}^{\infty} |c_j|^2$.

Let $\mathcal{H}$ and $\mathcal{K}$ be two Hilbert spaces. A **linear operator** from $\mathcal{H}$ into $\mathcal{K}$ is a mapping $T : \mathcal{H} \to \mathcal{K}$, such that (i) $T(\alpha h + \alpha' h') = \alpha Th + \alpha'Th'$ for any two $h, h' \in \mathcal{H}$ and $\alpha, \alpha' \in \mathbb{R}$.

A linear operator $T : \mathcal{H} \to \mathcal{K}$ is **bounded** if

$$\|T\|_{\mathcal{H} \to \mathcal{K}} := \sup_{h \in \mathcal{H}, h \neq 0} \frac{\|Th\|_\mathcal{K}}{\|h\|_\mathcal{H}} < \infty.$$

We will denote the space of all bounded linear operators $T : \mathcal{H} \to \mathcal{K}$ by $\mathcal{L}(\mathcal{H}, \mathcal{K})$. When $\mathcal{H} = \mathcal{K}$, we will write $\mathcal{L}(\mathcal{H})$ instead. For any operator $T \in \mathcal{L}(\mathcal{H}, \mathcal{K})$, we have the **adjoint operator** $T^* \in \mathcal{L}(\mathcal{K}, \mathcal{H})$, which is characterized by

$$\langle g, Th \rangle_\mathcal{K} = \langle T^* g, h \rangle_\mathcal{H}, \quad \forall g \in \mathcal{K}, h \in \mathcal{H}.$$

If $T \in \mathcal{L}(\mathcal{H})$ has the property that $T = T^*$, we say that $T$ is **self-adjoint**.

Some examples:

- The **identity operator** on $\mathcal{H}$, denoted by $I_\mathcal{H}$, maps each $h \in \mathcal{H}$ to itself. $I_\mathcal{H}$ is a self-adjoint operator with $\|I_\mathcal{H}\| \equiv \|I_\mathcal{H}\|_{\mathcal{H} \to \mathcal{H}} = 1$. We will often omit the index $\mathcal{H}$ and just write $I$.

- A **projection** is an operator $\Pi \in \mathcal{L}(\mathcal{H})$ satisfying $\Pi^2 = \Pi$, i.e., $\Pi(\Pi h) = \Pi h$ for any $h \in \mathcal{H}$. This is a bounded operator with $\|\Pi\| = 1$. Any projection is self-adjoint.

- An **isometry** is an operator $T \in \mathcal{L}(\mathcal{H}, \mathcal{K})$, such that $\|Th\|_\mathcal{K} = \|h\|_\mathcal{H}$ for all $h \in \mathcal{H}$, i.e., $T$ preserves norms. If $T$ is an isometry, then $T^*T = I_\mathcal{H}$, while $TT^* \in \mathcal{L}(\mathcal{K})$ is a projection. This is easy to see:

$$\langle TT^*TT^*, h \rangle_\mathcal{H} = \langle TT^*, h \rangle_\mathcal{K} = \langle h, h \rangle_\mathcal{H},$$

If $T \in \mathcal{L}(\mathcal{H})$ and $T^* \in \mathcal{L}(\mathcal{H})$ are both isometries, then $T$ is called a **unitary operator**.

- If $\Pi \in \mathcal{L}(\mathcal{H})$ is a projection whose range $\mathcal{K} \subseteq \mathcal{H}$ is a closed $k$-dimensional subspace, then there exists an isometry $T \in \mathcal{L}(\mathbb{R}^k, \mathcal{K})$, such that $\Pi = TT^*$. Here, $\mathbb{R}^k$ is a Hilbert space with the usual $\| \cdot \|_2$ norm. To see this, let $\{\psi_1, \ldots, \psi_k\} \subset \mathcal{H}$ be an orthonormal basis of $\mathcal{K}$, and complete it to a countable basis $\{\psi_1, \psi_2, \ldots, \psi_k, \psi_{k+1}, \psi_{k+2}, \ldots\}$ for the entire $\mathcal{H}$. Here, the elements of $\{\psi_j\}_{j=k+1}^\infty$
are mutually orthonormal and orthogonal to \( \{\psi_j\}_{j=1}^k \). Any \( h \in \mathcal{H} \) has a unique representation

\[
h = \sum_{j=1}^{\infty} \alpha_j \psi_j
\]

for some real coefficients \( \alpha_1, \alpha_2, \ldots \). With this, we can write out the action of \( \Pi \) explicitly as

\[
\Pi h = \sum_{j=1}^{k} \alpha_j \psi_j.
\]

Now consider the map \( T : \mathbb{R}^k \to \mathcal{K} \) that takes

\[
\alpha = (\alpha_1, \ldots, \alpha_k) \in \mathbb{R}^k \mapsto \sum_{j=1}^{k} \alpha_j \psi_j.
\]

It is easy to see that \( T \) is an isometry. Indeed,

\[
\|T\alpha\|_{\mathcal{H}} = \left\| \sum_{j=1}^{k} \alpha_j \psi_j \right\|_{\mathcal{H}} = \sqrt{\sum_{j=1}^{k} \alpha_j^2} = \|\alpha\|_2.
\]

The adjoint of \( T \) is easily computed: for any \( \alpha = (\alpha_1, \ldots, \alpha_k) \in \mathbb{R}^k \) and any \( h' = \sum_{j=1}^{\infty} \alpha'_j \psi_j \in \mathcal{H} \),

\[
\langle h', T\alpha \rangle_{\mathcal{H}} = \langle \Pi h', T\alpha \rangle_{\mathcal{H}}
\]

\[
= \left\langle \sum_{j=1}^{k} \alpha'_j \psi_j, \sum_{j=1}^{k} \alpha_j \psi_j \right\rangle
\]

\[
= \sum_{j=1}^{k} \alpha'_j \alpha_j
\]

\[
= \langle T^* h', \alpha \rangle.
\]

Since this must hold for arbitrary \( \alpha \in \mathbb{R}^k \) and \( h' \in \mathcal{H}' \), we must have \( T^* h' = T^* \left( \sum_{j=1}^{\infty} \alpha'_j \psi_j \right) = (\alpha'_1, \ldots, \alpha'_k) \). Now let’s compute \( T^* h \) for any \( h = \sum_{j=1}^{k} \alpha_j \psi_j \):

\[
TT^* h = T(T^* h)
\]

\[
= T \left( T^* \left( \sum_{j=1}^{\infty} \alpha_j \psi_j \right) \right)
\]

\[
= T \left( (\alpha_1, \ldots, \alpha_k) \right)
\]

\[
= \sum_{j=1}^{k} \alpha_j \psi_j
\]

\[
= \Pi h.
\]
In this chapter, we will look at an application of statistical learning theory to the problem of efficient stochastic simulation, which arises frequently in engineering design. The basic question is as follows. Suppose we have a system with input space \( Z \). The system has a tunable parameter \( \theta \) that lies in some set \( \Theta \). We have a performance index \( \ell : \mathbb{R} \times \Theta \to [0,1] \), where we assume that the lower the value of \( \ell \), the better the performance. Thus, if we use the parameter setting \( \theta \in \Theta \) and apply input \( z \in \mathbb{R} \), the performance of the corresponding system is given by the scalar \( \ell(z, \theta) \in [0,1] \). Now let’s suppose that the input to the system is actually a random variable \( Z \in \mathbb{R} \) with some distribution \( P \in \mathcal{P}(\mathbb{R}) \). Then we can define the operating characteristic

\[
L(\theta) := \mathbb{E}_P[\ell(Z, \theta)] = \int_{\mathbb{R}} \ell(z, \theta) P\{dz\}, \quad \theta \in \Theta.
\]

The goal is to find an optimal operating point \( \theta^* \in \Theta \) that achieves (or comes arbitrarily close to) \( \inf_{\theta \in \Theta} L(\theta) \).

In practice, the problem of minimizing \( L(\theta) \) is quite difficult for large-scale systems. First of all, computing the integral in (10.1) may be a challenge. Secondly, we may not even know the distribution \( P_Z \). Thirdly, there may be more than one distribution of the input, each corresponding to different operating regimes and/or environments. For this reason, engineers often resort to Monte Carlo simulation techniques: Assuming we can efficiently sample from \( P_Z \), we draw a large number of independent samples \( Z_1, Z_2, \ldots, Z_n \) and compute

\[
\hat{\theta}_n = \arg\min_{\theta \in \Theta} L_n(\theta) = \arg\min_{\theta \in \Theta} \frac{1}{n} \sum_{i=1}^{n} \ell(Z_i, \theta),
\]

where \( L_n(\cdot) \) denotes the empirical version of the operating characteristic (10.1). Given an accuracy parameter \( \varepsilon > 0 \) and a confidence parameter \( \delta \in (0,1) \), we simply need to draw enough samples, so that

\[
L(\hat{\theta}_n) \leq \inf_{\theta \in \Theta} L(\theta) + \varepsilon
\]

with probability at least \( 1 - \delta \), regardless of what the true distribution \( P_Z \) happens to be.

This is, of course, just another instance of the ERM algorithm we have been studying extensively. However, there are two issues. One is how many samples we need to guarantee that the empirically optimal operating point will be good. The other is the complexity of actually computing an empirical minimizer.

The first issue has already come up in the course under the name of sample complexity of learning. The second issue is often handled by relaxing the problem a bit: We choose a probability distribution \( Q \) over \( \Theta \) (assuming it can be equipped with an appropriate \( \sigma \)-algebra) and, instead of minimizing \( L(\theta) \) over \( \theta \in \Theta \), set some level parameter \( \alpha \in (0,1) \),
and seek any $\hat{\theta} \in \Theta$, for which there exists some exceptional set $\Lambda \subset \Theta$ with $Q(\Lambda) \leq \alpha$, such that

$$\inf_{\theta} L(\theta) - \varepsilon \leq L(\hat{\theta}) \leq \inf_{\theta \in \Theta \setminus \Lambda} L(\theta) + \varepsilon$$

with probability at least $1 - \delta$. Unless the actual optimal operating point $\theta^*$ happens to lie in the exceptional set $\Lambda$, we will come to within $\varepsilon$ of the optimum with confidence at least $1 - \delta$. Then we just need to draw a large enough number $n$ of samples $Z_1, \ldots, Z_n$ from $P_Z$ and a large enough number $m$ of samples $\theta_1, \ldots, \theta_m$ from $Q$, and then compute

$$\hat{\theta} = \arg \min_{\theta \in \{\theta_1, \ldots, \theta_m\}} L_n(\theta).$$

In the next several lectures, we will see how statistical learning theory can be used to develop such simulation procedures. Moreover, we will learn how to use Rademacher averages\(^1\) to determine how many samples we need in the process of learning. The use of statistical learning theory for simulation has been pioneered in the context of control by M. Vidyasagar [Vid98, Vid01]; the refinement of his techniques using Rademacher averages is due to Koltchinskii et al. [KAA+00a, KAA+00b]. We will essentially follow their presentation, but with slightly better constants.

We will follow the following plan. First, we will revisit the abstract ERM problem and its sample complexity. Then we will introduce a couple of refined tools pertaining to Rademacher averages. Next, we will look at sequential algorithms for empirical approximation, in which the sample complexity is not set a priori, but is rather determined by a data-driven stopping rule. And, finally, we will see how these sequential algorithms can be used to develop robust and efficient stochastic simulation strategies.

1. **Empirical Risk Minimization: a quick review**

Recall the abstract Empirical Risk Minimization problem: We have a space $Z$, a class $\mathcal{P}$ of probability distributions over $Z$, and a class $\mathcal{F}$ of measurable functions $f : Z \to [0, 1]$. Given an i.i.d. sample $Z^n$ drawn according to some unknown $P \in \mathcal{P}$, we compute

$$\hat{f}_n := \arg \min_{f \in \mathcal{F}} P_n(f) \equiv \arg \min_{f \in \mathcal{F}} \frac{1}{n} \sum_{i=1}^{n} f(Z_i).$$

We would like for $P(\hat{f}_n)$ to be close to $\inf_{f \in \mathcal{F}} P(f)$ with high probability. To that end, we have derived the bound

$$P(\hat{f}_n) - \inf_{f \in \mathcal{F}} P(f) \leq 2\|P_n - P\|_{\mathcal{F}},$$

where, as before, we have defined the uniform deviation

$$\|P_n - P\|_{\mathcal{F}} := \sup_{f \in \mathcal{F}} |P_n(f) - P(f)| = \sup_{f \in \mathcal{F}} \left| \frac{1}{n} \sum_{i=1}^{n} f(Z_i) - \mathbb{E}_P f(Z) \right|.$$ 

Hence, if $n$ is sufficiently large so that, for every $P \in \mathcal{P}$, $\|P_n - P\|_{\mathcal{F}} \leq \varepsilon/2$ with $P$-probability at least $1 - \delta$, then $P(\hat{f}_n)$ will be $\varepsilon$-close to $\inf_{f \in \mathcal{F}} P(f)$ with probability at least $1 - \delta$. This motivates the following definition:

\(^1\)More precisely, their stochastic counterpart, in which we do not take the expectation over the Rademacher sequence, but rather use it as a resource to aid the simulation.
**Definition 10.1.** Given the pair \((\mathcal{F}, \mathcal{P})\), an accuracy parameter \(\varepsilon > 0\), and a confidence parameter \(\delta \in (0, 1)\), the sample complexity of empirical approximation is

\[
N(\varepsilon; \delta) := \min \left\{ n \in \mathbb{N} : \sup_{P \in \mathcal{P}} \mathbb{P} \{ \| P_n - P \|_\mathcal{F} \geq \varepsilon \} \leq \delta \right\}.
\]

In other words, for any \(\varepsilon > 0\) and any \(\delta \in (0, 1)\), \(N(\varepsilon/2; \delta)\) is an upper bound on the number of samples needed to guarantee that \(P(\hat{f}_n) \leq \inf_{f \in \mathcal{F}} P(f) + \varepsilon\) with probability (confidence) at least \(1 - \delta\).

### 2. Empirical Rademacher averages

As before, let \(Z^n\) be an i.i.d. sample of length \(n\) from some \(P \in \mathcal{P}(Z)\). On multiple occasions we have seen that the performance of the ERM algorithm is controlled by the Rademacher average

\[
R_n(\mathcal{F}(Z^n)) := \frac{1}{n} \mathbb{E}_{\sigma^n} \left[ \sup_{f \in \mathcal{F}} \left| \sum_{i=1}^{n} \sigma_i f(Z_i) \right| \right],
\]

where \(\sigma^n = (\sigma_1, \ldots, \sigma_n)\) is an \(n\)-tuple of i.i.d. Rademacher random variables independent of \(Z^n\). More precisely, we have established the fundamental symmetrization inequality

\[
\mathbb{E} \| P_n - P \|_\mathcal{F} \leq 2 \mathbb{E} R_n(\mathcal{F}(Z^n)),
\]

as well as the concentration bounds

\[
\mathbb{P} \{ \| P_n - P \|_\mathcal{F} \geq \mathbb{E} \| P_n - P \|_\mathcal{F} + \varepsilon \} \leq e^{-2n\varepsilon^2}
\]

\[
\mathbb{P} \{ \| P_n - P \|_\mathcal{F} \leq \mathbb{E} \| P_n - P \|_\mathcal{F} - \varepsilon \} \leq e^{-2n\varepsilon^2}
\]

These results show two things:

1. The uniform deviation \(\| P_n - P \|_\mathcal{F}\) tightly concentrates around its expected value.
2. The expected value \(\mathbb{E} \| P_n - P \|_\mathcal{F}\) is bounded from above by \(\mathbb{E} R_n(\mathcal{F}(Z^n))\).

It turns out that the expected Rademacher average \(\mathbb{E} R_n(\mathcal{F}(Z^n))\) also furnishes a lower bound on \(\mathbb{E} \| P_n - P \|_\mathcal{F}\):

**Lemma 10.1 (Desymmetrization inequality).** For any class \(\mathcal{F}\) of measurable functions \(f : Z \to [0, 1]\), we have

\[
\frac{1}{2} \mathbb{E} R_n(\mathcal{F}(Z^n)) - \frac{1}{2\sqrt{n}} \leq \mathbb{E} \left[ \sup_{f \in \mathcal{F}} \left| \sum_{i=1}^{n} \sigma_i [f(Z_i) - P(f)] \right| \right] \leq \mathbb{E} \| P_n - P \|_\mathcal{F}.
\]

**Proof.** We will first prove the second inequality in (10.8). To that end, for each \(1 \leq i \leq n\) and each \(f \in \mathcal{F}\), let us define \(U_i(f) := f(Z_i) - P(f)\). Then \(\mathbb{E} U_i(f) = 0\). Let \(Z_1, \ldots, Z_n\) be an independent copy of \(Z_1, \ldots, Z_n\). Then we can define \(\overline{U}_i(f), 1 \leq i \leq n\), similarly.
Moreover, since $E U_i(f) = 0$, we can write

$$
E \left[ \sup_{f \in \mathcal{F}} \left| \sum_{i=1}^{n} \sigma_i [f(Z_i) - P(f)] \right| \right] = E \left[ \sup_{f \in \mathcal{F}} \left| \sum_{i=1}^{n} \sigma_i U_i(f) \right| \right]
$$

$$
= E \left[ \sup_{f \in \mathcal{F}} \left| \sum_{i=1}^{n} \sigma_i [U_i(f) - E U_i(f)] \right| \right]
$$

$$
\leq E \left[ \sup_{f \in \mathcal{F}} \left| \sum_{i=1}^{n} \sigma_i [U_i(f) - U_i(f)] \right| \right].
$$

Since, for each $i$, $U_i(f)$ and $\overline{U}_i(f)$ are i.i.d., the difference $U_i(f) - \overline{U}_i(f)$ is a symmetric random variable. Therefore,

$$
\{ \sigma_i [U_i(f) - U_i(f)] : 1 \leq i \leq n \} \overset{(d)}{=} \{ U_i(f) - \overline{U}_i(f) : 1 \leq i \leq n \}.
$$

Using this fact and the triangle inequality, we get

$$
E \left[ \sup_{f \in \mathcal{F}} \left| \sum_{i=1}^{n} \sigma_i [U_i(f) - \overline{U}_i(f)] \right| \right] = E \left[ \sup_{f \in \mathcal{F}} \left| \sum_{i=1}^{n} \sigma_i U_i(f) \right| \right]
$$

$$
\leq 2E \left[ \sup_{f \in \mathcal{F}} \left| \sum_{i=1}^{n} U_i(f) \right| \right]
$$

$$
= 2E \left[ \sup_{f \in \mathcal{F}} \sum_{i=1}^{n} |f(Z_i) - P(f)| \right]
$$

$$
= 2n \cdot E \|P_n - P\|_{\mathcal{F}}.
$$

To prove the first inequality in (10.8), we write

$$
ER_n(\mathcal{F}(Z^n)) = \frac{1}{n} E \left[ \sup_{f \in \mathcal{F}} \left| \sum_{i=1}^{n} \sigma_i [f(Z_i) - P(f) + P(f)] \right| \right]
$$

$$
\leq \frac{1}{n} E \left[ \sup_{f \in \mathcal{F}} \left| \sum_{i=1}^{n} \sigma_i [f(Z_i) - P(f)] \right| \right] + \frac{1}{n} E \left[ \sup_{f \in \mathcal{F}} P(f) \cdot \left| \sum_{i=1}^{n} \sigma_i \right| \right]
$$

$$
= \frac{1}{n} E \left[ \sup_{f \in \mathcal{F}} \left| \sum_{i=1}^{n} \sigma_i [f(Z_i) - P(f)] \right| \right] + \frac{1}{n} E \left| \sum_{i=1}^{n} \sigma_i \right|
$$

$$
\leq \frac{1}{n} E \left[ \sup_{f \in \mathcal{F}} \left| \sum_{i=1}^{n} \sigma_i [f(Z_i) - P(f)] \right| \right] + \frac{1}{\sqrt{n}}.
$$

Rearranging, we get the desired inequality. \(\square\)

In this section, we will see that we can get a lot of mileage out of the stochastic version of the Rademacher average. To that end, let us define

$$
r_n(\mathcal{F}(Z^n)) := \frac{1}{n} \sup_{f \in \mathcal{F}} \left| \sum_{i=1}^{n} \sigma_i f(Z_i) \right|.
$$

(10.9)
The key difference between (10.4) and (10.9) is that, in the latter, we do not take the expectation over the Rademacher sequence $\sigma^n$. In other words, both $R_n(\mathcal{F}(Z^n))$ and $r_n(\mathcal{F}(Z^n))$ are random variables, but the former depends only on the training data $Z^n$, while the latter also depends on the $n$ Rademacher random variables $\sigma_1, \ldots, \sigma_n$. We see immediately that $R_n(\mathcal{F}(Z^n)) = \mathbb{E}[r_n(\mathcal{F}(Z^n))|Z^n]$ and $\mathbb{E}R_n(\mathcal{F}(Z^n)) = \mathbb{E}r_n(\mathcal{F}(Z^n))$, where the expectation on the right-hand side is over both $Z^n$ and $\sigma^n$. The following result will be useful:

**Lemma 10.2** (Concentration inequalities for Rademacher averages). For any $\varepsilon > 0$,

\[
P\{r_n(\mathcal{F}(Z^n)) \geq \mathbb{E}r_n(\mathcal{F}(Z^n)) + \varepsilon\} \leq e^{-n\varepsilon^2/2}
\]

and

\[
P\{r_n(\mathcal{F}(Z^n)) \leq \mathbb{E}r_n(\mathcal{F}(Z^n)) - \varepsilon\} \leq e^{-n\varepsilon^2/2}.
\]

**Proof.** For each $1 \leq i \leq n$, let $U_i := (Z_i, \sigma_i)$. Then $r_n(\mathcal{F}(Z^n))$ can be represented as a real-valued function $g(U^n)$. Moreover, it is easy to see that this function has bounded differences with $c_1 = \ldots = c_n = 2/n$. Hence, McDiarmid’s inequality tells us that for any $\varepsilon > 0$

\[
P\{g(U^n) \geq \mathbb{E}g(U^n) + \varepsilon\} \leq e^{-n\varepsilon^2/2},
\]

and the same holds for the probability that $g(U^n) \leq \mathbb{E}g(U^n) - \varepsilon$. This completes the proof. \qed

### 3. Sequential learning algorithms

In a sequential learning algorithm, the sample complexity is a random variable. It is not known in advance, but rather is computed from data in the process of learning. In other words, instead of using a training sequence of fixed length, we keep drawing independent samples until we decide that we have acquired enough of them, and then compute an empirical risk minimizer.

To formalize this idea, we need the notion of a stopping time. Let $\{U_n\}_{n=1}^\infty$ be a random process. A random variable $\tau$ taking values in $\mathbb{N}$ is called a stopping time if and only if, for each $n \geq 1$, the occurrence of the event $\{\tau = n\}$ is determined by $U^n = (U_1, \ldots, U_n)$. More precisely:

**Definition 10.2.** For each $n$, let $\Sigma_n$ denote the $\sigma$-algebra generated by $U^n$ (in other words, $\Sigma_n$ consists of all events that occur by time $n$). Then a random variable $\tau$ taking values in $\mathbb{N}$ is a stopping time if and only if, for each $n \geq 1$, the event $\{\tau = n\} \in \Sigma_n$.

In other words, denoting by $U^\infty$ the entire sample path $(U_1, U_2, \ldots)$ of our random process, we can view $\tau$ as a function that maps $U^\infty$ into $\mathbb{N}$. For each $n$, the indicator function of the event $\{\tau = n\}$ is a function of $U^\infty$:

\[
1_{\{\tau = n\}} \equiv 1_{\{\tau(U^\infty) = n\}}.
\]

Then $\tau$ is a stopping time if and only if, for each $n$ and for all $U^\infty, V^\infty$ with $U^n = V^n$ we have

\[
1_{\{\tau(U^\infty) = n\}} = 1_{\{\tau(V^\infty) = n\}}.
\]

Our sequential learning algorithms will work as follows. Given a desired accuracy parameter $\varepsilon > 0$ and a confidence parameter $\delta > 0$, let $\pi(\varepsilon, \delta)$ be the initial sample size; we
will assume that \( \pi(\varepsilon, \delta) \) is a nonincreasing function of both \( \varepsilon \) and \( \delta \). Let \( \mathcal{T}(\varepsilon, \delta) \) denote the set of all stopping times \( \tau \) such that

\[
\sup_{P \in \mathcal{P}} \left\{ \| P_{\tau} - P \|_{\mathcal{F}} \leq \varepsilon \right\} \geq \delta.
\]

Now if \( \tau \in \mathcal{T}(\varepsilon, \delta) \) and we let

\[
\hat{f}_{\tau} := \arg\min_{f \in \mathcal{F}} P_{\tau}(f) \equiv \arg\min_{f \in \mathcal{F}} \frac{1}{\tau} \sum_{i=1}^{\tau} f(Z_i),
\]

then we immediately see that

\[
\sup_{P \in \mathcal{P}} \left\{ P(\hat{f}) \geq \inf_{f \in \mathcal{F}} P(f) + 2\varepsilon \right\} \leq \delta.
\]

Of course, the whole question is how to construct an appropriate stopping time without knowing \( P \).

**Definition 10.3.** A parametric family of stopping times \( \{\nu(\varepsilon, \delta) : \varepsilon > 0, \delta \in (0,1)\} \) is called strongly efficient (SE) (w.r.t. \( \mathcal{F} \) and \( \mathcal{P} \)) if there exist constants \( K_1, K_2, K_3 \geq 1 \), such that for all \( \varepsilon > 0, \delta \in (0,1) \)

\[
(10.12) \quad \nu(\varepsilon, \delta) \in \mathcal{T}(K_1\varepsilon, \delta)
\]

and for all \( \tau \in \mathcal{T}(\varepsilon, \delta) \)

\[
(10.13) \quad \sup_{P \in \mathcal{P}} \left\{ \nu( K_2 \varepsilon, \delta) > \tau \right\} \leq K_3 \delta.
\]

In other words, Eq. (10.12) says that any SE stopping time \( \{\nu(\varepsilon, \delta)\} \) guarantees that we can approximate statistical expectations by empirical expectations with accuracy \( K_1\varepsilon \) and confidence \( 1 - \delta \); similarly, Eq. (10.13) says that, with probability at least \( 1 - K_3 \delta \), we will require at most as many samples as would be needed by any sequential algorithm for empirical approximation with accuracy \( \varepsilon/K_2 \) and confidence \( 1 - \delta \).

**Definition 10.4.** A family of stopping times \( \{\nu(\varepsilon, \delta) : \varepsilon > 0, \delta \in (0,1)\} \) is weakly efficient (WE) for \( (\mathcal{F}, \mathcal{P}) \) if there exist constants \( K_1, K_2, K_3 \geq 1 \), such that for all \( \varepsilon > 0, \delta \in (0,1) \)

\[
(10.14) \quad \nu(\varepsilon, \delta) \in \mathcal{T}(K_1\varepsilon, \delta)
\]

and

\[
(10.15) \quad \sup_{P \in \mathcal{P}} \left\{ \nu( K_2 \varepsilon, \delta) > N(\varepsilon; \delta) \right\} \leq K_3 \delta.
\]

If \( \nu(\varepsilon, \delta) \) is a WE stopping time, then Eq. (10.14) says that we can solve the empirical approximation problem with accuracy \( K_1\varepsilon \) and confidence \( 1 - \delta \); Eq. (10.15) says that, with probability at most \( 1 - \delta \), the sample complexity will be less than the sample complexity of empirical approximation with accuracy \( \varepsilon/K_2 \) and confidence \( 1 - \delta \).

If \( N(\varepsilon; \delta) \geq \pi(\varepsilon, \delta) \), then \( N(\varepsilon, \delta) \in \mathcal{T}(\varepsilon, \delta) \). Hence, any WE stopping time is also SE. The converse, however, is not true.
3.1. A strongly efficient sequential learning algorithm. Let \( \{Z_n\}_{n=1}^\infty \) be an infinite sequence of i.i.d. draws from some \( P \in \mathcal{P} \); let \( \{\sigma_n\}_{n=1}^\infty \) be an i.i.d. Rademacher sequence independent of \( \{Z_n\} \). Choose

\[
\pi(\varepsilon, \delta) \geq \left\lfloor \frac{2}{\varepsilon^2} \log \frac{2}{\delta(1 - e^{-\varepsilon^2/2})} \right\rfloor + 1
\]

and let

\[
\nu(\varepsilon, \delta) := \min \{n \geq \pi(\varepsilon, \delta) : r_n(\mathcal{F}(Z^n)) \leq \varepsilon\}.
\]

This is clearly a stopping time for each \( \varepsilon > 0 \) and each \( \delta \in (0, 1) \).

**Theorem 10.1.** The family \( \{\nu(\varepsilon, \delta) : \varepsilon > 0, \delta \in (0, 1)\} \) defined in (10.17) with \( \pi(\varepsilon, \delta) \) set according to (10.16) is SE for any class \( \mathcal{F} \) of measurable functions \( f : \mathbb{Z} \to [0, 1] \) and \( \mathcal{P} = \mathcal{P}(Z) \) with \( K_1 = 5, K_2 = 6, K_3 = 1 \).

**Proof.** Let \( \overline{\pi} = \pi(\varepsilon, \delta) \). We will first show that, for any \( P \in \mathcal{P}(Z) \),

\[
\|P_n - P\|_\mathcal{F} \leq 2r_n(\mathcal{F}(Z^n)) + 3\varepsilon, \quad \forall n \geq \pi
\]

with probability at least \( 1 - \delta \). Since for \( n = \nu(\varepsilon, \delta) \geq \overline{\pi} \) we have \( r_n(\mathcal{F}(Z^n)) \leq \varepsilon \), we will immediately be able to conclude that

\[
P \{\|P_{\nu(\varepsilon, \delta)} - P\|_\mathcal{F} \geq 5\varepsilon\} \leq \delta,
\]

which will imply that \( \nu(\varepsilon, \delta) \in T(5\varepsilon, \delta) \). Now we prove (10.18). First of all, applying Lemma 10.2 and the union bound, we can write

\[
P \left\{ \bigcup_{n \geq \overline{\pi}} \{r_n(\mathcal{F}(Z^n)) \geq ER_n(\mathcal{F}(Z^n)) + \varepsilon\} \right\} \leq \sum_{n \geq \overline{\pi}} e^{-\pi n^2/2} = e^{-\pi^2/2} \sum_{n \geq 0} e^{-n^2/2} = \frac{e^{-\pi^2/2}}{1 - e^{-\varepsilon^2/2}} \leq \delta/2.
\]

From the symmetrization inequality (10.5), we know that \( E\|P_n - P\|_\mathcal{F} \leq 2ER_n(\mathcal{F}(Z^n)) \). Moreover, using (10.6) and the union bound, we can write

\[
P \left\{ \bigcup_{n \geq \pi} \{\|P_n - P\|_\mathcal{F} \geq E\|P_n - P\|_\mathcal{F} + \varepsilon\} \right\} \leq \sum_{n \geq \pi} e^{-2n^2} = \sum_{n \geq \pi} e^{-n^2/2} \leq \delta/2.
\]

Therefore, with probability at least \( 1 - \delta \),

\[
\|P_n - P\|_\mathcal{F} \leq E\|P_n - P\|_\mathcal{F} + \varepsilon \leq 2ER_n(\mathcal{F}(Z^n)) + \varepsilon \leq 2r_n(\mathcal{F}(Z^n)) + 3\varepsilon, \quad \forall n \geq \pi
\]

which is (10.18). This shows that (10.12) holds for \( \nu(\varepsilon, \delta) \) with \( K_1 = 5 \).
Next, we will prove that, for any $P \in \mathcal{P}(\mathcal{Z})$,

$$\Pr \left\{ \min_{\pi \leq n < \nu(6\varepsilon, \delta)} \| P_n - P \|_F < \varepsilon \right\} \leq \delta. \quad (10.19)$$

In other words, $(10.19)$ says that, with probability at least $1 - \delta$, $\| P_n - P \|_F \geq \varepsilon$ for all $\pi \leq n < \nu(6\varepsilon, \delta)$. This means that, for any $\tau \in \mathcal{T}(\varepsilon, \delta)$, $\nu(6\varepsilon, \delta) \leq \tau$ with probability at least $1 - \delta$, which will give us $(10.13)$ with $K_2 = 6$ and $K_3 = 1$.

To prove $(10.19)$, we have by $(10.7)$ and the union bound that

$$\Pr \left\{ \bigcup_{n \geq \pi} \left\{ \| P_n - P \|_F \leq \mathbb{E} \| P_n - P \|_F - \varepsilon \right\} \right\} \leq \delta/2.$$ 

By the desymmetrization inequality $(10.8)$, we have

$$\mathbb{E} \| P_n - P \|_F \geq \frac{1}{2} \mathbb{E} R_n(\mathcal{F}(Z^n)) - \frac{1}{2\sqrt{n}}, \quad \forall n.$$ 

Finally, by the concentration inequality $(10.10)$ and the union bound,

$$\Pr \left\{ \bigcup_{n \geq \pi} \left\{ r_n(\mathcal{F}(Z^n)) \geq \mathbb{E} R_n(\mathcal{F}(Z^n)) + \varepsilon \right\} \right\} \leq \delta/2.$$ 

Therefore, with probability at least $1 - \delta$,

$$\| P_n - P \|_F \geq \frac{3\varepsilon}{2} - \frac{1}{2\sqrt{n}} \geq \frac{3\varepsilon}{2} - \frac{1}{2\sqrt{\pi}} \geq \varepsilon, \quad \forall n \geq \pi.$$ 

If $\pi \leq n < \nu(6\varepsilon, \delta)$, then $r_n(\mathcal{F}(Z^n)) > 6\varepsilon$. Therefore, using the fact that $n \geq \pi$ and $\pi(\varepsilon, \delta)^{-1/2} \leq \varepsilon$, we see that, with probability at least $1 - \delta$,

$$\| P_n - P \|_F > \frac{3\varepsilon}{2} - \frac{1}{2\sqrt{n}} \geq \frac{3\varepsilon}{2} - \frac{1}{2\sqrt{\pi}} \geq \varepsilon, \quad \pi \leq n < \nu(6\varepsilon, \delta).$$ 

This proves $(10.19)$, and we are done. \hfill \square

### 3.2. A weakly efficient sequential learning algorithm.

Now choose

$$\pi(\varepsilon, \delta) \geq \left\lceil \frac{2}{\varepsilon^2 \log \frac{4}{\delta}} \right\rceil + 1, \quad (10.20)$$

for each $k = 0, 1, 2, \ldots$ let $n_k := 2^k \pi(\varepsilon, \delta)$, and let

$$\nu(\varepsilon, \delta) := \min \left\{ n_k : r_n(\mathcal{F}(Z^{n_k})) \leq \varepsilon \right\}. \quad (10.21)$$

**Theorem 10.2.** The family $\{ \nu(\varepsilon, \delta) : \varepsilon > 0, \delta \in (0, 1/2) \}$ defined in $(10.21)$ with $\pi(\varepsilon, \delta)$ set according to $(10.20)$ is WE for any class $\mathcal{F}$ of measurable functions $f : \mathcal{Z} \to [0, 1]$ and $\mathcal{P} = \mathcal{P}(\mathcal{Z})$ with $K_1 = 5$, $K_2 = 18$, $K_3 = 3$. 

122
Proof. As before, let \( \pi = \pi(\varepsilon, \delta) \). The proof of (10.14) is similar to what we have done in the proof of Theorem 10.1, except we use the bounds

\[
P \left\{ \bigcup_{k=0}^{\infty} \{ r_{n_k} (\mathcal{F}(Z^{n_k})) \geq E R_{n_k} (\mathcal{F}(Z^{n_k})) + \varepsilon \} \right\} \leq \sum_{k=0}^{\infty} e^{-2k\pi \varepsilon^2 / 2} \]

\[
= e^{-\pi \varepsilon^2 / 2} + e^{-\pi \varepsilon^2 / 2} \sum_{k=1}^{\infty} e^{-\pi \varepsilon^2 / 2 (2^k - 1)} \]

\[
\leq e^{-\pi \varepsilon^2 / 2} + e^{-\pi \varepsilon^2 / 2} \sum_{k=1}^{\infty} e^{-(2^k - 1)} \]

\[
\leq e^{-\pi \varepsilon^2 / 2} + e^{-\pi \varepsilon^2 / 2} \sum_{k=1}^{\infty} e^{-k} \]

\[
\leq 2e^{-\pi \varepsilon^2 / 2} \]

\[
\leq \delta / 2,
\]

where in the third step we have used the fact that \( \pi \varepsilon^2 / 2 \geq 1 \). Similarly,

\[
P \left\{ \bigcup_{k=0}^{\infty} \{ \| P_{n_k} - P \|_F \leq E \| P_{n_k} - P \|_F + \varepsilon \} \right\} \leq \delta^2.
\]

Therefore,

\[
\| P_{n_k} - P \|_F \leq 2r_{n_k} (\mathcal{F}(Z^{n_k})) + 3\varepsilon, \quad \forall k = 0, 1, 2, \ldots
\]

and consequently

\[
P \left\{ \| P_{\nu(\varepsilon, \delta)}^\varepsilon - P \|_F \geq 5\varepsilon \} \leq \delta,
\]

which proves (10.14).

Now we prove (10.15). Let \( N = N(\varepsilon, \delta) \), the sample complexity of empirical approximation that we have defined in (10.3). Let us choose \( k \) so that \( n_k \leq N < n_{k+1} \), which is equivalent to \( 2^k \pi \leq N < 2^{k+1} \). Then

\[
P \{ \nu(18\varepsilon, \delta) > N \} \leq P \{ \nu(18\varepsilon, \delta) > n_k \}.
\]

We will show that the probability on the right-hand side is less than \( 3\delta \). First of all, since \( N \geq \pi \) (by hypothesis), we have \( n_k \geq \pi / 2 \geq 1 / \varepsilon^2 \). Therefore, with probability at least \( 1 - \delta \)

\[
\| P_{n_k} - P \|_F \geq \frac{1}{2} r_{n_k} (\mathcal{F}(Z^{n_k})) - \frac{1}{2 \sqrt{n_k}} - \frac{9\varepsilon}{2} \geq \frac{1}{2} r_{n_k} (\mathcal{F}(Z^{n_k})) - 5\varepsilon.
\]

If \( \nu(18\varepsilon, \delta) > n_k \), then by definition \( r_{n_k} (\mathcal{F}(Z^{n_k})) > 18\varepsilon \). Writing \( r_{n_k} = r_{n_k} (\mathcal{F}(Z^{n_k})) \) for brevity, we see get

\[
P \{ \nu(18\varepsilon, \delta) > n_k \} \leq P \{ r_{n_k} > 18\varepsilon \}
\]

\[
= P \{ r_{n_k} > 18\varepsilon, \| P_{n_k} - P \|_F \geq 18\varepsilon \} + P \{ r_{n_k} > 18\varepsilon, \| P_{n_k} - P \|_F < 4\varepsilon \}
\]

\[
\leq P \{ \| P_{n_k} - P \|_F \geq 4\varepsilon \} + P \{ r_{n_k} > 18\varepsilon, \| P_{n_k} - P \|_F < 4\varepsilon \}.
\]

123
If \( r_{n_k} > 18\epsilon \) but \( \|P_{n_k} - P\|_\mathcal{F} < 4\epsilon \), the event in (10.22) cannot occur. Indeed, suppose it does. Then it must be the case that \( 4\epsilon > 9\epsilon - 5\epsilon = 4\epsilon \), which is a contradiction. Therefore, 
\[
P\{r_{n_k} > 18\epsilon, \|P_{n_k} - P\|_\mathcal{F} < 4\epsilon\} \leq \delta,
\]
and hence 
\[
P\{\nu(18\epsilon, \delta) > n_k\} \leq P\{\|P_{n_k} - P\|_\mathcal{F} \geq 4\epsilon\} + \delta.
\]
For each \( f \in \mathcal{F} \) and each \( n \in \mathbb{N} \) define 
\[
S_n(f) := \sum_{i=1}^{n} [f(Z_i) - P(f)]
\]
and let \( \|S_n\|_\mathcal{F} := \sup_{f \in \mathcal{F}} |S_n(f)| \). Then 
\[
P\{\|P_{n_k} - P\|_\mathcal{F} \geq 2\epsilon N\} \leq \frac{P\{\|S_{n_k}\|_\mathcal{F} \geq \epsilon N\}}{\inf_{f \in \mathcal{F}} P\{|S_N(f) - S_{n_k}(f)| \leq \epsilon N\}}.
\]
By definition of \( N = N(\epsilon, \delta) \), the probability in the numerator is at most \( \delta \). To analyze the probability in the denominator, we use Hoeffding’s inequality to get 
\[
\inf_{f \in \mathcal{F}} P\{|S_N(f) - S_{n_k}(f)| \leq \epsilon N\} = 1 - \sup_{f \in \mathcal{F}} P\{|S_N(f) - S_{n_k}(f)| > \epsilon N\}
\]
\[
\geq 1 - 2e^{-N\epsilon^2/2}
\]
\[
\geq 1 - \delta.
\]
Therefore, 
\[
P\{\nu(18\epsilon, \delta) > n_k\} \leq \frac{\delta}{1 - \delta} + \delta \leq 3\delta
\]
for \( \delta < 1/2 \). Therefore, \( \{\nu(\epsilon, \delta) : \epsilon \in (0, 1), \delta \in (0, 1/2)\} \) is WE with \( K_1 = 5, K_2 = 18, K_3 = 3 \) \( \square \)

4. A sequential algorithm for stochastic simulation

Armed with these results on sequential learning algorithms, we can take up the question of constructing efficient simulation strategies. We fix an accuracy parameter \( \epsilon > 0 \), a confidence parameter \( \delta \in (0, 1) \), and a level parameter \( \alpha \in (0, 1) \). Given two probability distributions, \( P \) on the input space \( Z \) and \( Q \) on the parameter space \( \Theta \), we draw a large i.i.d. sample \( Z_1, \ldots, Z_n \) from \( P \) and a large i.i.d. sample \( \theta_1, \ldots, \theta_m \) from \( Q \). We then compute 
\[
\hat{\theta} = \arg\min_{\theta \in \Theta} L_n(\theta),
\]
where 
\[
L_n(\theta) := \frac{1}{n} \sum_{i=1}^{n} \ell(Z_i, \theta).
\]
The goal is to pick $n$ and $m$ large enough so that, with probability at least $1 - \delta$, $\hat{\theta}$ is an $\varepsilon$-minimizer of $L$ to level $\alpha$, i.e., with probability at least $1 - \delta$ there exists some set $\Lambda \subset \Theta$ with $Q(\Lambda) \leq \alpha$, such that Eq. (10.2) holds with probability at least $1 - \delta$.

To that end, consider the following algorithm based on Theorem 10.2, proposed by Koltchinskii et al. [KAA+00a, KAA+00b]:

<table>
<thead>
<tr>
<th>Algorithm 1</th>
</tr>
</thead>
<tbody>
<tr>
<td>choose positive integers $m$ and $n$ such that $m \geq \frac{\log(2/\delta)}{\log[1/(1-\alpha)]}$ and $n \geq \lceil 50 \varepsilon^2 \log 8 \delta \rceil + 1$</td>
</tr>
<tr>
<td>draw $m$ independent samples $\theta_1, \ldots, \theta_m$ from $Q$</td>
</tr>
<tr>
<td>draw $n$ independent samples $Z_1, \ldots, Z_n$ from $P_Z$</td>
</tr>
<tr>
<td>evaluate the stopping variable $\gamma = \max_{1 \leq j \leq m} \left{ \frac{1}{n} \sum_{i=1}^{n} \sigma_i \ell(Z_i, \theta_j) \right}$</td>
</tr>
<tr>
<td>where $\sigma_1, \ldots, \sigma_n$ are i.i.d. Rademacher r.v.’s independent of $\theta^m$ and $Z^n$</td>
</tr>
<tr>
<td>if $\gamma &gt; \varepsilon/5$, then</td>
</tr>
<tr>
<td>add $n$ more i.i.d. samples from $P_Z$ and repeat</td>
</tr>
<tr>
<td>else stop and output</td>
</tr>
<tr>
<td>$\hat{\theta} = \arg\min_{\theta \in {\theta_1, \ldots, \theta_n}} L_n(\theta)$</td>
</tr>
</tbody>
</table>

Then we claim that, with probability at least $1 - \delta$, $\hat{\theta}$ is an $\varepsilon$-minimizer of $L$ to level $\alpha$. To see this, we need the following result [Vid03, Lemma 11.1]:

**Lemma 10.3.** Let $Q$ be a probability distribution on the parameter set $\Theta$, and let $h : \Theta \to \mathbb{R}$ be a (measurable) real-valued function on $\Theta$, bounded from above, i.e., $h(\theta) < +\infty$ for all $\theta \in \Theta$. Let $\theta_1, \ldots, \theta_m$ be $m$ i.i.d. samples from $Q$, and let $\bar{h}(\theta^m) := \max_{1 \leq j \leq m} h(\theta_m)$.

Then for any $\alpha \in (0, 1)$

$$(10.23) \quad Q \left( \left\{ \theta \in \Theta : h(\theta) > \bar{h}(\theta^m) \right\} \right) \leq \alpha$$

with probability at least $1 - (1 - \alpha)^m$.

**Proof.** For each $c \in \mathbb{R}$, let $$F(c) := P \left( \{ \theta \in \Theta : h(\theta) \leq c \} \right).$$

Note that $F$ is the CDF of the random variable $\xi = h(\theta)$ with $\theta \sim Q$. Therefore, it is right-continuous, i.e., $\lim_{c' \searrow c} F(c') = F(c)$. Now define $$c_\alpha := \inf \{ c : F(c) \geq 1 - \alpha \}.$$ Since $F$ is right-continuous, $F(c_\alpha) \geq 1 - \alpha$. Moreover, if $c < c_\alpha$, then $F(c) < 1 - \alpha$. Now let us suppose that $\bar{h}(\theta^m) \geq c_\alpha$. Then, since $F$ is monotone nondecreasing, $$P \left( \{ \theta \in \Theta : h(\theta) \leq \bar{h}(\theta^m) \} \right) = F(\bar{h}(\theta^m)) \geq F(c_\alpha) \geq 1 - \alpha,$$ or, equivalently, if $\bar{h}(\theta^m) \geq c_\alpha$, then $$P \left( \{ \theta \in \Theta : h(\theta) > \bar{h}(\theta^m) \} \right) \leq \alpha.$$
Therefore, if $\theta^m$ is such that
\[ P \left( \{ \theta \in \Theta : h(\theta) > \bar{h}(\theta^m) \} \right) > \alpha, \]
then it must be the case that $\bar{h}(\theta^m) < c_\alpha$, which in turn implies that $F(\bar{h}(\theta^m)) < 1 - \alpha$, the complement of the event in (10.23). But $\bar{h}(\theta^m) < c_\alpha$ means that $h(\theta_j) < c_\alpha$ for every $1 \leq j \leq m$. Since the $\theta_j$’s are independent, the events $\{ h(\theta_j) < c_\alpha \}$ are independent, and each occurs with probability at most $1 - \alpha$. Therefore,
\[ P \left( \{ \theta^m \in \Theta^m : Q \left( \{ \theta \in \Theta : h(\theta) > \bar{h}(\theta^m) \} \right) \right) \leq (1 - \alpha)^m, \]
which is what we intended to prove. □

We apply this lemma to the function $h(\theta) = -L(\theta)$. Then, provided $m$ is chosen as described in Algorithm 1, we will have
\[ Q \left( \left\{ \theta \in \Theta : L(\theta) < \min_{1 \leq j \leq m} L(\theta_j) \right\} \right) \leq \delta/2. \]

Now consider the finite class of functions $F = \{ f_j(z) = \ell(z, \theta_j) : 1 \leq j \leq m \}$. By Theorem 10.2, the final output $\hat{\theta} \in \{ \theta_1, \ldots, \theta_m \}$ will satisfy
\[ \left| L(\hat{\theta}) - \min_{1 \leq j \leq m} L(\theta_j) \right| \leq \varepsilon \]
with probability at least $1 - \delta/2$. Hence, with probability at least $1 - \delta$ there exists a set $\Lambda \subset \Theta$ with $Q(\Lambda) \leq \alpha$, such that (10.2) holds. Moreover, the total number of samples used up by Algorithm 1 will be, with probability at least $1 - 3\delta/2$, no more than
\[ N_F, P_Z(\varepsilon/18, \delta/2) \equiv \min \{ n \in \mathbb{N} : P(\| P_n - P_Z \|_F > \varepsilon/18) < \delta/2 \}. \]

We can estimate $N_F, P_Z(\varepsilon/18, \delta/2)$ as follows. First of all, the function
\[ \Delta(Z^n) := \| P_n - P_Z \|_F \equiv \max_{1 \leq j \leq m} | P_n(f_j) - P_Z(f_j) | \]
has bounded differences with $c_1 = \ldots = c_n = 1/n$. Therefore, by McDiarmid’s inequality
\[ P(\Delta(Z^n) \geq \varepsilon) \leq \mathbb{E}(\Delta(Z^n) + t) \leq e^{-2nt^2}, \quad \forall t > 0. \]

Secondly, since the class $F$ is finite with $|F| = m$, the symmetrization inequality (10.5) and the Finite Class Lemma give the bound
\[ \mathbb{E}(\| P_n - P_Z \|_F) \leq 4\sqrt{\frac{\log m}{n}}. \]

Therefore, if we choose $t = \varepsilon/18 - 4\sqrt{n^{-1}\log m}$ and $n$ is large enough so that $t > \varepsilon/20$ (say), then
\[ P(\| P_n - P \|_F > \varepsilon/18) \leq e^{-n\varepsilon^2/200}. \]

Hence, a fairly conservative estimate is
\[ N_F, P_Z(\varepsilon/18, \delta/2) \leq \max \left\{ \left\lfloor \frac{200}{\varepsilon^2} \log \frac{2}{\delta} \right\rfloor + 1, \left\lfloor \left( \frac{720}{\varepsilon} \right)^2 \log m \right\rfloor + 1 \right\} \]

It is instructive to compare Algorithm 1 with a simple Monte Carlo strategy:
Algorithm 0

choose positive integers \( m \) and \( n \) such that
\[
m \geq \frac{\log(2/\delta)}{\log(1/(1-\alpha))} \quad \text{and} \quad n \geq \frac{1}{2\epsilon^2} \log \frac{4m}{\delta},
\]
draw \( m \) independent samples \( \theta_1, \ldots, \theta_m \) from \( Q \)
draw \( n \) independent samples \( Z_1, \ldots, Z_n \) from \( P_Z \)
for \( j = 1 \) to \( m \)
compute \( L_n(\theta_j) = \frac{1}{n} \sum_{i=1}^{n} \ell(Z_i, \theta_j) \)
end for
output \( \hat{\theta} = \arg \min_{\theta \in \{\theta_1, \ldots, \theta_m\}} L_n(\theta_j) \)

The selection of \( m \) is guided by the same considerations as in Algorithm 1. Moreover, for each \( 1 \leq j \leq m \), \( L_n(\theta_j) \) is an average of \( n \) independent random variables \( \ell(Z_i, \theta_j) \in [0, 1] \), and \( L(\theta_j) = \mathbb{E}L_n(\theta_j) \). Hence, Hoeffding’s inequality says that
\[
P(\{Z^n \in Z^n : |L_n(\theta_j) - L(\theta_j)| > \epsilon\}) \leq 2e^{-2n\epsilon^2}.
\]

If we choose \( n \) as described in Algorithm 0, then
\[
P \left( \left| L_n(\hat{\theta}) - \min_{1 \leq j \leq m} L(\theta_j) \right| > \epsilon \right) \leq \sum_{j=1}^{m} P(\{|L_n(\theta_j) - L(\theta_j)| > \epsilon\})
\]
\[
\leq \frac{m}{\delta} / 2
\]

Hence, with probability at least \( 1 - \delta \) there exists a set \( \Lambda \subset \Theta \) with \( Q(\Lambda) \leq \alpha \), so that (10.2) holds. It may seem at first glance that Algorithm 0 is more efficient than Algorithm 1. However, this is not the case in high-dimensional situations. There, one can actually show that, with probability practically equal to one, the empirical minimum of \( L \) can be much larger than the true minimum (cf. [KAA+00b] for a very vivid numerical illustration). This is an instance of the so-called Curse of Dimensionality, which adaptive schemes like Algorithm 1 can often avoid.

5. Technical lemma

**Lemma 10.4.** Let \( \{\xi_1(f) : f \in F\} \) and \( \{\xi_2(f) : f \in F\} \) be two independent \( F \)-indexed stochastic processes with
\[
\|\xi_j\|_F := \sup_{f \in F} |\xi_j(f)| < \infty, \quad j = 1, 2.
\]
Then for all \( t > 0, c > 0 \)
\[
(10.24) \quad P\left\{ \|\xi_1\|_F \geq t + c \right\} \leq \frac{P\{\|\xi_1 - \xi_2\|_F \geq t\}}{\inf_{f \in F} P\{|\xi_2(f)| \leq c\}}.
\]

**Proof.** If \( \|\xi_1\|_F \geq t + c \), then there exists some \( f \in F \), such that \( |\xi_1(f)| \geq t + c \). Then for this particular \( f \) by the triangle inequality we see that
\[
|\xi_1(f)| \leq c \quad \Rightarrow \quad |\xi_1(f) - \xi_2(f)| \geq t
\]
Therefore,

\[
\inf_{f \in \mathcal{F}} P_{\xi_2}\left\{ \left| \xi_2(f) \right| \leq c \right\} \leq P_{\xi_2}\left\{ \left| \xi_2(f) \right| \leq c \right\} \leq P_{\xi_2}\left\{ \left| \xi_1(f) - \xi_2(f) \right| \geq t \right\} \leq P_{\xi_2}\left\{ \| \xi_1 - \xi_2 \|_{\mathcal{F}} \geq t \right\}.
\]

The leftmost and the rightmost terms in the above inequality do not depend on the particular \( f \), and the inequality between them is valid on the event \( \{ \| \xi_1 \|_{\mathcal{F}} \geq t + c \} \). Therefore, integrating the two sides w.r.t. \( \xi_1 \) on this event, we get

\[
\inf_{f \in \mathcal{F}} P_{\xi_2}\left\{ \left| \xi_2(f) \right| \leq c \right\} \cdot P_{\xi_1}\left\{ \| \xi_1 \|_{\mathcal{F}} \geq t + c \right\} \leq P_{\xi_1, \xi_2}\left\{ \| \xi_1 - \xi_2 \|_{\mathcal{F}} \geq t \right\}.
\]

Rearranging, we get (10.24). \( \square \)
Part 4

Advanced Topics
CHAPTER 11

Stability of learning algorithms

Recall our abstract formulation of the learning problem: we have a collection $Z_1, \ldots, Z_n$ of i.i.d. samples from some unknown distribution $P$ on a set $Z$ and a class $\mathcal{F}$ of functions $f : Z \rightarrow [0, 1]$. A learning algorithm is a sequence $A = \{A_n\}_{n=1}^{\infty}$ of mappings $A_n : Z^n \rightarrow \mathcal{F}$ that take training data as input and generate functions in $\mathcal{F}$ as output. We say that $A$ is consistent if

$$L(\hat{f}_n) = \int_Z \hat{f}_n(z)P(dz), \quad \hat{f}_n = A_n(Z^n)$$

converges in some sense to $L^* = \inf_{f \in \mathcal{F}} L(f)$, for any $P$. If a consistent algorithm exists, we say that the problem is learnable. Early on, we have identified one sufficient condition for the existence of a consistent learning algorithm: uniform convergence of empirical means (UCEM). One way of stating the UCEM property is to require that

$$\sup_P \mathbb{E}_P \|P_n - P\|_F \xrightarrow{n \rightarrow \infty} 0,$$

where the expectation is with respect to an i.i.d. process $Z_1, Z_2, \ldots$ with common marginal distribution $P$, and $P_n$ is the empirical distribution based on the first $n$ samples of the process:

$$P_n = \frac{1}{n} \sum_{i=1}^{n} \delta_{Z_i}.$$

We have proved that, if $\mathcal{F}$ satisfies (11.1), then the ERM algorithm

$$\hat{f}_n = \arg\min_{f \in \mathcal{F}} \frac{1}{n} \sum_{i=1}^{n} f(Z_i)$$

is consistent. In some cases, the UCEM property is both necessary and sufficient for learnability — for example, in the binary classification setting, where $Z = (X,Y)$ with arbitrary $X, Y \in \{0, 1\}$, and $f(Z) = f(X,Y)$ taking values in $\{0, 1\}$.

However, it is easy to see that, in general, one can have learnability without the UCEM property. For example, suppose that the function class $\mathcal{F}$ is such that one can find a function $\tilde{f} \not\in \mathcal{F}$ with the property that $\tilde{f}(z) < \inf_{f \in \mathcal{F}} f(z)$ for every $z \in Z$. Consider now a modified class $\tilde{\mathcal{F}} = \mathcal{F} \cup \{\tilde{f}\}$ obtained by adding $\tilde{f}$ to $\mathcal{F}$. Then the ERM algorithm over $\tilde{\mathcal{F}}$ will always return $\tilde{f}$, and moreover $L(\tilde{f}) \equiv L^*(\tilde{\mathcal{F}})$. Thus, not only do we have consistency, but we also have perfect generalization, and the only condition the original class $\mathcal{F}$ has to satisfy is that we can find at least one $\tilde{f}$ with the desired property. Of course, this imposes some minimal richness requirements on the ranges of all functions in $\mathcal{F}$ — for example, we could not pull this off when the functions in $\mathcal{F}$ are binary valued. And yet, the UCEM property is not required for perfect learnability!
So, what’s going on here? It turns out that the main attraction of the UCEM property – namely, its algorithm-independence – is also its main disadvantage. Learnability is closely tied up with properties of learning algorithms: how well can they generalize? how good are they at rejecting obviously bad hypotheses and focusing on good ones? Thus, our goal is to connect learnability to certain properties of learning algorithms. This lecture is based primarily on a paper by Shalev-Shwartz et al. [SSSS10].

1. An in-depth view of learning algorithms

For future convenience, let us slightly modify our notation pertaining to the learning problem. As before, we will have the data space $Z$ and a function class $\mathcal{F}$. However, now we do not require the functions in $\mathcal{F}$ to be real-valued — they will be elements of some Hilbert space. Instead, we introduce a loss function $\ell : \mathcal{F} \times Z \to [0, 1]$. We will still use the notation $L_P(f) = \mathbb{E}_P[\ell(f, Z)] \equiv \int_Z \ell(f, z) P(dz)$ for the expected loss of $f$ with respect to $P$, and will often omit the subscript $P$ when it’s clear from context. Also, given an $n$-tuple $Z^n = (Z_1, \ldots, Z_n)$ of i.i.d. samples from $P$, we have the empirical loss

$$L_n(f) = \frac{1}{n} \sum_{i=1}^n \ell(f, Z_i).$$

Finally, we define

$$L^*(\mathcal{F}) := \inf_{f \in \mathcal{F}} L(f) \quad \text{and} \quad L^*_n(\mathcal{F}) := \inf_{f \in \mathcal{F}} L_n(f).$$

Here, $L^*(\mathcal{F})$ is a deterministic quantity that depends on $\ell$, $\mathcal{F}$, and the underlying distribution $P$, whereas $L^*_n(\mathcal{F})$ is a random variable.

Also, let us define $Z^* := \bigcup_{n=1}^{\infty} Z^n$, i.e., $Z^*$ is the collection of all tuples over $Z$. This definition allows us to treat a learning algorithm as a single mapping $A : Z^* \to \mathcal{F}$ — the size of the training set is now clear from context. For example, $A(Z^n)$ is the output of $A$ fed with an $n$-tuple $Z^n = (Z_1, \ldots, Z_n)$, and so, in particular,

$$L(A(Z^n)) = \int_Z \ell(A(Z^n), z) P(dz)$$

is the expected loss of the function $A(Z^n) \in \mathcal{F}$ on a fresh sample $Z \sim P$, independent of $Z^n$. This new notation is rather flexible: for example,

$$L_n(A(Z^n)) = \frac{1}{n} \sum_{i=1}^n \ell(A(Z^n), Z_i)$$

is the empirical loss of the algorithm output $A(Z^n)$ on the same sample $Z^n$ that was supplied to $A$.

Our goal is to understand what makes a good learning algorithm. To keep things simple, we will focus on expected-value guarantees. We say that a learning algorithm $A$ is consistent if

$$c_n(A) := \sup_P \mathbb{E}_P \left[ L(A(Z^n)) - L^* \right] \xrightarrow{n \to \infty} 0.$$
We say that the learning problem specified by \( \ell \) and \( F \) is learnable if there exists at least one consistent learning algorithm \( A \). As we have already seen on multiple occasions, under certain conditions the ERM algorithm is consistent. A learning algorithm \( A \) is an \textit{Asymptotic Empirical Risk Minimizer} (AERM) if

\[
e_n(A) := \sup_P \mathbb{E}_P \left[ L_n(A(Z^n)) - L^*_n \right] \xrightarrow{n \to \infty} 0.
\]  

(11.3)

Of course, if \( A \) is the exact ERM algorithm, then \( e_n(A) = 0 \) for all \( n \), but there are many situations in which it is preferable to use AERM algorithms. Next, we say that \( A \) generalizes if

\[
g_n(A) := \sup_P \mathbb{E}_P \left| L(A(Z^n)) - L_n(A(Z^n)) \right| \xrightarrow{n \to \infty} 0.
\]  

(11.4)

A weaker notion of generalization is as follows: \( A \) generalizes \textit{on average} if

\[
\bar{g}_n(A) := \sup_P \mathbb{E}_P \left[ |L(A(Z^n)) - L_n(A(Z^n))| \right] \xrightarrow{n \to \infty} 0.
\]  

(11.5)

Our goal is to show that learnability is possible without requiring the UCEM property; instead, we will investigate the relationship between the above properties of learning algorithms to \textit{stability}, i.e., weak dependence of the algorithm output on any individual training sample.

2. A primer on convex functions

In order to proceed, we first need to introduce some ideas from convex analysis. Let \( \mathcal{H} \) be a Hilbert space. A subset \( F \subseteq \mathcal{H} \) is \textit{convex} if

\[
f_1, f_2 \in F \implies \lambda f_1 + (1 - \lambda) f_2 \in F, \forall \lambda \in [0, 1].
\]

A function \( \varphi : F \to \mathbb{R} \) is convex if

\[
\varphi(\lambda f_1 + (1 - \lambda) f_2) \leq \lambda \varphi(f_1) + (1 - \lambda) \varphi(f_2), \quad \forall f_1, f_2 \in F, \lambda \in [0, 1].
\]

A vector \( g \in \mathcal{H} \) is a \textit{subgradient} of \( \varphi \) at \( f \in F \) if

\[
\varphi(f') \geq \varphi(f) + \langle g, f' - f \rangle, \quad \forall f' \in F.
\]

The set of all subgradients of \( \varphi \) at \( f \) is denoted by \( \partial \varphi(f) \) and is referred to as the \textit{subdifferential} of \( \varphi \) at \( f \). It can be shown that \( \partial \varphi(f) \neq \emptyset \) for every \( f \in F \). We say that \( \varphi \) is differentiable at \( f \) if \( \partial \varphi(f) \) has only one element, in which case we refer to this element as the \textit{gradient} of \( \varphi \) at \( f \) and denote it by \( \nabla \varphi(f) \).

Given a convex function \( \varphi \) on \( F \), it is often of interest to minimize it, i.e., to find some \( f^* \in F \), such that \( \varphi(f^*) \leq \varphi(f) \) for all other \( f \in F \), in which case we say that \( f^* \) is a minimizer of \( \varphi \) on \( F \). We have the following basic result:

**Lemma 11.1** (First-order optimality condition). Let \( \varphi : F \to \mathbb{R} \) be a differentiable convex function. The point \( f^* \in F \) is a minimizer of \( \varphi \) on \( F \) if and only if

\[
\langle \nabla \varphi(f^*), f - f^* \rangle \geq 0, \quad \forall f \in F.
\]  

(11.6)
PROOF. To prove sufficiency, note that, by definition of the subgradient,
\[ \varphi(f) \geq \varphi(f^*) + \langle g^*, f - f^* \rangle \]
for any \( g^* \in \partial \varphi(f^*) \). If (11.6) holds, then \( \varphi(f) \geq \varphi(f^*) \) for all \( f \in \mathcal{F} \). (Note that here we do not require differentiability of \( \varphi \).)

To prove necessity, let \( f^* \) be a minimizer of \( \varphi \) on \( \mathcal{F} \), and suppose that (11.6) does not hold. That is, there exists some \( f \in \mathcal{F} \), such that \( \langle \nabla \varphi(f^*), f - f^* \rangle < 0 \). By convexity of \( \mathcal{F} \), \( f^* + t(f - f^*) \in \mathcal{F} \) for all sufficiently small \( t > 0 \). Consider the function \( F(t) := \varphi(f^* + t(f - f^*)) \). Since \( \varphi \) is differentiable, so is \( F \). By the chain rule, which holds in a Hilbert space, we have
\[ F'(0) = \langle \nabla \varphi(f^*), f - f^* \rangle \bigg|_{t=0} = \langle \nabla \varphi(f^*), f - f^* \rangle < 0. \]
But this means that \( F(t) < F(0) \) for all small \( t > 0 \), which contradicts the optimality of \( f^* \). \( \square \)

Next, we say that a function \( \varphi : \mathcal{F} \to \mathbb{R} \) is \( \sigma \)-strongly convex, for some \( \sigma \geq 0 \), if
\[ \varphi(f') \geq \varphi(f) + \langle g, f' - f \rangle + \frac{\sigma}{2} \| f - f' \|^2, \]
for all \( f, f' \in \mathcal{F} \) and all \( g \in \partial \varphi(f) \). In the case \( \sigma = 0 \), we recover the usual definition of convexity; the real power of this condition is when \( \sigma > 0 \), so from now on we will only use this term when \( \sigma > 0 \). Fix any two \( f, f' \in \mathcal{F} \) and any \( \lambda \in [0,1] \). Then
\[ \varphi(f) \geq \varphi(\lambda f + (1 - \lambda)f') + (1 - \lambda)\langle g, f - f' \rangle + \frac{(1 - \lambda)^2\sigma}{2} \| f - f' \|^2 \]
and
\[ \varphi(f') \geq \varphi(\lambda f + (1 - \lambda)f') - \lambda\langle g, f - f' \rangle + \frac{\lambda^2\sigma}{2} \| f - f' \|^2, \]
for any \( g \in \partial \varphi(\lambda f + (1 - \lambda)f') \). Multiplying the first inequality by \( \lambda \), the second one by \( 1 - \lambda \), and adding them, we get
\[ \lambda \varphi(f) + (1 - \lambda)\varphi(f') \geq (1 - \lambda)\varphi(f') + \frac{\lambda(1 - \lambda)\sigma}{2} \| f - f' \|^2. \]
Rearranging, we see that a \( \sigma \)-strongly convex function has the property that
\[ \varphi(\lambda f + (1 - \lambda)f') \leq \lambda \varphi(f) + (1 - \lambda)\varphi(f') - \frac{\lambda(1 - \lambda)\sigma}{2} \| f - f' \|^2. \]
In other words, the value of \( \varphi \) at \( \lambda f + (1 - \lambda)f' \) is strictly smaller than the weighted average \( \lambda \varphi(f) + (1 - \lambda)\varphi(f') \). It can be shown that a strongly convex function \( \varphi \) has a unique minimizer \( f^* \in \mathcal{F} \), and moreover, for any other \( f \in \mathcal{F} \),
\[ \varphi(f) - \varphi(f') \geq \frac{\sigma}{2} \| f - f' \|^2. \]
Indeed, for any \( \lambda \in (0,1) \) and any \( f \in \mathcal{F} \), we have
\[ \lambda \varphi(f) + (1 - \lambda)\varphi(f^*) \geq \varphi(\lambda f + (1 - \lambda)f^*) + \frac{\lambda(1 - \lambda)\sigma}{2} \| f - f' \|^2 \geq \varphi(f^*) + \frac{\lambda(1 - \lambda)\sigma}{2} \| f - f^* \|^2, \]
133
where the first step uses (11.8) and the second step uses the optimality of \( f^* \). Thus, for any \( f \in \mathcal{F} \) and any \( \lambda \in (0, 1) \),

\[
\varphi(f) \geq \varphi(f^*) + \frac{(1 - \lambda)\sigma}{2}\|f - f'\|^2.
\]

Sending \( \lambda \to 0 \), we obtain (11.9).

We say that a differentiable (not necessarily convex) function \( \varphi : \mathcal{F} \to \mathbb{R} \) is \( \beta \)-smooth, for some \( \beta \geq 0 \), if the gradient mapping \( f \mapsto \nabla \varphi(f) \) is \( \beta \)-Lipschitz:

\[
\|\nabla \varphi(f) - \nabla \varphi(f')\| \leq \beta\|f - f'\|, \quad \forall f, f' \in \mathcal{F}.
\]

(11.10)

3. Learnability without uniform convergence

We now show that we can have learnability without assuming uniform convergence:

**Theorem 11.1.** Suppose that \( \mathcal{F} \) is a convex subset of a Hilbert space \( \mathcal{H} \), and there constants \( L, \sigma > 0 \), such that, for every \( z \in \mathcal{Z} \), the function \( f \mapsto \ell(f, z) \) is \( \sigma \)-strongly convex and \( L \)-Lipschitz. Then the ERM algorithm

\[
\hat{f}_n = A(Z^n) = \arg\min_{f \in \mathcal{F}} \frac{1}{n} \sum_{i=1}^n \ell(f, Z_i)
\]

is such that

\[
L(\hat{f}_n) - L^* \leq \frac{4L^2}{\delta \sigma n},
\]

with probability at least \( 1 - \delta \).

**Proof.** The idea is to compare the output of \( A \) on the original training data \( Z^n \) to the output of \( A \) on the modified data, with one of the training samples replaced. Specifically, let \( Z'_1, \ldots, Z'_n \) be \( n \) i.i.d. samples from \( P \), independent of \( Z^n \). For each \( i \), define the modified training data

\[
Z^n_{(i)} := (Z_1, \ldots, Z_{i-1}, Z'_i, Z_{i+1}, \ldots, Z_n),
\]

and consider the corresponding ERM solution:

\[
\hat{f}^{(i)}_n := \arg\min_{f \in \mathcal{F}} L^{(i)}_n(f),
\]

where

\[
L^{(i)}_n(f) := \frac{1}{n} \ell(f, Z'_i) + \frac{1}{n} \sum_{j \neq i} \ell(f, Z_j)
\]
is the empirical loss of \( \ell \) on the modified data \( \hat{Z}_{n_i}' \). Let us compare the empirical losses of \( \hat{f}_n^{(i)} \) and \( \hat{f}_n \) on the original training data \( Z^n \): using the definitions, we write
\[
L_n(\hat{f}_n^{(i)}) - L_n(\hat{f}_n) = \frac{1}{n} \ell(\hat{f}_n^{(i)}, Z_i) + \frac{1}{n} \sum_{j \neq i} \ell(\hat{f}_n^{(i)}, Z_j) - \frac{1}{n} \ell(\hat{f}_n, Z_i) - \frac{1}{n} \sum_{j \neq i} \ell(\hat{f}_n, Z_j)
\]
\[
= \frac{1}{n} \ell(\hat{f}_n^{(i)}, Z_i) - \ell(\hat{f}_n, Z_i) + \sum_{j \neq i} \left[ \frac{1}{n} \ell(\hat{f}_n^{(i)}, Z_j) - \frac{1}{n} \ell(\hat{f}_n, Z_j) \right]
\]
\[
= \ell(\hat{f}_n^{(i)}, Z_i) - \ell(\hat{f}_n, Z_i) - \frac{1}{n} \sum_{j \neq i} \left[ \ell(\hat{f}_n^{(i)}, Z_j) - \ell(\hat{f}_n, Z_j) \right] + \frac{1}{n} \sum_{j \neq i} \ell(\hat{f}_n, Z_j) - \ell(\hat{f}_n^{(i)}, Z_j) + \frac{1}{n} \sum_{j \neq i} \ell(\hat{f}_n^{(i)}, Z_j) - \ell(\hat{f}_n^{(i)}, Z_j)
\]
\[
= \left[ \ell(\hat{f}_n^{(i)}, Z_i) - \ell(\hat{f}_n, Z_i) \right] - T_1 + T_2 + T_3.
\]

Now, \( T_2 \leq 0 \) because \( \hat{f}_n^{(i)} \) minimizes empirical loss over the modified data \( \hat{Z}_{n_i}' \), whereas both \( T_1 \) and \( T_3 \) are bounded from above by \( \frac{L}{n} \| \hat{f}_n - \hat{f}_n^{(i)} \| \), by the Lipschitz property of \( \ell \). Therefore,
\[
L_n(\hat{f}_n^{(i)}) - L_n(\hat{f}_n) \leq \frac{2L}{n} \| \hat{f}_n - \hat{f}_n^{(i)} \|.
\]

On the other hand, by the strong convexity assumption on \( \ell \), the functional \( f \mapsto L_n(f) \) is \( \sigma \)-strongly convex, and \( \hat{f}_n \) is its minimizer of \( \mathcal{F} \). Therefore, by (11.9),
\[
L_n(\hat{f}_n^{(i)}) - L_n(\hat{f}_n) \geq \frac{\sigma}{2} \| \hat{f}_n - \hat{f}_n^{(i)} \|^2.
\]

From Eqs. (11.11) and (11.12), it follows that
\[
\| \hat{f}_n - \hat{f}_n^{(i)} \| \leq \frac{4L}{\sigma n}.
\]

In other words, arbitrarily replacing any one sample in \( Z^n \) by some other \( Z_i' \) has only limited effect on the ERM solution, i.e., the algorithm output \( A(Z^n) \) does not depend too much on any individual sample! But, because \( \ell \) is Lipschitz, this implies that, for any \( z \in Z \),
\[
\left| \ell(\hat{f}_n, z) - \ell(\hat{f}_n^{(i)}, z) \right| \leq L \| \hat{f}_n - \hat{f}_n^{(i)} \| \leq \frac{4L^2}{\sigma n}.
\]

We now claim that the stability property (11.14) implies
\[
\mathbb{E} \left[ L(\hat{f}_n) - L_n(\hat{f}_n) \right] \leq \frac{4L^2}{\sigma n}.
\]

Indeed, since \( \hat{f}_n \) is a function of \( Z^n \), and since \( Z_1', \ldots, Z_n' \) are independent of \( Z_1, \ldots, Z_n \) and are draws from the same distribution, we can write
\[
\mathbb{E} L(\hat{f}_n) = \frac{1}{n} \sum_{i=1}^{n} \mathbb{E} [\ell(\hat{f}_n, Z_i')].
\]

On the other hand, since, for every \( i \), \( \ell(\hat{f}_n, Z_n) \) and \( \ell(\hat{f}_n^{(i)}, Z_i') \) have the same distribution, we have
\[
\mathbb{E} L_n(\hat{f}_n) = \frac{1}{n} \sum_{i=1}^{n} \mathbb{E} [\ell(\hat{f}_n, Z_i)] = \frac{1}{n} \sum_{i=1}^{n} \mathbb{E} [\ell(\hat{f}_n^{(i)}, Z_i')] = \frac{1}{n} \sum_{i=1}^{n} \mathbb{E} [\ell(\hat{f}_n^{(i)}, Z_i')].
\]
Therefore,

\[
\mathbb{E} \left[ L(\hat{f}_n) - L_n(\hat{f}_n) \right] = \frac{1}{n} \sum_{i=1}^{n} \mathbb{E} \left[ \ell(\hat{f}_n, Z_i') - \ell(\hat{f}_n^{(i)}, Z_i') \right]
\]

\[
\leq \frac{1}{n} \sum_{i=1}^{n} \sup_{z \in \mathcal{Z}} \left| \ell(\hat{f}_n, z) - \ell(\hat{f}_n^{(i)}, z) \right|
\]

\[
\leq \frac{4L^2}{\sigma n},
\]

as claimed. Eq. (11.15) shows that the ERM algorithm generalizes well on average, i.e., the empirical loss of \( \hat{f}_n = A(Z^n) \) on the data \( Z^n \) is a good estimate of \( L(\hat{f}_n) = L(A(Z^n)) \) in expectation.

Now let \( f^* \in \mathcal{F} \) achieve \( L^* \). Since \( f^* \) doesn’t depend on \( Z^n \), we have \( L^* = L(f^*) = \mathbb{E}[L_n(f^*)] \), and therefore

\[
\mathbb{E} \left[ L(\hat{f}_n) - L^* \right] = \mathbb{E} \left[ L(\hat{f}_n) - L_n(\hat{f}_n) + L_n(\hat{f}_n) - L_n(f^*) \right]
\]

\[
\leq \mathbb{E} \left[ L(\hat{f}_n) - L_n(\hat{f}_n) \right]
\]

\[
\leq \frac{4L^2}{\sigma n}.
\]

From Markov’s inequality, it then follows that

\[
L(\hat{f}_n) - L^* \leq \frac{4L^2}{\delta \sigma n}
\]

with probability at least \( 1 - \delta \), and we are done. \( \square \)

Armed with this theorem, we can now establish the following result for a complexity-regularized ERM:

**Theorem 11.2.** Let \( \mathcal{F} \) be a convex and norm-bounded subset of a Hilbert space \( \mathcal{H} \), i.e., there exists some \( B < \infty \), such that \( \|f\| \leq B \) for all \( f \in \mathcal{F} \). Suppose also that, for each \( z \in \mathcal{Z} \), the function \( f \mapsto \ell(f, z) \) is convex and \( L \)-Lipschitz (note: we are not assuming strong convexity). For each \( \lambda > 0 \), consider the complexity-regularized ERM algorithm

\[
\hat{f}_{n,\lambda} = A_{\lambda}(Z^n) := \arg \min_{f \in \mathcal{F}} \left\{ \frac{1}{n} \sum_{i=1}^{n} \ell(f, Z_i) + \frac{\lambda}{2} \|f\|^2 \right\}.
\]

Then \( \hat{f}_n = \hat{f}_{n,\lambda} \) with \( \lambda = \frac{B}{L\sqrt{n}} \) satisfies

\[
L(\hat{f}_n) \leq L^* + \frac{LB}{2\sqrt{n}} + \frac{8LB}{\delta \sqrt{n}} + \frac{8LB}{\delta n^{3/2}}
\]

with probability at least \( 1 - \delta \).
Proof. Consider the function \( \ell_\lambda(f, z) := \ell(f, z) + \frac{\lambda}{2} \|f\|^2 \). This function is clearly \( \lambda \)-strongly convex. Moreover, for any fixed \( z \) and any \( f, f' \in \mathcal{F} \), we have

\[
|\ell_\lambda(f, z) - \ell_\lambda(f', z)| \leq |\ell(f, z) - \ell(f', z)| + \frac{\lambda}{2} \|f\|^2 - \|f'\|^2
\]

\[
\leq L \|f - f'\| + \frac{\lambda}{2} \|f\| - \|f'\| \cdot \|f\| + \|f'\|
\]

\[
\leq L \|f - f'\| + \lambda B \|f - f'\|
\]

i.e., \( \ell_\lambda \) is \( \lambda \)-strongly convex and \((L + \lambda B)\)-Lipschitz. For each \( f \in \mathcal{F} \), let \( L_\lambda(f) := L(f) + \frac{\lambda}{2} \|f\|^2 = E[\ell_\lambda(f, Z)] \). Applying Theorem 11.1, we conclude that, with probability at least \( 1 - \delta \),

\[
L_\lambda(\hat{f}_{n, \lambda}) - L_\lambda^* \leq \frac{4(L + \lambda B)^2}{\delta \lambda n},
\]

where \( L_\lambda^* := \inf_{f \in \mathcal{F}} L_\lambda(f) \). Therefore, with the same probability,

\[
L(\hat{f}_{n, \lambda}) \leq L_\lambda^* + \frac{4(L + \lambda B)^2}{\delta \lambda n}
\]

\[
= \inf_{f \in \mathcal{F}} \left\{ L(f) + \frac{\lambda}{2} \|f\|^2 \right\} + \frac{4(L + \lambda B)^2}{\delta \lambda n}
\]

\[
\leq L^* + \frac{\lambda}{2} \|f^*\|^2 + \frac{4(L + \lambda B)^2}{\delta \lambda n}
\]

\[
\leq L^* + \frac{\lambda B^2}{2} + \frac{4(L + \lambda B)^2}{\delta \lambda n}
\]

\[
\leq L^* + \frac{\lambda B^2}{2} + \frac{8L^2}{\delta \lambda n} + \frac{8\lambda B^2}{\delta n}.
\]

□

4. Learnability and stability

Let us now see how the above ideas can be abstracted into a general set of results about learnability and stability. We say that a learning algorithm \( A : Z^* \to \mathcal{F} \) is stable on average (with respect to replace-one operation) if

\[
\bar{s}_n(A) := \sup_p \frac{1}{n} \sum_{i=1}^{n} \mathbb{E} \left[ \ell(A(Z^n_i), Z_i') - \ell(A(Z^n), Z_i') \right] \xrightarrow{n \to \infty} 0.
\]

We have already proved the following:

**Lemma 11.2.** For any learning algorithm, \( \bar{g}_n(A) = \bar{s}_n(A) \). In particular, \( A \) is stable on average if and only if it generalizes on average.

Now we can show more:

**Lemma 11.3.** If \( A \) is an AERM that generalizes on average, then it generalizes, and moreover

\[
g_n(A) \leq \bar{g}_n(A) + 2c_n(A) + \frac{2}{\sqrt{n}}.
\]
Proof. We begin by decomposing the difference $L_n(A(Z^n)) - L(A(Z^n))$:

$$L_n(A(Z^n)) - L(A(Z^n)) = L_n(A(Z^n)) - L_n^* + L_n^*(f^*) + L_n(f^*) - L(A(Z^n)) \leq 0$$

Applying Lemma 11.8 in the Appendix to $U := L_n(A(Z^n)) - L(A(Z^n))$ and $V := L_n(A(Z^n)) - L_n^* + L_n(f^*) - L(f^*)$, we get

$$\mathbb{E} |L_n(A(Z^n)) - L(A(Z^n))| \leq |\mathbb{E}[L_n(A(Z^n)) - L(A(Z^n))]| + 2\mathbb{E} |L(A(Z^n)) - L_n^* + L_n(f^*) - L(f^*)| \leq \bar{g}_n(A) + 2e_n(A) + \frac{2}{\sqrt{n}},$$

where in the last line we have used the assumed properties of $A$, together with the fact that, for any $f$, $\mathbb{E}|L_n(f) - L(f)| = \mathbb{E}|L_n(f) - \mathbb{E}L_n(f)| \leq \sqrt{\mathbb{E}(L_n(f) - \mathbb{E}L_n(f))^2} \leq \frac{1}{\sqrt{n}}$. Since $\ell$ is bounded between 0 and 1. This completes the proof.

Corollary 11.1. If $A$ is an AERM which is stable on average, then it generalizes, and moreover

$$g_n(A) \leq \bar{g}_n(A) + 2e_n(A) + \frac{2}{\sqrt{n}}.$$

All of this leads to the following result:

Theorem 11.3. An AERM learning algorithm $A$ is stable on average if and only if it generalizes, with

$$g_n(A) - 2e_n(A) - \frac{2}{\sqrt{n}} \leq \bar{s}_n(A) \leq g_n(A).$$

Moreover, if $A$ is an AERM which is stable on average, then it is consistent, with

$$c_n(A) \leq \bar{s}_n(A) + e_n(A).$$

Proof. We have already proved that stability is equivalent to generalization on average, but for an AERM generalization on average implies generalization. Conversely, if $A$ generalizes, then it generalizes on average, and is therefore stable on average.

To prove the second part, since $\bar{s}_n(A) = \bar{g}_n(A)$, we have

$$\mathbb{E}[L(A(Z^n)) - L^*] = \mathbb{E}[L(A(Z^n)) - L_n(A(Z^n)) + L_n(A(Z^n)) - L_n(f^*)] \leq \mathbb{E}[L(A(Z^n)) - L_n(A(Z^n))] + \mathbb{E}[L_n(A(Z^n)) - L_n^*] \leq \bar{g}_n(A) + e_n(A) = \bar{s}_n(A) + e_n(A).$$

\[\square\]
5. Stability of stochastic gradient descent

**WARNING:** This section is still very rough, needs more editing.

One of the most popular algorithms for learning over complicated hypothesis classes (such as deep neural networks) is the Stochastic Gradient Descent (SGD) algorithm. The basic idea behind SGD is as follows. For a fixed training set $Z^n = (Z_1, \ldots, Z_n)$, the usual ERM approach requires minimizing the function

$$L_n(f) = \frac{1}{n} \sum_{i=1}^{n} \ell(f, Z_i)$$

over the hypothesis class $\mathcal{F}$. One way to go about this is to use gradient descent: assuming that the function $f \mapsto \ell(f, z)$ is differentiable for each $z \in Z$, we can set the initial condition $f_0 \in \mathcal{F}$ and iteratively compute

$$f_t = f_{t-1} - \alpha_t \nabla L_n(f_{t-1}), \quad t = 1, 2, \ldots$$

(11.22)

where

$$\nabla L_n(f_{t-1}) = \frac{1}{n} \sum_{i=1}^{n} \nabla \ell(f_{t-1}, Z_i)$$

is the gradient of $L_n$ at $f_{t-1}$, and $\{\alpha_t\}_{t=1}^{\infty}$ is a monotonically decreasing sequence of nonnegative reals typically referred to as step sizes. (For simplicity, we are assuming here that the updates defined in (11.22) stay in $\mathcal{F}$; in general, one needs an additional step of projecting onto $\mathcal{F}$.) Under certain mild conditions on $\ell$ and $\mathcal{F}$, and with appropriately tuned step sizes, one can guarantee that

$$L_n(f_t) \to \inf_{f \in \mathcal{F}} L_n(f) \equiv L_n^* \quad \text{as} \quad t \to \infty.$$ 

In other words, for each $n$, we can find a large enough $T_n$, such that $A(Z^n) = f_{T_n}$ is an AERM algorithm.

However, one disadvantage of gradient descent is that each update (11.22) requires a sweep through the entire sample $Z^n$ in order to compute the gradient $\nabla L_n$. Thus, the complexity of each step of the gradient descent method scales as $O(n)$. SGD offers a way around this limitation and allows to reduce the complexity of each iteration to $O(1)$. If we look at (11.21), we see that the empirical loss $L_n(f)$ can be written as an average of $n$ functions of $f$:

$$L_n(f) = \frac{1}{n} \sum_{i=1}^{n} \ell_i(f), \quad \text{where} \quad \ell_i(f) := \ell(f, Z_i).$$

In each iteration of SGD, we pick a random index $I_t \in \{1, \ldots, n\}$ and update

$$f_t = f_{t-1} - \alpha_t \nabla \ell_{I_t}(f_{t-1}) \equiv f_{t-1} - \alpha_t \nabla \ell(f_{t-1}, Z_{I_t}).$$

(11.23)

Thus, SGD is a randomized algorithm. Two popular choices for selecting the indices $I_t$ are:

- **Random selection:** At each time step $t$, $I_t$ is drawn uniformly at random from $\{1, \ldots, n\}$, independently of all past realizations $I_1, \ldots, I_{t-1}$.
• **Random permutation:** At time $t = 0$, we draw a permutation $\sigma$ of the set $\{1, \ldots, n\}$ uniformly at random and then cycle through the samples $Z_{\sigma(1)}, Z_{\sigma(2)}, \ldots, Z_{\sigma(n)}$:

$$I_t = \sigma(1 + [(t - 1) \mod n]).$$

In a recent paper, Hardt et al. [HRS15] have shown that SGD with suitably tuned step sizes and number of updates gives a stable learning algorithm. Under different assumptions on the loss function $\ell$, we end up with different conditions for stability. In order to proceed, let us first examine the evolution of SGD updates for a fixed training set $Z^n$.

For each $t$, define the random indices $I_t \in \{1, \ldots, n\}$. Fix a differentiable function $\varphi : \mathcal{F} \to \mathbb{R}$ and a step size $\alpha \geq 0$, and define an operator $G_{\varphi, f} : \mathcal{F} \to \mathcal{F}$ by

$$G(f) := f - \alpha \nabla \varphi(f).$$

Again, to keep things simple, we assume that the image of $\mathcal{F}$ under $G$ is contained in $\mathcal{F}$. Then we can write the $t$th update of SGD as

$$f_t = G_t(f_{t-1}), \quad \text{where } G_t = G_{\ell(t, Z_{I_t}), \alpha_t}.$$  

Now let us fix some $i \in \{1, \ldots, n\}$ and consider running SGD with the same realization of the random indices $\{I_t\}$ on another training set $Z^n = (Z'_1, \ldots, Z'_n)$ that differs from $Z^n$ only in one sample. Denoting by $\{f'_t\}$ the corresponding updates with $f'_0 = f_0$, we can write

$$f'_t = G'_t(f'_{t-1}), \quad \text{where } G'_t = \begin{cases} G_t, & \text{if } Z_{I_t} = Z'_{I_t} \\ G_{\ell(t, Z'_{I_t}), \alpha_t}, & \text{otherwise.} \end{cases}$$

For each $t = 0, 1, \ldots$, let $\delta_t := \|f_t - f'_t\|$, with the initial condition $\delta_0 = 0$. We can now track the evolution of $\delta_t$ as follows:

- If $G_t = G'_t$, then

$$\begin{align*}
\delta_t &= \|f_t - f'_t\| \\
&= \|G_t(f_{t-1}) - G_t(f'_{t-1})\| \\
&\leq \eta_t \|f_{t-1} - f'_{t-1}\| \\
&\equiv \eta_t \delta_t,
\end{align*}$$

where we have defined

$$\eta_t := \sup_{f, f' \in \mathcal{F}} \frac{\|G_t(f) - G_t(f')\|}{\|f - f'\|}.$$  

- If $G_t \neq G'_t$, then, on the one hand,

$$\begin{align*}
\delta_t &= \|G_t(f_{t-1}) - G'_t(f_{t-1})\| \\
&\leq \|G_t(f_{t-1}) - f_{t-1}\| + \|f_{t-1} - f'_{t-1}\| + \|G'_t(f_{t-1}) - f'_{t-1}\| \\
&\leq 2c_t + \delta_{t-1},
\end{align*}$$

where we have defined

$$c_t := \max \left\{ \sup_{f \in \mathcal{F}} \|G_t(f) - f\|, \sup_{f \in \mathcal{F}} \|G'_t(f) - f\| \right\},$$

140
and on the other hand,
\begin{align}
\delta_t &= \|G_t(f_{t-1}) - G'_t(f'_{t-1})\| \\
&\leq \|G_t(f_{t-1}) - G_t(f'_{t-1})\| + \|G_t(f'_{t-1}) - f'_{t-1}\| + \|G'_t(f'_{t-1}) - f'_{t-1}\| \\
&\leq \eta_t \delta_{t-1} + 2c_t.
\end{align}

This gives us the bound
\begin{equation}
\delta_t \leq (1 \land \eta_t) \delta_{t-1} + 2c_t.
\end{equation}

Summarizing:
\begin{equation}
\delta_t \leq \begin{cases} 
\eta_t \delta_{t-1}, & \text{if } G_t = G'_t \\
(1 \land \eta_t) \delta_{t-1} + 2c_t, & \text{otherwise.}
\end{cases}
\end{equation}

This will be our main tool for analyzing the stability of SGD. Another tool is the following estimate:

**Lemma 11.4.** Suppose that, for each \( z \in \mathbb{Z} \), the function \( f \mapsto \ell(f, z) \) is \( L \)-Lipschitz, and takes values in \([0, 1]\). Let \( \{f_t^T\}_{t=0}^T \) and \( \{f'_t\}_{t=0}^T \) be the updates of SGD (either with random selection or with random permutation) run on two datasets \( Z^n \) and \( Z'^n \) that differ only in one sample, with \( f_0 = f'_0 \). Then, for any \( t_0 \in \{0, \ldots, n\} \) and for any \( z \in \mathbb{Z} \),
\begin{equation}
\mathbb{E}[|\ell(f_T, z) - \ell(f'_T, z)|] \leq LE[\delta_T \mathbf{1}\{\delta_{t_0} = 0\}] + \frac{t_0}{n}.
\end{equation}

**Proof.** We start by writing
\begin{align}
|\ell(f_T, z) - \ell(f'_T, z)| &= |\ell(f_T, z) - \ell(f'_T, z)| \mathbf{1}\{\delta_{t_0} = 0\} + |\ell(f_T, z) - \ell(f'_T, z)| \mathbf{1}\{\delta_{t_0} \neq 0\} \\
&\leq L\|f_T - f'_T\| \mathbf{1}\{\delta_{t_0} = 0\} + \mathbf{1}\{\delta_{t_0} \neq 0\},
\end{align}

where in the second step we have used the fact that \( \ell \) is \( L \)-Lipschitz and takes values in \([0, 1]\). Taking expectations, we get
\begin{equation}
\mathbb{E}[|\ell(f_T, z) - \ell(f'_T, z)|] \leq LE[\delta_T \mathbf{1}\{\delta_{t_0} = 0\}] + \mathbb{P}\{\delta_{t_0} \neq 0\}.
\end{equation}

It remains to bound the probability on the right-hand side. To that end, let \( i^* \in \{1, \ldots, n\} \) be the position where the two training sets differ. Define an integer-valued random variable \( I \) as the first time that the SGD algorithm uses the sample \( Z_{i^*} \). Now observe that if \( I > t_0 \), then \( \delta_{t_0} = 0 \), because the updates \( f_t \) and \( f'_t \) are the same for all \( t < I \). Consequently, \( \mathbb{P}\{\delta_{t_0} \neq 0\} \leq \mathbb{P}\{I \leq t_0\} \). To upper-bound the latter probability, we consider the two index selection rules separately:

- In the case of random permutation, the samples are reshuffled as
  \( (Z_1, \ldots, Z_{i^*}, \ldots, Z_n) \mapsto (Z_{\sigma(1)}, \ldots, Z_{\sigma(i^*)}, \ldots, Z_{\sigma(n)}) \)
  \( (Z'_{1}, \ldots, Z'_{i^*}, \ldots, Z'_n) \mapsto (Z_{\sigma(1)}, \ldots, Z_{\sigma(i^*)}, \ldots, Z_{\sigma(n)}) \).

  While the two original datasets \( Z^n \) and \( Z'^n \) differed in the \( i^* \)th position, the permuted datasets now differ in position \( J^* = \sigma^{-1}(i^*) \), where \( \sigma \) is the permutation of \( \{1, \ldots, n\} \) drawn uniformly at random at time \( t = 0 \). Therefore, \( I = J^* \). It is not hard to see that the event \( \{J^* = j\} \) has probability \( 1/n \) for all \( j = 1, \ldots, n \)—
there are \( n! \) permutations, and among these there are \((n - 1)!\) permutations with \( \sigma(j) = i^* \). Therefore, in the random permutation case,

\[
P[I \leq t_0] = P[\sigma^{-1}(i^*) \leq t_0] = \frac{t_0}{n}.
\]

- In the case of random selection, the index \( I_t \) is drawn uniformly at random from \( \{1, \ldots, n\} \), independently of the past realizations \( I_1, \ldots, I_{t-1} \). Therefore,

\[
P[I \leq t_0] = P[\bigcup_{t=1}^{t_0} \{I_t = i^*\}] \leq \sum_{t=1}^{t_0} P[I_t = i^*] = \frac{t_0}{n}.
\]

Thus, in both cases, the probability \( P[\delta_{t_0} \neq 0] \leq \frac{t_0}{n} \). \( \square \)

Now we can analyze the stability of SGD under several assumptions on the loss \( \ell \):

**Theorem 11.4.** Suppose that, for each \( z \in Z \), the loss function \( f \mapsto \ell(f, z) \) is convex, \( \beta \)-smooth, and \( L \)-Lipschitz. Suppose that we run SGD with step sizes \( \alpha_t \leq \frac{2}{\beta} \) for \( T \) time steps. Then, for any two datasets \( Z^m \) and \( Z^m' \) that differ in only one sample,

\[
\sup_{z \in Z} E|\ell(f_T, z) - \ell(f_T', z)| \leq \frac{2L^2}{n} \sum_{t=1}^{T} \alpha_t,
\]

where the expectation is only with respect to the internal randomness of SGD (i.e., index selection).

**Proof.** It can be shown that, if \( \varphi \) is a convex, \( \beta \)-smooth, \( L \)-Lipschitz function, then the mapping \( G = G_{\varphi, \alpha} \) with \( \alpha \leq \frac{2}{\beta} \) satisfies

\[
\sup_{f, f' \in \mathcal{F}} \frac{\|G(f) - G(f')\|}{\|f - f'\|} \leq 1 \quad \text{and} \quad \sup_{f \in \mathcal{F}} \|G(f) - f\| \leq \alpha L.
\]

Applying Lemma 11.4 with \( t_0 = 0 \), we have

\[
E[\ell(f_T, z) - \ell(f_T', z)] \leq L E[\delta_T].
\]

In order to bound \( E[\delta_T] \), we will use (11.38). Let’s consider what happens at time \( t \). Let \( F_t \) denote the event that, at time \( t \), the SGD algorithm does not use different samples in \( Z^n \) and \( Z^m \). If \( F_t \) occurs, then \( G_t = G_t' \), otherwise \( G_t \neq G_t' \). In that case,

\[
E[\delta_t] = E[\delta_t 1_{F_t}] + E[\delta_t 1_{F_t'}] \leq E[\eta_t \delta_{t-1} 1_{F_t}] + E\left[((1 \wedge \eta_t) \delta_{t-1} + 2c_t) 1_{F_t'}\right].
\]

By (11.46), we can take \( \eta_t = 1 \) and \( c_t = \alpha_t L \). Thus,

\[
E[\delta_t] \leq E[\delta_{t-1}] + 2\alpha_t L E[F_t'].
\]

In both the random permutation and the random selection case, \( P[F_t'] = 1/n \). Therefore, we end up with the recursion

\[
E[\delta_t] \leq E[\delta_{t-1}] + \frac{2\alpha_t L}{n}, \quad t = 1, 2, \ldots, T
\]
with the initial condition $\delta_0 = 0$. Unwinding the recursion, we get
\begin{equation}
E[\delta_T] \leq \frac{2L}{n} \sum_{t=1}^{T} \alpha_t.
\end{equation}
Substituting this into Eq. (11.47), we are done. \hfill \Box

For example, if we set $T = n$ and $\alpha_t = 2/\beta \sqrt{n}$ for all $t$, then
\begin{equation}
\sum_{t=1}^{T} \alpha_t = \frac{2 \sqrt{n}}{\beta},
\end{equation}
and then the algorithm $A(Z^n)$ obtained by running SGD for $\sqrt{n}$ steps with constant step size $\alpha = 2/\beta \sqrt{n}$ is stable with $s_n(A) \leq 4L^2/\beta \sqrt{n}$.

If we now assume that $\ell$ is also strongly convex, we get a bound that does not depend on the number of iterations $T$:

**Theorem 11.5.** Suppose that $\ell$ satisfies the conditions of Theorem 11.4, and also that the function $f \mapsto \ell(f, z)$ is $\gamma$-strongly convex for each $z \in Z$. Suppose that we run SGD with a constant step size $\frac{1}{\beta} \leq \alpha \leq \frac{2}{\beta + \gamma}$ for $T$ time steps. Then, for any two datasets $Z^n$ and $Z'^n$ that differ in only one sample,
\begin{equation}
\sup_{z \in Z} E|\ell(f_T, z) - \ell(f'_T, z)| \leq \frac{2L^2}{\gamma n},
\end{equation}
where the expectation is only with respect to the internal randomness of SGD (i.e., index selection).

**Proof.** The proof is similar to the proof of Theorem 11.4. First of all, it can be shown that, under our assumptions on $\ell$ and on $\alpha$, we have
\begin{equation}
\eta_t \leq 1 - \alpha \gamma \quad \text{and} \quad c_t \leq \alpha L.
\end{equation}
Then the same steps that led to (11.51) give
\begin{equation}
E[\delta_t] \leq (1 - \alpha \gamma) E[\delta_{t-1}] + \frac{2 \alpha L}{n},
\end{equation}
with the initial condition $\delta_0 = 0$. Unwinding the recursion, we get
\begin{equation}
E[\delta_T] \leq \frac{2 \alpha L}{n} \sum_{t=1}^{T} (1 - \alpha \gamma)^{t-1} \leq \frac{2 \alpha L}{n} \cdot \frac{1}{\alpha \gamma} = \frac{2L}{\gamma n}.
\end{equation}
The result follows. \hfill \Box

Finally, we derive a stability estimate for SGD without requiring convexity, but still assuming Lipschitz-continuity and smoothness:

**Theorem 11.6.** Suppose that, for each $z \in Z$, the loss function $f \mapsto \ell(f, z)$ is $\beta$-smooth and $L$-Lipschitz. Suppose that we run SGD with step sizes $\alpha_t \leq c/t$ for $T$ time steps, where $c > 0$ is some constant. Then, for any two datasets $Z^n$ and $Z'^n$ that differ in only one sample,
\begin{equation}
\sup_{z \in Z} E|\ell(f_T, z) - \ell(f'_T, z)| \leq \frac{1 + 1/\beta c}{n} (2cL^2)^{1/\beta c + 1} T^{\beta c}.
\end{equation}
where the expectation is only with respect to the internal randomness of SGD (i.e., index selection).

**Proof.** Here the idea is to apply Lemma 11.4 with an arbitrary \( t_0 \in \{0,1,\ldots,n\} \), and then optimize over \( t_0 \). Under the assumptions on \( \ell \), we can apply (11.38) with
\[
\eta_t \leq 1 + \alpha_t \beta \quad \text{and} \quad c_t \leq \alpha_t L.
\]
By Lemma 11.4, for a fixed \( t_0 \in \{0,1,\ldots,n\} \), we have
\[
E[|\ell(f_T,z) - \ell(f'_T,z)|] \leq LE[\delta_T \mathbf{1}\{\delta_{t_0} = 0\}] + \frac{t_0}{n}.
\]
Let us denote \( \Delta_t := E[\delta_t | \delta_{t_0} = 0] \). For any time \( t > t_0 \), we have
\[
\Delta_t = E[\delta_t \mathbf{1}_{F_t} | \delta_{t_0} = 0] + E[\delta_t \mathbf{1}_{F_t^c} | \delta_{t_0} = 0] \\
\leq (1 + \alpha_t \beta)E[\delta_{t-1} \mathbf{1}_{F_{t-1}} | \delta_{t_0} = 0] + E[\delta_{t-1} \mathbf{1}_{F_{t-1}^c} | \delta_{t_0} = 0] + 2\alpha_t LP[F_t^c | \delta_{t_0} = 0]
\]
\[
\leq \left(1 + \frac{\beta L}{t}\right) \Delta_{t-1} + \frac{2cL}{tn}
\]
\[
\leq \exp(\beta c/t) \Delta_{t-1} + \frac{2cL}{tn},
\]
where in the last line we have used the inequality \( 1 + u \leq \exp(u) \). Unwinding the recursion down to \( t = t_0 + 1 \) and using the initial condition \( \Delta_{t_0} = 0 \), we have
\[
\Delta_T \leq \sum_{t=t_0+1}^{T} \prod_{k=t+1}^{T} \exp(\beta c/k) \frac{2cL}{tn}
\]
\[
= \sum_{t=t_0+1}^{T} \exp \left( \beta c \sum_{k=t+1}^{T} \frac{1}{k} \right) \frac{2cL}{tn}
\]
\[
\leq \sum_{t=t_0+1}^{T} \exp \left( \beta c \log \frac{T}{t} \right) \frac{2cL}{tn}
\]
\[
\leq \frac{2cL}{n} T^\beta c \sum_{t=t_0+1}^{T} t^{-(1+\beta c)}
\]
\[
\leq \frac{2cL}{n} T^\beta c \frac{1}{\beta c} \left( t_0^{-\beta c} - T^{-\beta c} \right)
\]
\[
\leq \frac{2L}{n\beta} \left( \frac{T}{t_0} \right)^{\beta c}.
\]
Plugging this estimate into (11.60), we get
\[
E[|\ell(f_T,z) - \ell(f'_T,z)|] \leq \frac{t_0}{n} + \frac{2L^2}{n\beta} \left( \frac{T}{t_0} \right)^{\beta c}.
\]
The right-hand side is (approximately) minimized by setting
\[
t_0 = (2cL^2)^{\frac{1}{\beta c}} T^{\frac{2}{\beta c + 1}}, \quad q = \beta c
\]
which gives

\[
E \left[ |\ell(f_T, z) - \ell(f_T', z)| \right] \leq \frac{1 + \beta c}{n} \frac{1}{(2cL^2)^\frac{1}{\beta c}} T^{\frac{\beta c}{\beta c + 1}}.
\]

\[\square\]

In this case, we can set \( T = n^{\varepsilon(1 + 1/\beta c)} \) for any \( \varepsilon \in (0, 1) \), and obtain the stability bound

\[
(11.73) \quad s_n(A) \leq \frac{1 + \beta c}{n} \frac{1}{(2cL^2)^\frac{1}{\beta c}} n^{\varepsilon - 1}
\]

for \( A(Z^n) = f_T \).

6. Differentially private algorithms and generalization

Recall that we have defined a randomized learning algorithm \( A \) to be stable if the outputs \( A(Z^n) \) and \( A(Z'^n) \) of \( A \) on two training sets \( Z^n \) and \( Z'^n \) that differ in only one example are close in terms of their losses: for example, \( A \) is \( \varepsilon \)-uniformly stable if

\[
(11.74) \quad \sup_{z \in Z} |E[\ell(A(Z^n), z) - E[\ell(A(Z'^n), z)]| \leq \varepsilon
\]

for all \( Z^n \) and \( Z'^n \) that differ in only one example.

In this section, we will examine a much stronger stability property that pertains to the sensitivity of the conditional distribution of the output of \( A \) given \( Z^n = z^n \) to individual training examples comprising \( Z^n \). For this purpose, it is convenient to think of \( F = A(Z^n) \) as a random object taking values in the hypothesis class \( \mathcal{F} \). Then the operation of \( A \) is fully described by the conditional distribution \( P_{F|Z^n} \). Moreover, we can rewrite the stability condition \((11.74)\) in the following equivalent form:

\[
(11.75) \quad \sup_{z \in Z} |E[\ell(F; z)|Z^n = z^n] - E[\ell(F; z)|Z^n = z'^n]| \leq \varepsilon
\]

for any two training sets \( z^n, z'^n \) that differ in at most one example. Let us now consider a stronger property that compares the conditional distribution of \( F \) given \( Z^n = z^n \) against the one given \( Z^n = z'^n \):

**Definition 11.1.** A randomized algorithm \( A \) specified by the conditional distribution \( P_{F|Z^n} \) is \((\varepsilon, \delta)\)-differentially private if, for any measurable subset \( B \) of \( \mathcal{F} \) and for any two training sets \( z^n, z'^n \) that differ in at most one example, we have

\[
(11.76) \quad P \left[ F \in B \mid Z^n = z^n \right] \leq e^\varepsilon P \left[ F \in B \mid Z^n = z'^n \right] + \delta.
\]

Equivalently, \( P_{F|Z^n} \) is \((\varepsilon, \delta)\)-differentially private if, for any function \( g : \mathcal{F} \to [0, 1] \),

\[
(11.77) \quad E[g(F)|Z^n = z^n] \leq e^\varepsilon E[g(F)|Z^n = z'^n] + \delta.
\]

This definition was proposed by Cynthia Dwork in the context of protecting individual information in statistical databases [Dwo06]. Of course, it is useful only for \( \delta \in [0, 1] \) and for suitably small values of \( \varepsilon \).

We start with the following simple observation:

**Lemma 11.5.** If a learning algorithm \( P_{F|Z^n} \) is \((\varepsilon, \delta)\)-differentially private, then it is \((e^\varepsilon - 1 + \delta)\)-uniformly stable in the sense of \((11.74)\). If \( \varepsilon \in [0, 1] \), then the algorithm is \((2\varepsilon + \delta)\)-uniformly stable.
Proof. A direct consequence of the definition: let $z^n, z'^m$ be two training sets differing in only one example. Then, for any $z \in Z$,

$$E[\ell(F, z)|Z^n = z^n] - E[\ell(F, z)|Z^n = z'^m] \leq (e^{\varepsilon} - 1)E[\ell(F, z)|Z^n = z'^m] + \delta \leq e^{\varepsilon} - 1 + \delta.$$ 

Since $e^u - 1 \leq 2u$ for $u \in [0, 1]$, we also obtain the second part of the lemma. \hfill $\square$

This stability estimate immediately implies that a differentially private algorithm should generalize. However, the resulting bounds are rather loose. We will now present a tighter bound, due to Nissim and Stemmer [NS15].

First, we need to collect some preliminaries on the properties of differentially private algorithms. Fix a randomized algorithm $A = P_{F|Z^n}$ and consider a new algorithm obtained by running $M$ copies of $A$ in parallel on $m$ training sets $(Z_{j,1}, \ldots, Z_{j,n})$, $1 \leq j \leq m$. In other words, we form the matrix

$$Z^{m \times n} = \begin{pmatrix} Z_{1,1} & Z_{1,2} & \ldots & Z_{1,n} \\ Z_{2,1} & Z_{2,2} & \ldots & Z_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ Z_{m,1} & Z_{m,2} & \ldots & Z_{m,n} \end{pmatrix}$$

and let $F_j$ be the output of $A$ on the $j$th row of $Z^{m \times n}$. This defines a new algorithm, which we denote by $A^m$ and which is described by the following conditional distribution $P_{F^m|Z^{m \times n}}$:

For any $m$ measurable sets $B_1, \ldots, B_m \subset \mathcal{F}$,

$$P \left[ F_1 \in B_1, \ldots, F_m \in B_m | Z^{m \times n} = z^{m \times n} \right] = \prod_{j=1}^m P \left[ F \in B_m | Z^n = (z_{j,1}, \ldots, z_{j,n}) \right].$$

If $A$ is $(\varepsilon, \delta)$-differentially private, then the algorithm $A^m$ constructed in this way is also $(\varepsilon, \delta)$-differentially private. This follows almost immediately from the fact that the $j$th component of the output of the new algorithm depends only on the $j$th row of the matrix $Z^{m \times n}$.

Another way of combining algorithms is by adaptive composition. Consider two randomized algorithms, $A_1 = P_{F_1|Z^n}$ and $A_2 = P_{F_2|Z^n,F_1}$. Here, the first algorithm takes a dataset $Z^n$ and produces an output $F_1 \in \mathcal{F}_1$; the second algorithm takes a dataset $Z^n$ and an additional $\mathcal{F}_1$-valued input $F_1$ and produces an output $F_2 \in \mathcal{F}_2$. The adaptive composition of $A_1$ and $A_2$ takes $Z^n$ as input and produces an output $F_2 \in \mathcal{F}_2$ using a two-stage procedure:

- Generate $F_1$ by running $A_1$ on $Z^n$.
- Generate $F_2$ by running $A_2$ on $Z^n$ and on $F_1$ generated by $A_1$.

Suppose that $A_1$ is $(\varepsilon_1, \delta_1)$-differentially private, and that, for each $f_1 \in \mathcal{F}_1$, $P_{F_2|Z^n,F_1=f_1}$ is $(\varepsilon_2, \delta_2)$-differentially private. Then their adaptive composition is $(\varepsilon_1 + \varepsilon_2, \delta_1 + \delta_2)$-differentially private. We will now prove this: Fix an arbitrary function $g : \mathcal{F}_2 \rightarrow [0, 1]$ and two datasets
\[ z^n, z'^m \text{ that differ in only one sample, and write} \]
\[
\int_{\mathcal{F}_2} g(f_2)P_{F_1,F_2|Z^n=zn}(df_1, df_2) = \int_{\mathcal{F}_1} \left( \int_{\mathcal{F}_2} g(f_2)P_{F_2|Z^n=zn,F_1=f_1}(df_2) \right) P_{F_1|Z^n=zn}(df_1) \\
\leq \int_{\mathcal{F}_1} \min \left( 1, e^{\varepsilon_2} \int_{\mathcal{F}_2} g(f_2)P_{F_2|Z^n=zn,F_1=f_1}(df_2) + \delta_2 \right) P_{F_1|Z^n=zn}(df_1) \\
= \int_{\mathcal{F}_1} \min \left( 1, e^{\varepsilon_1} \int_{\mathcal{F}_2} g(f_2)P_{F_2|Z^n=zn,F_1=f_1}(df_2) \right) P_{F_1|Z^n=zn}(df_1) + \delta_2, \tag{11.78}
\]
where we have used the differential privacy assumption on \( A_2 \). Now, for a fixed realization \( z^n \), we can define the function
\[
g'(f_1) := \min \left( 1, e^{\varepsilon_2} \int_{\mathcal{F}_2} g(f_2)P_{F_2|Z^n=zn,F_1=f_1}(df_2) \right)
\]
that takes values in \([0,1]\). Therefore, by the differential privacy assumption on \( A_1 \),
\[
\int_{\mathcal{F}_1} \min \left( 1, e^{\varepsilon_2} \int_{\mathcal{F}_2} g(f_2)P_{F_2|Z^n=zn,F_1=f_1}(df_2) \right) P_{F_1|Z^n=zn}(df_1) \\
= \int_{\mathcal{F}_1} g'(f_1)P_{F_1|Z^n=zn}(df_1) \\
\leq e^{\varepsilon_1} \int_{\mathcal{F}_1} g'(f_1)P_{F_1|Z^n=zn}(df_1) + \delta_1 \\
\leq e^{\varepsilon_1+\varepsilon_2} \int_{\mathcal{F}_1} \int_{\mathcal{F}_2} g(f_2)P_{F_1,F_2|Z^n=zn}(df_1, df_2) + \delta_1. \tag{11.79}
\]
Using the bound (11.79) in (11.78), we obtain
\[
\mathbb{E}[g(F_2)|Z^n = zn] \leq e^{\varepsilon_1+\varepsilon_2} \mathbb{E}[g(F_2)|Z^n = zm] + (\delta_1 + \delta_2).
\]
Since \( g \) was arbitrary, we have established the desired differential privacy property.

Finally, we will need a particular differentially private algorithm, the so-called exponential mechanism of McSherry and Talwar [MT07]. Suppose that we are given a function \( U : S \times Z^n \to \mathbb{R} \), where \( S \) is a finite set, such that
\[
\max_{s \in S} |U(s, z^n) - U(s, z'^m)| \leq 1
\]
for all \( z^n, z'^m \) that differ in only one sample. Consider a randomized algorithm that takes input \( Z^n \) and generates an output \( S \) taking values in \( S \) according to the following distribution:
\[
P_{S|Z^n=zn}(s) = \frac{e^{\varepsilon U(s,z^n)/2}}{\sum_{s' \in S} e^{\varepsilon U(s',z^n)/2}}. \tag{11.80}
\]
We have the following:

**Lemma 11.6.** The exponential algorithm (11.80) has the following properties:

1. It is \( \varepsilon \)-differentially private.
2. Let \( U^*(zn) := \max_{s \in S} U(s, z^n) \). Then, for any \( t \),
\[
P \left[ U(S, Z^n) < U^*(Z^n) - t | Z^n = zn \right] \leq |S|e^{-\varepsilon t/4}. \tag{11.81}
\]
PROOF. For part 1, fix $z^n, z'^n$ differing in only one sample. Then we have
\[
\frac{P[S = s | Z^n = z^n]}{P[S = s | Z^n = z'^n]} = \frac{e^{\varepsilon U(s, z^n)/2} \sum_{s' \in S} e^{\varepsilon U(s', z^n)/2}}{e^{\varepsilon U(s, z'^n)/2} \sum_{s' \in S} e^{\varepsilon U(s', z'^n)/2}}
\]
\[
= \exp \left( \frac{\varepsilon (U(s, z^n) - U(s, z'^n))}{2} \right) \frac{\sum_{s' \in S} e^{\varepsilon U(s', z^n)/2}}{\sum_{s' \in S} e^{\varepsilon U(s', z'^n)/2}}
\]
\[
\leq e^{\varepsilon/2} |S| e^{(\varepsilon/2) \max_{s \in S} U(s, z^n)}
\]
\[
\leq e^{\varepsilon/2} \cdot \exp \left( \frac{\varepsilon}{2} \cdot \max_{s \in S} |U(s, z^n) - U(s, z'^n)| \right)
\]
\[
\leq e^{\varepsilon}.
\]

For part 2: for each $t$, define the set
\[
S_t := \{ s \in S : U(s, z^n) \geq U^*(z^n) - t \}.
\]
Then
\[
P \left[ S \in S_t | Z^n = z^n \right] = \frac{\sum_{s \in S_t} e^{\varepsilon U(s, z^n)/2}}{\sum_{s \in S} e^{\varepsilon U(s, z^n)/2}}
\]
\[
= \frac{\sum_{s \in S_t} e^{\varepsilon U(s, z^n)/2}}{\sum_{s \in S_{t/2}} e^{\varepsilon U(s, z^n)/2} + \sum_{s \in S_{t/2}} e^{\varepsilon U(s, z'^n)/2}}
\]
\[
\leq \frac{\sum_{s \in S_t} e^{\varepsilon U(s, z^n)/2}}{\sum_{s \in S_{t/2}} e^{\varepsilon U(s, z^n)/2}}
\]
\[
\leq e^{(\varepsilon/2)(U^*(z^n) - t)} e^{-(\varepsilon/2)(U^*(z^n) - t/2)} |S_t|
\]
\[
\leq |S| e^{-\varepsilon t/4}.
\]

\[\square\]

Finally, we need the following result, due to Nissim and Stemmer [NS15]:

**Lemma 11.7.** Let the parameters $\varepsilon, \delta$ be such that $0 < \delta \leq \varepsilon \leq \frac{1}{5}$ and $m = \frac{\varepsilon}{\delta}$ is an integer. Consider an algorithm $B$ that takes an input $Z_{m \times n}$ and outputs a pair $(F_j, J) \in \mathcal{F} \times \{1, \ldots, m\}$. If $B$ is $(\varepsilon, \delta)$-differentially private, then

\[(11.82) \quad P \left[ L_n^{(j)}(F_j) \leq L(F_j) + 5\varepsilon \right] \geq \varepsilon.\]

*Here, for each $j \in \{1, \ldots, m\}$, $L_n^{(j)}(f)$ denotes the empirical loss of $f \in \mathcal{F}$ on the $j$th row of the matrix $Z_{m \times n}$.***

**Proof.** We first derive a version of this result that holds in expectation. Let $Z_{m \times n}'$ be an independent copy of $Z_{m \times n}$, and let $Z_{m \times n}''$ be obtained from $Z_{m \times n}'$ by replacing the sample $Z_{ji}$ in the $j$th row and the $i$th column with $Z_{ji}'$.  

\[148\]
Now, we write

\[
\mathbb{E} \left[ L_n^{(j)}(F_j) \right] = \sum_{j=1}^{m} \mathbb{E} \left[ L_n^{(j)}(F_j) \mathbf{1}\{J = j\} \right]
\]

\[
= \frac{1}{n} \sum_{j=1}^{m} \sum_{i=1}^{n} \mathbb{E} \left[ \ell(F_j, Z_{ji}) \mathbf{1}\{J = j\} \right]
\]

\[
= \frac{1}{n} \sum_{j=1}^{m} \sum_{i=1}^{n} \int P_{Z_{m \times n}}(dz_{m \times n}) \int P_{Z_{m \times n}}(dz'_{m \times n}) \int P_{(F_j, J)}|Z_{m \times n} = z_{m \times n}}(df_j, j) \ell(f_j, z_{ji})
\]

(11.83)

\[
= \frac{1}{n} \sum_{j=1}^{m} \sum_{i=1}^{n} \int P_{Z_{m \times n}}(dz_{m \times n}) \int P_{Z_{m \times n}}(dz'_{m \times n}) \int P_{(F_j, J)}|Z_{m \times n} = z_{m \times n}}(df_j, j) \ell(f_j, z'_{ji}),
\]

where in the last line we have used the assumption that the entries of $Z_{m \times n}$ and $Z'_{m \times n}$ are i.i.d. draws from the same distribution. Since $P_{(F_j, J)}|Z_{m \times n}$ is $(\varepsilon, \delta)$-differentially private, we have

\[
\int P_{(F_j, J)}|Z_{m \times n} = z_{m \times n}}(df_j, j) \ell(f_j, z'_{ji}) \leq e^\varepsilon \int P_{(F_j, J)}|Z_{m \times n} = z_{m \times n}}(df_j, j) \ell(f_j, z_{ji}) + \delta.
\]

Averaging with respect to $Z_{m \times n}$ and $Z'_{m \times n}$ and exploiting independence, we obtain

\[
\int P_{Z_{m \times n}}(dz_{m \times n}) \int P_{Z'_{m \times n}}(dz'_{m \times n}) \int P_{(F_j, J)}|Z_{m \times n} = z_{m \times n}}(df_j, j) \ell(f_j, z'_{ji})
\]

\[
\leq e^\varepsilon \int P_{Z_{m \times n}}(dz_{m \times n}) \int P_{Z'_{m \times n}}(dz'_{m \times n}) \int P_{(F_j, J)}|Z_{m \times n} = z_{m \times n}}(df_j, j) \ell(f_j, z_{ji}) + \delta
\]

\[
= e^\varepsilon \mathbb{E} \left[ \ell(F_j, Z'_{ji}) \mathbf{1}\{J = j\} \right] + \delta
\]

\[
= e^\varepsilon \mathbb{E} \left[ L(F_j) \mathbf{1}\{J = j\} \right] + \delta.
\]

Substituting this into (11.83), we obtain

(11.84) \quad \mathbb{E} \left[ L_n^{(j)}(F_j) \right] \leq e^\varepsilon \mathbb{E} \left[ L(F_j) \right] + m\delta \leq \mathbb{E} \left[ L(F_j) \right] + 2\varepsilon + m\delta \leq \mathbb{E} \left[ L(F_j) \right] + 3\varepsilon,

where the second step follows from the inequality $ae^x \leq 2x + a$ for $a, x \in [0, 1]$. The probability bound (11.82) follows from Lemma 11.9 in the Appendix. \hfill \square

Now we are ready to state and prove the main result of this section:

**Theorem 11.7** (Nissim–Stemmer). Let the parameters $\varepsilon, \delta$ be such that $0 < \delta \leq \varepsilon \leq \frac{1}{10}$ and $m = \frac{\varepsilon}{\delta}$ is an integer. Let $A = P_{F \times Z_n}$ be an $(\varepsilon, \delta)$-differentially private randomized learning algorithm operating on a sample of size $n \geq \frac{4}{\varepsilon^2} \log \frac{8}{\delta}$. Assume that $\varepsilon \geq \delta$. Then, for any loss function $\ell : \mathcal{F} \times \mathcal{Z} \rightarrow [0, 1]$,

(11.85) \quad \mathbb{P} \left[ |L_n(F) - L(F)| > 13\varepsilon \right] \leq \frac{2\delta}{\varepsilon} \log \frac{2}{\varepsilon}.

149
6.1. The proof of Theorem 11.7. Suppose, to the contrary, that \( A \) does not generalize, i.e., that

\[
\begin{align*}
\Pr[L_n(F) - L(F) > 13\varepsilon] &> \frac{\delta}{\varepsilon} \log \frac{2}{\varepsilon}.
\end{align*}
\]

Draw \( m + 1 \) independent datasets \((Z_{j,1}, \ldots, Z_{j,n}), \, j \in \{1, \ldots, m+1\}\), from \( P_Z \), and form the \((m + 1) \times n\) matrix

\[
Z^{(m+1)\times n} = \begin{pmatrix}
Z_{1,1} & Z_{1,2} & \cdots & Z_{1,n} \\
Z_{2,1} & Z_{2,2} & \cdots & Z_{2,n} \\
\vdots & \vdots & \ddots & \vdots \\
Z_{m,1} & Z_{m,2} & \cdots & Z_{m,n} \\
Z_{m+1,1} & Z_{m+1,2} & \cdots & Z_{m+1,n}
\end{pmatrix}.
\]

Think of the first \( m \) rows of this matrix as \( m \) independent training sets, and of the last row as a separate validation set. For \( j \in \{1, \ldots, m\} \), let \( F_j \in \mathcal{F} \) be the output of an independent copy of \( A \) on the \( j \)th row of this matrix. Next, for each \( f \in \mathcal{F} \), define the empirical losses

\[
L_n^{(j)}(f) := \frac{1}{n} \sum_{i=1}^{n} \ell(f, Z_{j,i}), \quad j \in \{1, \ldots, m+1\}
\]

of \( f \) on the \( j \)th training set and on the validation set. For the random set \( \mathcal{S} = \{(F_j, j)\}_{j=1}^{m} \), define a function \( U : \mathcal{S} \times Z^{(m+1)\times n} \to \mathbb{R} \) by

\[
U((F_j, j), z^{(m+1)\times n}) := n \left( L_n^{(j)}(F_j) - L_n^{(m+1)}(F_j) \right)
\]

and generate a random pair \((F_I, I) \in \mathcal{S}\) by running the McSherry–Talwar exponential algorithm (11.80) with this function \( U \) on \( Z^{(m+1)\times n} \).

For \( j \in \{1, \ldots, m\} \), denote by \( E_j \) the event \( \{L_n^{(j)}(F_j) - L(F_j) > 13\varepsilon\} \), and let \( E = \bigcup_{j=1}^{m} E_j \). By hypothesis, cf. Eq. (11.86), \( \Pr[E_j] > \frac{\delta}{\varepsilon} \log \frac{2}{\varepsilon} \) for each \( j \). Since the events \( E_1, \ldots, E_m \) are independent,

\[
\Pr[E^c] = \Pr\left[\bigcap_{j=1}^{m} E_j^c\right] = \prod_{j=1}^{m} \Pr[E_j^c] \leq \left(1 - \frac{\delta}{\varepsilon} \log \frac{2}{\varepsilon}\right)^m \leq \left(1 - \frac{\delta}{\varepsilon} \log \frac{2}{\varepsilon}\right)^{\varepsilon/\delta} \leq \varepsilon^2.
\]

Next, for each \( j \in \{1, \ldots, m\} \), let \( G_j \) denote the event that \( |L_n^{(m+1)}(F_j) - L(F_j)| \leq \varepsilon \), and let \( G = \bigcap_{j=1}^{m} G_j \). On the other hand, since \( F_1, \ldots, F_m \) are independent of the last row of the matrix \( Z^{(m+1)\times n} \), Hoeffding’s lemma and the union bound guarantee that

\[
\Pr[G] \geq 1 - 2m e^{-2n\varepsilon^2} = 1 - \frac{2\varepsilon}{\delta} e^{-2n\varepsilon^2}.
\]

By the union bound,

\[
\Pr[E \cap G] = 1 - \Pr[E^c \cup G^c] \geq 1 - (\Pr[E^c] + \Pr[G^c]) \geq 1 - \frac{2\varepsilon}{\delta} e^{-2n\varepsilon^2} - \varepsilon.
\]

Consequently, if we choose \( n \geq \frac{1}{2\varepsilon^2} \log \frac{8}{\delta} \), then we will have \( \Pr[E \cap G] \geq 1 - \frac{\delta}{4} \varepsilon \).
Now, on the event $E \cap G$, the function $U$ defined in (11.87) will satisfy
\[
U^*(Z^{(m+1)\times n}) = \max_{j \in \{1, \ldots, m\}} U(j, Z^{(m+1)\times n})
\]
\[
= n \max_{j \in \{1, \ldots, m\}} [L_n^{(j)}(F_j) - L_n^{(m+1)}(F_j)]
\]
\[
= n \max_{j \in \{1, \ldots, m\}} [(L_n^{(j)}(F_j) - L(F_j)) + (L(F_j) - L_n^{(m+1)}(F_j))]
\]
\[
\geq 12n\varepsilon.
\]

Therefore, on the event $E \cap G$, with probability at least $1 - me^{-n\varepsilon^2/4}$, the output $(F_I, I)$ the exponential mechanism with (11.87) will be such that
\[
L(I)_{n(F_I)} - L(F_I) = L(I)_{n(F_I)} - L(F_I) + L_n^{(m+1)}(F_I) - L(F_I)
\]
\[
\geq \frac{U^*(Z^{(m+1)\times n})}{n} - 2\varepsilon > 10\varepsilon.
\]

Thus, if $n$ is also chosen to be larger then \(\frac{1}{\varepsilon} \log \frac{8}{\delta}\), then the output $(F_I, I)$ will satisfy
\[
P[L_n^{(j)}(F_I) \leq L(F_I) + 10\varepsilon] \leq \varepsilon.
\]

(11.88)

By Lemma 11.7, this is impossible if we can show that the algorithm $B = P_{(F_J, J) \mid Z^{(m+1)\times n}}$ is $(2\varepsilon, \delta)$-differentially private.

To see this, we observe that the algorithm $B = P_{(F_J, J) \mid Z^{(m+1)\times n}}$ is an adaptive composition of $A^m$ and the McSherry–Talwar algorithm. Since $A$ is $(\varepsilon, \delta)$-differentially private, so is $A^m$, and the McSherry–Talwar algorithm is $(\varepsilon, 0)$-differentially private. Therefore, $B$ is $(2\varepsilon, \delta)$-differentially private. Therefore, by Lemma 11.7, its output must satisfy
\[
P[L_n^{(j)}(F_J) \leq L(F_J) + 10\varepsilon] \geq 2\varepsilon.
\]

which contradicts (11.88).

### 7. Technical lemmas

**Lemma 11.8.** Let $U$ and $V$ be two random variables, such that $U \leq V$ almost surely. Then
\[
E[U] \leq |E[U]| + 2E|V|.
\]

**Proof.** We have
\[
\]

**Lemma 11.9.** Let $U$ and $V$ be two random variables, such that $0 \leq U, V \leq 1$ almost surely, and
\[
E[U] \leq E[V] + 3\varepsilon
\]
for some $0 \leq \varepsilon \leq \frac{1}{5}$. Then
\[
P[U \leq V + 5\varepsilon] \geq \varepsilon.
\]
Proof. Suppose, by way of contradiction, that $P[U \leq V + 5\varepsilon] < \varepsilon$. Then

\[
E[U] = E[U1\{U - V \leq 5\varepsilon\}] + E[U1\{U - V > 5\varepsilon\}] \\
> E[(5\varepsilon + V)1\{U - V > 5\varepsilon\}] \\
= (5\varepsilon)P[U - V > 5\varepsilon] + E[V1\{U - V > 5\varepsilon\}].
\]

On the other hand, since $0 \leq V \leq 1$

\[
E[V1\{U - V \leq 5\varepsilon\}] \leq E[1\{U - V \leq 5\varepsilon\}] = P[U - V \leq 5\varepsilon] < \varepsilon.
\]

Therefore,

\[
E[U] > (5\varepsilon)P[U - V > 5\varepsilon] + E[V] - \varepsilon \\
> (5\varepsilon)(1 - \varepsilon) + E[V] - \varepsilon \\
= E[V] + 4\varepsilon - 5\varepsilon^2 \\
\geq E[V] + 3\varepsilon,
\]

which contradicts the assumption that $E[U] \leq E[V] + 3\varepsilon$. \qed
CHAPTER 12

Minimax lower bounds

Now that we have a good handle on the performance of ERM and its variants, it is time to ask whether we can do better. For example, consider binary classification: we observe $n$ i.i.d. training samples from an unknown joint distribution $P$ on $X \times \{0, 1\}$, where $X$ is some feature space, and for a fixed class $\mathcal{F}$ of candidate classifiers $f : X \to \{0, 1\}$ we let $\hat{f}_n$ be the ERM solution

$$\hat{f}_n = \arg\min_{f \in \mathcal{F}} \frac{1}{n} \sum_{i=1}^{n} 1_{\{f(X_i) \neq Y_i\}}.$$  

(12.1)

If $\mathcal{F}$ is a VC class with VC dimension $V$, then the excess risk of $\hat{f}_n$ over the best-in-class performance $L^*(\mathcal{F}) \equiv \inf_{f \in \mathcal{F}} L(f)$ satisfies

$$L(\hat{f}_n) \leq L^*(\mathcal{F}) + C \left( \sqrt{\frac{V}{n}} + \sqrt{\frac{\log(1/\delta)}{n}} \right)$$

with probability at least $1 - \delta$, where $C > 0$ is some absolute constant. Integrating, we also get the following bound on the expected excess risk:

$$\mathbb{E} \left[ L(\hat{f}_n) - L^*(\mathcal{F}) \right] \leq C \sqrt{\frac{V}{n}},$$  

(12.2)

for some constant $C > 0$. Crucially, the bound (12.2) holds for all possible joint distributions $P$ on $X \times \{0, 1\}$, and the right-hand side is independent of $P$ — it depends only on the properties of the class $\mathcal{F}$! Thus, we deduce the following remarkable distribution-free guarantee for ERM: for any VC class $\mathcal{F}$, the ERM algorithm (12.1) satisfies

$$\sup_{P \in \mathcal{P}(X \times \{0, 1\})} \mathbb{E}_P \left[ L_P(\hat{f}_n) - L_P^*(\mathcal{F}) \right] \leq C \sqrt{\frac{V}{n}}.$$  

(12.3)

(We have used subscript $P$ to explicitly indicate the fact that the quantity under the supremum depends on the underlying distribution $P$. In the sequel, we will often drop the subscript to keep the notation uncluttered.) Let’s take a moment to reflect on the significance of the bound (12.3). What it says is that, regardless of how “weird” the stochastic relationship between the feature $X \in X$ and the label $Y \in \{0, 1\}$ might be, as long as we scale our ambition back and aim at approaching the performance of the best classifier in some VC class $\mathcal{F}$, the ERM algorithm will produce a good classifier with a uniform $O(\sqrt{V/n})$ guarantee on its excess risk.

At this point, we stop and ask ourselves: could this bound be too pessimistic, even when we are so lucky that the optimal (Bayes) classifier happens to be in $\mathcal{F}$? (Recall that the
Bayes classifier for a given $P$ has the form

$$f^*(x) = \begin{cases} 1, & \text{if } \eta(x) \geq 1/2 \\ 0, & \text{otherwise} \end{cases},$$

where $\eta(x) = \mathbb{E}[Y|X = x] = \mathbb{P}(Y = 1|X = x)$ is the regression function. Let $\mathcal{P}(\mathcal{F})$ denote the subset of $\mathcal{P}(X \times \{0, 1\})$ consisting of all joint distributions of $X \in X$ and $Y \in \{0, 1\}$, such that $f^* \in \mathcal{F}$. Then from (12.2) we have

$$\sup_{P \in \mathcal{P}(\mathcal{F})} \mathbb{E} \left[ L(\hat{f}_n) - L(f^*) \right] \leq C \sqrt{\frac{V}{n}},$$

(12.4)

where $\hat{f}_n$ is the ERM solution (12.1). However, we know that if the relationship between $X$ and $Y$ is deterministic, i.e., if $Y = f^*(X)$, then ERM performs much better. More precisely, let $\mathcal{P}_0(\mathcal{F})$ be the zero-error class:

$$\mathcal{P}_0(\mathcal{F}) := \{ P \in \mathcal{P}(\mathcal{F}) : Y = f^*(X) \ \text{a.s.} \}.$$

Then one can show that

$$\sup_{P \in \mathcal{P}_0(\mathcal{F})} \mathbb{E} \left[ L(\hat{f}_n) - L(f^*) \right] \leq C \frac{V}{n},$$

(12.5)

a much better bound than the “global” bound (12.4) (see, e.g., the book by Vapnik [Vap98]).

This suggests that the performance of ERM is somehow tied to how “sharp” the behavior of $\eta$ is around the decision boundary that separates the sets $\{x \in X : \eta(x) \geq 1/2\}$ and $\{x \in X : \eta(x) < 1/2\}$. To see whether this is the case, let us define, for any $h \in [0, 1]$, the class of distributions

$$\mathcal{P}(h, \mathcal{F}) := \{ P \in \mathcal{P}(\mathcal{F}) : |2\eta(X) - 1| \geq h \ \text{a.s.} \}.$$

(12.6)

From that case, the distributions in $\mathcal{P}(h, \mathcal{F})$ are said to satisfy the Massart noise condition with margin $h$.) We have already seen the two extreme cases:

- $h = 0$ — this gives $\mathcal{P}(0, \mathcal{F}) = \mathcal{P}(\mathcal{F})$ (the bound $|2\eta - 1| \geq 0$ holds trivially for any $P$).
- $h = 1$ — this gives the zero-error regime $\mathcal{P}(1, \mathcal{F}) = \mathcal{P}_0(\mathcal{F})$ (if $|2\eta - 1| \geq 1$ a.s., then $\eta$ can take only values 0 and 1 a.s.).

However, intermediate values of $h$ are also of interest: if a distribution $P$ belongs to $\mathcal{P}(h, \mathcal{F})$ for some $0 < h < 1$, then its regression function $\eta$ makes a jump of size $h$ as we cross the decision boundary. With this in mind, for any $n \in \mathbb{N}$ and $h \in [0, 1]$ let us define the minimax risk

$$R_n(h, \mathcal{F}) := \inf_{\hat{f}_n} \sup_{P \in \mathcal{P}(h, \mathcal{F})} \mathbb{E} \left[ L(\hat{f}_n) - L(f^*) \right],$$

(12.7)

where the infimum is over all learning algorithms $\hat{f}_n$ based on $n$ i.i.d. training samples. The term “minimax” indicates that we are minimizing over all admissible learning algorithms, while maximizing over all distributions in a given class. The following result was proved by Pascal Massart and Élodie Nédélec [MN06]:

154
Theorem 12.1. Let $\mathcal{F}$ be a VC class of binary-valued functions on $X$ with VC dimension $V \geq 2$. Then for any $n \geq V$ and any $h \in [0, 1]$ we have the lower bound

$$R_n(h, \mathcal{F}) \geq c \min \left( \sqrt{\frac{V}{n}}, \frac{V}{nh} \right),$$

where $c > 0$ is some absolute constant.

Let us examine some implications:

- When $h = 0$, the right-hand side of (12.7) is equal to $c\sqrt{V/n}$. Thus, without any further assumptions, ERM is as good as it gets (it is minimax-optimal), up to multiplicative constants.

- When $h = 1$ (the zero-error case), the right-hand side of (12.7) is equal to $cV/n$, which matches the upper bound (12.5) up to constants. Thus, if we happen to know that we are in a zero-error situation, ERM is minimax-optimal as well.

- For intermediate values of $h$, the lower bound depends on the relative sizes of $h$, $V$, and $n$. In particular, if $h \geq \sqrt{V/n}$, we have the minimax lower bound $R_n(h, \mathcal{F}) \geq cV/nh$. Alternatively, for a fixed $h \in (0, 1)$, we may think of $n^* = \lceil V/h^2 \rceil$ as the cutoff sample size, beyond which the effect of the margin condition on $\eta$ can be “spotted” and exploited by a learning algorithm.

- In the same paper, Massart and Nédélec obtain the following upper bound on ERM:

$$\sup_{P \in \mathcal{P}(h, \mathcal{F})} \mathbb{E} \left[ L(\hat{f}_n) - L(f^*) \right] \leq \begin{cases} C\sqrt{\frac{V}{n}}, & \text{if } h \leq \sqrt{V/n} \\ C \frac{V}{nh} \left( 1 + \log \frac{nh^2}{V} \right), & \text{if } h > \sqrt{V/n} \end{cases}.$$  

Thus, ERM is nearly minimax-optimal (we say “nearly” because of the extra log factor in the above bound; in fact, as Massart and Nédélec show, the log factor is unavoidable when the function class $\mathcal{F}$ is “rich” in a certain sense). The proof of the above upper bound is rather involved and technical, and we will not get into it here.

The appearance of the logarithmic term in (12.8) is rather curious. Given the lower bound of Theorem 12.1, one may be tempted to dismiss it as an artifact of the analysis used by Massart and Nédélec. However, as we will now see, in certain situations this logarithmic term is unavoidable. To that end, we first need a definition: We say that a class $\mathcal{F}$ binary-valued functions $f : X \to \{0, 1\}$ is $(N, D)$-rich, for some $N, D \in \mathbb{N}$, if there exist $N$ distinct points $x_1, \ldots, x_N \in X$, such that the projection

$$\mathcal{F}(x^N) = \left\{ (f(x_1), \ldots, f(x_N)) : f \in \mathcal{F} \right\}$$

of $\mathcal{F}$ onto $x^N$ contains all binary strings of Hamming weight\(^1\) $D$. Some examples:

- If $\mathcal{F}$ is a VC-class with VC dimension $V$, then it is $(V, D)$-rich for all $1 \leq D \leq V$. This follows directly from definitions.

\(^1\)The Hamming weight of a binary string is the number of nonzero bits it has.
• A nontrivial example, and one that is relevant to statistical learning, is as follows. Let \( \mathcal{F} \) be the collection of indicators of all halfspaces in \( \mathbb{R}^d \), for some \( d \geq 2 \). There is a result in computational geometry which says that, for any \( N \geq d + 1 \), one can find \( N \) distinct points \( x_1, \ldots, x_N \), such that \( \mathcal{F}(x^n) \) contains all strings in \( \{0, 1\}^N \) with Hamming weight up to, and including, \( \lfloor d/2 \rfloor \). Consequently, \( \mathcal{F} \) is \((N, \lfloor d/2 \rfloor)\)-rich for all \( N \geq d + 1 \).

We can now state the following result [MN06]:

**Theorem 12.2.** Given some \( D \geq 1 \), suppose that \( \mathcal{F} \) is \((N, D)\)-rich for all \( N \geq 4D \). Then

\[
R_n(h, \mathcal{F}) \geq c(1 - h) \frac{D}{nh} \left[ 1 + \log \frac{nh^2}{D} \right]
\]

for any \( \sqrt{D/n} \leq h < 1 \), where \( c > 0 \) is some absolute constant.

We will present the proofs of Theorems 12.1 and 12.2 in Sections 2 and 3, after giving some necessary background on minimax lower bounds.

1. Preparation: minimax lower bounds for statistical estimation

To prove Theorem 12.1, we need some background on minimax lower bounds for statistical estimation problems. The presentation here follows an excellent paper by Bin Yu [Yu97].

The setting is as follows: we have an indexed set \( \{P_\theta : \theta \in \Theta\} \) of probability distributions on some set \( Z \), where \( \Theta \) is some parameter set. For our purposes, it suffices to consider the case when \( Z \) is a finite set. We observe a random sample \( Z \) from one of the \( P_\theta \)'s, and our goal is to estimate \( \theta \). We will measure the quality of any estimator \( \hat{\theta} = \hat{\theta}(Z) \) by its expected risk

\[
E_\theta[d(\theta, \hat{\theta}(Z))] = \sum_{z \in Z} P_\theta(z)d(\theta, \hat{\theta}(z)),
\]

where \( E_\theta[\cdot] \) denotes expectation with respect to \( P_\theta \), and \( d : \Theta \times \Theta \to \mathbb{R}^+ \) is a given loss function. Here, we will assume that \( d \) is a pseudometric on \( \Theta \), i.e., it has the following properties:

1. Symmetry – \( d(\theta, \theta') = d(\theta', \theta) \) for any \( \theta, \theta' \in \Theta \).
2. Triangle inequality – \( d(\theta, \theta') \leq d(\theta, \eta) + d(\eta, \theta') \) for any \( \theta, \theta', \eta \in \Theta \).

(We do not require that \( d(\theta, \theta') = 0 \) if and only if \( \theta = \theta' \), in which case \( d \) is a metric.) Since we do not know ahead of time which of the \( \theta \)'s we will be facing, it is natural to expect the worst and seek an estimator \( \hat{\theta} \) to minimize the worst-case risk \( \sup_{\theta \in \Theta} E_\theta[d(\theta, \hat{\theta}(Z))] \). With this in mind, let us define the minimax risk

\[
\mathcal{M}(\Theta) := \inf_{\hat{\theta}} \sup_{\theta \in \Theta} E_\theta[d(\theta, \hat{\theta}(Z))],
\]

where the infimum is over all estimators \( \hat{\theta} = \hat{\theta}(Z) \). We are particularly interested in tight lower bounds on \( \mathcal{M}(\Theta) \), since they will give us some idea of how difficult the estimation problem is.

A simple yet powerful technique for getting lower bounds is the two-point method introduced by Lucien Le Cam:
Lemma 12.1. For any two \( \theta, \theta' \in \Theta \) and any estimator \( \hat{\theta} \),

\[
E_{\theta}[d(\theta, \hat{\theta}(Z))] + E_{\theta'}[d(\theta', \hat{\theta}(Z))] \geq d(\theta, \theta') \cdot \sum_{z \in Z} \min(P_{\theta}(z), P_{\theta'}(z)).
\] (12.10)

Proof. Consider an arbitrary \( z \in Z \). If \( P_\theta(z) \leq P_{\theta'}(z) \), then

\[
P_\theta(z)d(\theta, \hat{\theta}(z)) + P_{\theta'}d(\theta', \hat{\theta}(z)) = P_\theta(z) \left[ d(\theta, \hat{\theta}(z)) + d(\theta', \hat{\theta}(z)) \right] + [P_{\theta'}(z) - P_\theta(z)] d(\theta', \hat{\theta}(z))
\]
\[
\geq P_\theta(z) \left[ d(\theta, \hat{\theta}(z)) + d(\theta', \hat{\theta}(z)) \right]
\]
\[
\geq P_\theta(z)d(\theta, \theta'),
\]
where the second line is because \( P_{\theta'}(z) \geq P_\theta(z) \) and \( d(\cdot, \cdot) \) is nonnegative, while the third line is by the triangle inequality. By the same token, if \( P_\theta(z) \geq P_{\theta'}(z) \), then

\[
P_\theta(z)d(\theta, \hat{\theta}(z)) + P_{\theta'}d(\theta', \hat{\theta}(z)) \geq P_{\theta'}(z)d(\theta, \theta').
\]

Summing over all \( z \in Z \), we get (12.10). \( \square \)

The sum on the right-hand side of (12.10) can be expressed in terms of the so-called total variation distance between \( P_\theta \) and \( P_{\theta'} \). For any two probability distributions \( P, Q \in \mathcal{P}(Z) \), the total variation distance is

\[
\|P - Q\|_{TV} := \frac{1}{2} \sum_{z \in Z} |P(z) - Q(z)|.
\] (12.11)

Moreover,

\[
\|P - Q\|_{TV} = 1 - \sum_{z \in Z} \min(P(z), Q(z)).
\] (12.12)
To prove (12.12), we just use the definition (12.11): if we let \( M := \{ z \in Z : P(z) \geq Q(z) \} \), then
\[
\| P - Q \|_{TV} = \frac{1}{2} \sum_{z \in M} (P(z) - Q(z)) + \frac{1}{2} \sum_{z \in M^c} (Q(z) - P(z))
\]
\[
= \frac{1}{2} (P(M) - Q(M)) + \frac{1}{2} (Q(M^c) - P(M^c))
\]
\[
= \frac{1}{2} (P(M) - Q(M)) + \frac{1}{2} (P(M) - Q(M))
\]
\[
= P(M) - Q(M)
\]
\[
= \sum_{z : P(z) \geq Q(z)} (P(z) - Q(z))
\]
\[
= \sum_{z : P(z) \geq Q(z)} (P(z) - \min(P(z), Q(z)))
\]
\[
= \sum_{z \in Z} \min(P(z), Q(z)) - \sum_{z \in Z} \min(P(z), Q(z))
\]
\[
= 1 - \sum_{z \in Z} \min(P(z), Q(z)).
\]
and we are done. Thus, we can rewrite the bound (12.10) as
\[
(12.13) \quad E_\theta[d(\theta, \hat{\theta}(Z))] + E_{\theta'}[d(\theta', \hat{\theta}(Z))] \geq d(\theta, \theta') \cdot (1 - \| P_\theta - P_{\theta'} \|_{TV}).
\]
Let us examine some consequences. If we take the supremum of both sides of (12.13) over the choices of \( \theta \) and \( \theta' \), then we see that, for any estimator \( \hat{\theta} \),
\[
(12.14) \quad \sup_{\theta' \in \Theta} E_\theta[d(\theta, \hat{\theta}(Z))] \geq \frac{1}{2} \sup_{\theta', \theta' \neq \theta} \{ d(\theta, \theta') \cdot (1 - \| P_\theta - P_{\theta'} \|_{TV}) \}.
\]
Notice that the right-hand side does not depend on the choice of \( \hat{\theta} \), so we can take the infimum of both sides of (12.14) over \( \hat{\theta} \) and obtain the following:

**Corollary 12.1.** The minimax risk \( \mathcal{M}(\Theta) \) can be lower-bounded as
\[
(12.15) \quad \mathcal{M}(\Theta) \geq \frac{1}{2} \sup_{\theta, \theta' \neq \theta} \{ d(\theta, \theta') \cdot (1 - \| P_\theta - P_{\theta'} \|_{TV}) \}.
\]

The “two-point” bound (12.15) gives us an idea of when the problem of estimating \( \theta \) based on observations \( Z \sim P_\theta \) is difficult: when there exists at least one pair of distinct parameter values \( \theta, \theta' \in \Theta \) such that \( d(\theta, \theta') \) is large, while the total variation distance \( \| P_\theta - P_{\theta'} \|_{TV} \) is small. This means that the observation \( Z \) does not give us enough information to reliably distinguish between \( \theta \) and \( \theta' \), but the consequences of mistaking one for the other are severe (since \( d(\theta, \theta') \) is large).

Another useful consequence of Lemma 12.1 comes about when we consider the Bayesian setting, i.e., when we have a *prior distribution* \( \pi \) on \( \Theta \) and consider the *average risk* of any
estimator \( \hat{\theta} \):
\[
E_{\pi}[d(\theta, \hat{\theta}(Z))] := \int_{\Theta} \pi(d\theta)E_{\theta}[d(\theta, \hat{\theta}(Z))].
\]
Then we have the following lower bound on \( \mathcal{M}(\Theta) \):
\[
\mathcal{M}(\Theta) \geq \inf_{\hat{\theta}} E_{\pi}\left[d(\theta, \hat{\theta}(Z))\right].
\]
To prove this, we simply note that, for any \( \hat{\theta} \),
\[
E_{\pi}[d(\theta, \hat{\theta}(Z))] := \int_{\Theta} \pi(d\theta)E_{\theta}[d(\theta, \hat{\theta}(Z))] \leq \sup_{\theta \in \Theta} E_{\theta}[d(\theta, \hat{\theta})].
\]
(In fact, under suitable regularity conditions, one can prove that the minimax risk is equal to the worst-case Bayes risk:
\[
\mathcal{M}(\Theta) = \inf_{\hat{\theta}} \sup_{\pi \in P(\Theta)} E_{\pi}\left[d(\theta, \hat{\theta}(Z))\right] = \sup_{\pi \in P(\Theta)} \inf_{\hat{\theta}} E_{\pi}\left[d(\theta, \hat{\theta}(Z))\right],
\]
where the first equality always holds, while the second equality is valid whenever the conditions of the minimax theorem are satisfied.) With these definitions, we have the following:\( ^2 \)

**Corollary 12.2.** Let \( \pi \) be any prior distribution on \( \Theta \), and let \( \mu \) be any joint probability distribution of a random pair \((\theta, \theta') \in \Theta \times \Theta\), such that the marginal distributions of both \( \theta \) and \( \theta' \) are equal to \( \pi \). Then
\[
(12.16) \quad \mathcal{M}(\Theta) \geq \inf_{\hat{\theta}} E_{\pi}\left[d(\theta, \hat{\theta}(Z))\right] \geq \frac{1}{2} E_{\mu}[d(\theta, \theta') \cdot (1 - \|P_{\theta} - P_{\theta'}\|_{TV})].
\]

**PROOF.** Take the expectation of both sides of (12.13) with respect to \( \mu \) and then use the fact that, under \( \mu \), both \( \theta \) and \( \theta' \) have the same distribution. \( \square \)

In many cases, the analysis of minimax lower bounds can be reduced to the following problem: Suppose that the parameter set \( \Theta \) can be identified with the \( m \)-dimensional binary hypercube \( \{0, 1\}^m \) for some \( m \), and the objective is to determine every bit of the underlying unknown parameter \( \theta \in \{0, 1\}^m \) based on an observation \( Z \sim P_{\theta} \). In that setting, a key result known as Assouad’s lemma says that the difficulty of estimating the entire bit string \( \theta \) is related to the difficulty of estimating each bit of \( \theta \) separately, assuming you already know all other bits:

**Theorem 12.3 (Assouad’s lemma).** Suppose that \( \Theta = \{0, 1\}^m \) and consider the Hamming metric
\[
(12.17) \quad d_H(\theta, \theta') := \sum_{i=1}^{m} 1_{\{\theta_i \neq \theta'_i\}}.
\]
Then
\[
(12.18) \quad \mathcal{M}(\Theta) \geq \frac{m}{2} \left(1 - \max_{\theta, \theta': d_H(\theta, \theta') = 1} \|P_{\theta} - P_{\theta'}\|_{TV}\right).
\]

\( ^2 \)I have learned this particular formulation from my colleagues Yihong Wu (here at Illinois) and Yury Polyanskiy (MIT).
Proof. Notice that we can write \( d_H(\theta, \theta') \) as a sum \( \sum_{i=1}^{m} d_i(\theta, \theta') \), where \( d_i(\theta, \theta') := 1_{\{\theta_i \neq \theta'_i\}} \), and each \( d_i \) is a pseudometric. Now let \( \pi \) be the uniform distribution on \( \Theta = \{0, 1\}^m \), and for each \( i \in \{1, \ldots, m\} \) let \( \mu_i \) be the joint distribution of a random pair \( (\theta, \theta') \in \Theta \times \Theta \), under which \( \theta \sim \pi \) and \( \theta' \) differs from \( \theta \) only in the \( i \)th bit, i.e., \( \theta \sim \pi \) and \( d_i(\theta, \theta') = 1 \). Then the marginal distribution of \( \theta' \) under \( \mu_i \) is

\[
\sum_{\theta \in \{0, 1\}^m} \mu_i(\theta, \theta') = \frac{1}{2^m} \sum_{\theta \in \{0, 1\}^m} 1_{\{\theta_i \neq \theta'_i \text{ and } \theta_j = \theta'_j, j \neq i\}} = \frac{1}{2^m} = \pi(\theta'),
\]
since for each \( \theta' \) there is only one \( \theta \) that differs from it in a single bit. Now the idea is to apply Corollary 12.2 separately to each bit:

\[
\mathcal{M}(\Theta) = \inf_{\hat{\theta}} E_\pi \left[ d_H(\theta, \hat{\theta}(Z)) \right]
= \inf_{\hat{\theta}} \sum_{i=1}^{m} E_\pi \left[ d_i(\theta, \hat{\theta}(Z)) \right]
\geq \sum_{i=1}^{m} \inf_{\hat{\theta}} E_\pi \left[ d_i(\theta, \hat{\theta}(Z)) \right]
\geq \sum_{i=1}^{m} \frac{1}{2} E_{\mu_i} \left[ d_i(\theta, \theta') \cdot (1 - \|P_\theta - P_{\theta'}\|_{TV}) \right],
\]

where the last step is by Corollary 12.2. Since \( d_i(\theta, \theta') = 1 \) under \( \mu_i \) for every \( i \), we have

\[
\mathcal{M}(\Theta) \geq \frac{1}{2} \sum_{i=1}^{m} E_{\mu_i} [1 - \|P_\theta - P_{\theta'}\|_{TV}]
\geq \frac{1}{2} \sum_{i=1}^{m} \min_{\theta, \theta': d_H(\theta, \theta') = 1} (1 - \|P_\theta - P_{\theta'}\|_{TV})
= \frac{m}{2} \left(1 - \max_{\theta, \theta': d_H(\theta, \theta') = 1} \|P_\theta - P_{\theta'}\|_{TV}\right),
\]

and we are done. \( \square \)

In order to apply Assouad’s lemma, we need to have an upper bound on the total variation distance between any two \( P_\theta \) and \( P_{\theta'} \) with \( d_H(\theta, \theta') = 1 \). More often than not, it is easier to work with another distance between probability distributions, the so-called Hellinger distance. For any two \( P, Q \in \mathcal{P}(Z) \), their squared Hellinger distance is given by

\[
H^2(P, Q) := \frac{1}{2} \sum_{z \in Z} \left(\sqrt{P(z)} - \sqrt{Q(z)}\right)^2.
\]

The total variation distance can be both upper- and lower-bounded by Hellinger:

\[
\frac{1}{2} H^2(P, Q) \leq \|P - Q\|_{TV} \leq H(P, Q).
\]

(12.19)
Moreover, for any \( n \) pairs of distributions \((P_1, Q_1), \ldots, (P_n, Q_n)\),
\[
H^2(P_1 \times \ldots \times P_n, Q_1 \times \ldots \times Q_n) \leq \sum_{i=1}^{n} H^2(P_i, Q_i).
\]

(12.20)

Armed with these facts, we can prove the following version of Assouad’s lemma:

**Corollary 12.3.** Let \( \{P_\theta : \theta \in \{0, 1\}^m\} \) be a collection of probability distributions on some set \( Z \) indexed by the vertices of the binary hypercube \( \Theta = \{0, 1\}^m \). Suppose that there exists some constant \( \alpha > 0 \), such that
\[
H^2(P_\theta, P_{\theta'}) \leq \alpha, \quad \text{if } d_H(\theta, \theta') = 1.
\]

(12.21)

Consider the problem of estimating the parameter \( \theta \in \Theta \) based on \( n \) i.i.d. observations from \( P_\theta \), where the loss is measured by the Hamming distance. Then the corresponding minimax risk, which we denote by \( M_n(\Theta) \), is lower-bounded as
\[
M_n(\Theta) \geq \frac{m}{2} (1 - \sqrt{\alpha n}).
\]

(12.22)

**Proof.** Fix any \( \varepsilon > 0 \)-separated set \( \Theta_0 \subset \Theta \). Then, since \( \Theta_0 \subset \Theta \), we have \( M(\Theta_0) \geq M(\Theta) \). Given any estimator \( \hat{\theta} = \hat{\theta}(Z) \) taking values in \( \Theta \), define another estimator \( \tilde{\theta} = \tilde{\theta}(Z) \) taking
values in $\Theta_0$ as follows:

$$
\tilde{\theta} = \arg \min_{\theta' \in \Theta_0} d(\tilde{\theta}, \theta').
$$

Then, for any $\theta \in \Theta_0$,

$$
d(\tilde{\theta}, \theta) \leq d(\tilde{\theta}, \hat{\theta}) + d(\hat{\theta}, \theta) \leq 2d(\theta, \hat{\theta}),
$$

where the first step is by the triangle inequality, while the second step is by definition of $\tilde{\theta}$. Consequently,

$$(12.24) \quad \mathfrak{M}(\Theta) \geq \mathfrak{M}(\Theta_0) \geq \frac{1}{2} \inf_{\tilde{\theta}} \sup_{\theta \in \Theta_0} E_{\theta}[d(\tilde{\theta}, \theta)].$$

Now let us consider the event $\{z \in Z : \tilde{\theta}(z) \neq \theta\}$ for some $\theta \in \Theta_0$. Since $\tilde{\theta} \in \Theta_0$ by construction, and $\Theta_0$ is $\varepsilon$-separated, we have $\{z \in Z : \tilde{\theta}(z) \neq \theta\} \subseteq \{z \in Z : d(\tilde{\theta}(z), \theta) \geq \varepsilon\}$. Using this fact and Markov’s inequality, we can write

$$(12.25) \quad P_{\theta}(\tilde{\theta} \neq \theta) \leq P_{\theta}(d(\tilde{\theta}, \theta) \geq \varepsilon) \leq \frac{E_{\theta}[d(\tilde{\theta}, \theta)]}{\varepsilon}.$$

Using this in (12.24), we get (12.23).

Lemma 12.2 is at its most effective when we can find a finite set $\Theta_0$ which is $\varepsilon$-separated and has large cardinality. The reason for the latter requirement is that then it should not be too hard to arrange things in such a way that the probability of error $P_{\theta}(\tilde{\theta} \neq \theta)$ is uniformly bounded away from zero for any estimator $\tilde{\theta}$. In particular, if we can find an $\varepsilon$-separated set $\Theta_0 \subset \Theta$, such that

$$
\inf_{\tilde{\theta}} \max_{\theta \in \Theta_0} P_{\theta}(\tilde{\theta} \neq \theta) \geq \alpha
$$

for some absolute constant $\alpha > 0$, then we can lower-bound the minimax risk $\mathfrak{M}(\Theta)$ by $\alpha \varepsilon / 2$. So now we need tight lower bounds on the probability of error when testing multiple hypotheses that hold for any estimation procedure. Bounds of this sort rely, in one way or another, on a fundamental result from information theory known as Fano’s inequality [CT06] (or Fano’s lemma, as statisticians call it [Yu97]). We will use a particular version, due to Lucien Birgé [Bir05]. To state it, we first need to define relative entropy (or Kullback–Leibler divergence). Given any two probability distributions $P, Q$ on $Z$, the relative entropy (or Kullback–Leibler divergence) between $P$ and $Q$ is defined as

$$(12.26) \quad D(P \| Q) := \begin{cases} 
\sum_{z \in Z} P(z) \log \frac{P(z)}{Q(z)}, & \text{if supp}(P) \subseteq \text{supp}(Q) \\
+\infty, & \text{otherwise}
\end{cases}$$

where supp$(P) := \{z \in Z : P(z) > 0\}$ is the support of $P$. Here are some useful properties:

- $D(P \| Q) \geq 0$, with equality if and only if $P \equiv Q$;
- for any $n$ pairs of distributions $(P_i, Q_i)$, $1 \leq i \leq n$, we have

$$(12.27) \quad D(P_1 \times \ldots \times P_n \| Q_1 \times \ldots \times Q_n) = \sum_{i=1}^{n} D(P_i \| Q_i).$$

162
Also, one can bound the total variation distance in terms of the KL divergence as follows:

\begin{equation}
\| P - Q \|_{TV} \leq \sqrt{\frac{1}{2} D(P \| Q)}.
\end{equation}

This inequality is usually referred to as Pinsker’s inequality after Mark S. Pinsker, although Pinsker didn’t prove it. In the present form, the inequality (12.28), with the optimal constant $1/2$ in front of $D(P \| Q)$, was obtained independently by I. Csiszár, J.H.B. Kemperman, and S. Kullback.

With these preliminaries out of the way, we can state Birgé’s bound:

**Lemma 12.3 (Birgé).** Let $\{ P_i \}_{i=0}^N$ be a finite family of probability distributions on $\mathbb{Z}$, and let $\{ A_i \}_{i=0}^N$ be a family of disjoint events. Then

\[ \min_{0 \leq i \leq N} P_i(A_i) \leq \max \left( \alpha, \frac{\bar{K}}{\log(N+1)} \right), \]

where $\alpha = 0.71$ and

\[ \bar{K} = \frac{1}{N} \sum_{i=1}^N D(P_i \| P_0). \]

Now let’s see how we can apply Birgé’s lemma: Let $\Theta_0 = \{ \theta_0, \ldots, \theta_N \}$ be some $\varepsilon$-separated subset of $\Theta$. Fix an estimator $\hat{\theta}$ taking values in $\Theta_0$. For each $0 \leq i \leq N$, consider the probability distribution $P_i = P_{\theta_i}$ and the event $A_i = \{ z \in \mathbb{Z} : \hat{\theta}(z) = \theta_i \}$. Since the elements of $\Theta_0$ are all distinct, the events $A_0, \ldots, A_N$ are disjoint. Now suppose that we have chosen $\Theta_0$ in such a way that

\begin{equation}
\bar{K} = \frac{1}{N} \sum_{i=1}^N D(P_0 \| P_i) = \frac{1}{N} \sum_{i=1}^N D(P_0 \| P_{\theta_i}) \leq \alpha \log(N + 1).
\end{equation}

Then, by Birgé’s lemma,

\[ \max_{\theta \in \Theta_0} P_{\theta}(\hat{\theta} \neq \theta) = \max_{0 \leq i \leq N} P_i(A_i^c) \]

\[ = 1 - \min_{0 \leq i \leq N} P_i(A_i) \]

\[ \geq 1 - \alpha \]

\[ \equiv 0.29. \]

This bound holds for any estimator $\hat{\theta}$. Consequently, using Lemma 12.2, we get the lower bound $\mathfrak{R}(\Theta) \geq (1 - \alpha)\varepsilon/2$.

**2. Proof of Theorem 12.1**

Roughly speaking, the strategy of the proof will be as follows: We start by observing that we can lower-bound the minimax risk $R_n(h, \mathcal{F})$ by

\[ R_n(h, \mathcal{F}) \geq \inf_{f_n} \sup_{P \in \mathcal{Q}} \mathbb{E} \left[ L(\hat{f}_n) - L(f^*) \right] \]

for any subset $\mathcal{Q} \subset \mathcal{P}(h, \mathcal{F})$. We will then construct $\mathcal{Q}$ in such a way that its elements can be naturally indexed by the vertices of a binary hypercube of dimension $V - 1$ (where $V$ is
the VC dimension of $\mathcal{F}$, and the expected excess risk for each $P \in \mathcal{Q}$ can be related to the minimax risk for the problem of estimating the corresponding binary string of length $V - 1$. At that point, we will be in a position to apply Assouad’s lemma.

2.1. Construction of $\mathcal{Q}$. As stated above, our set $\mathcal{Q}$ of “difficult” distributions will consist of $2^{V-1}$ distributions $P_b$, $b \in \{0, 1\}^{V-1}$. To construct these distributions, we will first pick the marginal distribution $P_X \in \mathcal{P}(\mathcal{X})$ of the feature $X$, and then specify the conditional distributions $P_{Y|X}^{(b)}$ of the binary label $Y$ given $X$, for each $b \in \{0, 1\}^{V-1}$. For now, let us assume that $h > 0$.

We construct $P_X$ as follows. Since $\mathcal{F}$ is a VC class with VC dimension $V$, there exists a set $\{x_1, \ldots, x_V\} \subset \mathcal{X}$ of points that can be shattered by $\mathcal{F}$, i.e., for any binary string $\beta \in \{0, 1\}^V$ there exists at least one $f \in \mathcal{F}$, such that $f(x_j) = \beta_j$ for all $1 \leq j \leq V$. Given a parameter $p \in [0, 1/(V - 1)]$, which will be chosen later, we choose $P_X$ so that $P_X(\{x_1, \ldots, x_V\}) = 1$, and

$$P_X(x_j) = \begin{cases} p, & \text{if } 1 \leq j \leq V - 1 \\ 1 - (V - 1)p, & \text{otherwise} \end{cases}.$$  

(12.30)

In other words, $P_X$ is a discrete distribution supported on the shattered set $\{x_1, \ldots, x_V\}$ that puts the same mass $p$ on each of the first $V - 1$ points and dumps the rest of the probability mass, equal to $1 - (V - 1)p$, on the last point $x_V$. Owing to our condition on $p$, this is a valid probability distribution.

Next we choose $P_{Y|X}^{(b)}$ for each $b \in \{0, 1\}^{V-1}$ as follows: For a fixed $b$, the conditional distribution of $Y$ given $X = x$ is

$$\begin{align*}
\text{Bernoulli} \left( \frac{1 + (2b_j - 1)h}{2} \right), & \quad \text{if } x = x_j \text{ and } j \in \{1, \ldots, V - 1\} \\
\text{Bernoulli}(0), & \quad \text{otherwise}
\end{align*}$$

In other words, for a fixed $b$, we have

$$\eta_b(x) \equiv P_{Y|X}^{(b)}(Y = 1|X = x) = \begin{cases} \frac{1-h}{2}, & \text{if } x = x_j \text{ for some } j \in \{1, \ldots, V - 1\}, \text{ and } b_j = 0 \\ \frac{1+h}{2}, & \text{if } x = x_j \text{ for some } j \in \{1, \ldots, V - 1\}, \text{ and } b_j = 1 \\ 0, & \text{otherwise} \end{cases}.$$  

(12.31)

Therefore, the corresponding Bayes classifier, which we denote by $f^*_b$, is given by

$$f^*_b(x) = \begin{cases} 0, & \text{if } x = x_j \text{ for some } j \in \{1, \ldots, V - 1\}, \text{ and } b_j = 0 \\ 1, & \text{if } x = x_j \text{ for some } j \in \{1, \ldots, V - 1\}, \text{ and } b_j = 1 \\ 0, & \text{otherwise} \end{cases}.$$  

(12.32)

That is, the output of the Bayes classifier on each $x_j$, $1 \leq j \leq V - 1$, is simply equal to the bit value $b_j$, and is zero everywhere else.

It remains to check whether the resulting set $\mathcal{Q} = \{P_b : b \in \{0, 1\}^{V-1}\}$ is contained in $\mathcal{P}(h, \mathcal{F})$. First of all, from (12.31) we see that $|2\eta_b(x) - 1| \geq h$ for all $x$ (indeed, $|2\eta_b(x) - 1| = h$ when $x \in \{x_1, \ldots, x_{V-1}\}$, and $|2\eta_b(x) - 1| = 1$ otherwise). Secondly, because $\{x_1, \ldots, x_V\}$
is shattered by \( \mathcal{F} \), there exists at least one \( f \in \mathcal{F} \), such that \( f^*_b(x) = f(x) \) for all \( x \in \{x_1, \ldots, x_V\} \). Thus, \( Q \subset \mathcal{P}(h, \mathcal{F}) \), as claimed.

### 2.2. Reduction to an estimation problem on the binary hypercube

Now that we have constructed \( Q \), we will show that the problem of learning a classifier when the \( n \) training samples are drawn i.i.d. from some \( P_b \in Q \) is at least as difficult as reconstructing the underlying bit string \( b \) — indeed, intuitively this makes sense, given the structure of the Bayes classifier \( f^*_b \) corresponding to \( P_b \).

We start by noting that, for any classifier \( f: X \to \{0, 1\} \) and any distribution \( P \) on \( X \times \{0, 1\} \), we have\(^3\)

\[
L(f) - L(f^*) = \mathbb{E} \left[ \|2\eta(X) - 1\|f(X) - f^*(X)\| \right].
\]

From this, we see that if \( P \in \mathcal{P}(h, \mathcal{F}) \), then

\[
L(f) - L(f^*) \geq h \mathbb{E} \left[ \|f(X) - f^*(X)\| \right] \equiv h \|f - f^*\|_{L_1},
\]

where the \( L_1 \) norm is computed w.r.t. the marginal distribution \( P_X \). Hence, we have

\[
\inf_{\tilde{f}_n} \sup_{P \in Q} \mathbb{E} \left[ L(\tilde{f}_n) - L(f^*) \right] = \inf_{\tilde{f}_n} \max_{b \in \{0,1\}^{V-1}} \mathbb{E}_b \left[ L(\tilde{f}_n) - L(f^*_b) \right] 
\geq h \inf_{\tilde{f}_n} \max_{b \in \{0,1\}^{V-1}} \mathbb{E}_b \|\tilde{f}_n - f^*_b\|_{L_1},
\]

(12.33)

where the \( L_1 \) norm is w.r.t. the distribution \( P_X \) defined in (12.30), and \( \mathbb{E}_b[\cdot] \) denotes expectation w.r.t. \( P_b \). Now we are ready to carry out the reduction to an estimation problem on the binary hypercube \( \{0, 1\}^{V-1} \). Given any candidate estimator \( \tilde{f}_n \), let \( \tilde{b}_n \) be an estimator that takes values in \( \{0, 1\}^{V-1} \), and is defined as follows:

\[
\tilde{b}_n := \arg \min_{b \in \{0,1\}^{V-1}} \|\tilde{f}_n - f^*_b\|_{L_1}.
\]

(12.34)

In other words, \( \tilde{b}_n \) is the binary string that indexes the element of \( \{f^*_b: b \in \{0, 1\}^{V-1}\} \) which is the closest to \( \tilde{f}_n \) in the \( L_1 \) norm. Then, for any \( b \),

\[
\|f^*_b - f^*_b\|_{L_1} \leq \|f^*_b - \tilde{f}_n\|_{L_1} + \|\tilde{f}_n - f^*_b\|_{L_1} 
\leq 2\|\tilde{f}_n - f^*_b\|_{L_1},
\]

(12.35)

where the first step is by the triangle inequality, while the second step is by (12.34). Combining (12.35) with (12.33), we get

\[
\inf_{\tilde{f}_n} \sup_{P \in Q} \mathbb{E} \left[ L(\tilde{f}_n) - L(f^*) \right] \geq \frac{h}{2} \inf_{\tilde{b}_n} \max_{b \in \{0,1\}^{V-1}} \mathbb{E}_b \|f^*_b - f^*_b\|_{L_1},
\]

(12.36)

where the infimum is over all estimators that take values in \( \{0, 1\}^{V-1} \) based on \( n \) i.i.d. samples from one of the \( P_b \)'s.

\(^3\)Exercise: prove this!
Now let us inspect the $L_1$ norm $\|f_b^* - f_{b'}^*\|_{L_1}$ for any two $b, b'$. Using (12.32), we have

$$\|f_b^* - f_{b'}^*\|_{L_1} = \int_X |f_b^*(x) - f_{b'}^*(x)| \, P_X(dx)$$

$$= \sum_{j=1}^{V} P_X(x_j) |f_b^*(x_j) - f_{b'}^*(x_j)|$$

$$= p \sum_{j=1}^{V-1} |f_b^*(x_j) - f_{b'}^*(x_j)|$$

$$= p \sum_{j=1}^{V-1} |b_j - b'_j|$$

$$= p \, d_H(b, b').$$

Substituting this into (12.36) gives

$$\inf_{\hat{f}_n} \sup_{P \in Q} E \left[ L(\hat{f}_n) - L(f^*) \right] \geq \frac{ph}{2} \inf_{\hat{b}_n} \max_{b \in \{0,1\}^{V-1}} E_b \left[ d_H(\hat{b}_n, b) \right],$$

as claimed. Now we are in a position to apply Assouad’s lemma.

**2.3. Applying Assouad’s lemma.** In order to apply Assouad’s lemma, we need an upper bound on the squared Hellinger distance $H^2(P_b, P_{b'})$ for all $b, b'$ with $d_H(b, b') = 1$. This is a simple computation. In fact, for any two $b, b' \in \{0,1\}^{V-1}$ we have

$$H^2(P_b, P_{b'}) = \sum_{j=1}^{V} \sum_{y \in \{0,1\}} \left( \sqrt{P_b(x_j, y)} - \sqrt{P_{b'}(x_j, y)} \right)^2$$

$$= p \sum_{j=1}^{V-1} \sum_{y \in \{0,1\}} \left( \sqrt{P_b^{(b)}(y|x_j)} - \sqrt{P_{b'}^{(b')}(y|x_j)} \right)^2$$

$$= p \sum_{j=1}^{V-1} H^2 \left( \text{Bernoulli} \left( \frac{1 + (2b_j - 1)h}{2} \right), \text{Bernoulli} \left( \frac{1 + (2b'_j - 1)h}{2} \right) \right).$$

For each $j \in \{1, \ldots, V - 1\}$, the $j$th term in the above summation is nonzero if and only if $b_j \neq b'_j$, in which case it is equal to the squared Hellinger distance between the Bernoulli($\frac{1-h}{2}$) and Bernoulli($\frac{1+h}{2}$) distributions. Thus,

$$H^2(P_b, P_{b'}) = pH^2 \left( \text{Bernoulli} \left( \frac{1-h}{2} \right), \text{Bernoulli} \left( \frac{1+h}{2} \right) \right) \cdot d_H(b, b')$$

$$= 2p \left( \sqrt{\frac{1-h}{2}} - \sqrt{\frac{1+h}{2}} \right)^2 d_H(b, b')$$

$$= 2p \left( 1 - \sqrt{1-h^2} \right) d_H(b, b').$$

In particular, the collection of distributions $\{P_b : b \in \{0,1\}^{V-1}\}$ satisfies the condition (12.21) of Corollary 12.3 with $\alpha = 2p(1 - \sqrt{1-h^2}) \leq 2ph$. Therefore, applying the bound
Putting together (12.38) and (12.39), we get the bound of Theorem 12.1. (12.38)

If we let \( p = 2/9nh^2 \), the term in parentheses will be equal to 1/3, and

\[
\inf_{f_n} \sup_{P \in \mathcal{Q}} \mathbf{E} \left[ L(\tilde{f}_n) - L(f^*) \right] \geq \frac{V - 1}{54nh}, \quad \text{if } h \geq \sqrt{(V - 1)/n}.
\]

assuming that the condition \( p \leq 1/(V - 1) \) holds. This will be the case if \( h \geq \sqrt{(V - 1)/n} \). Therefore,

\[
(12.38) \quad \inf_{f_n} \sup_{P \in \mathcal{Q}} \mathbf{E} \left[ L(\tilde{f}_n) - L(f^*) \right] \geq \frac{V - 1}{54nh}, \quad \text{if } h \geq \sqrt{(V - 1)/n}.
\]

If \( h \leq \sqrt{(V - 1)/n} \), we can use the above construction with \( \tilde{h} = \sqrt{(V - 1)/n} \). In that case, because \( \mathcal{P}(h, \mathcal{F}) \subseteq \mathcal{P}(h', \mathcal{F}) \) whenever \( h \geq h' \), we see that

\[
\inf_{f_n} \sup_{P \in \mathcal{Q}(h, \mathcal{F})} \mathbf{E} \left[ L(\tilde{f}_n) - L(f^*) \right] \geq \inf_{f_n} \sup_{P \in \mathcal{Q}(h, \mathcal{F})} \mathbf{E} \left[ L(\tilde{f}_n) - L(f^*) \right] \geq \frac{V - 1}{54nh}
\]

(12.39)

\[
= \frac{1}{54} \sqrt{\frac{V - 1}{n}}, \quad \text{if } h \leq \sqrt{(V - 1)/n}.
\]

Putting together (12.38) and (12.39), we get the bound of Theorem 12.1.

3. Proof of Theorem 12.2

In its broad outline, the proof is very similar to the proof of Theorem 12.1. Fix some \( N \geq 4D \). Since \( \mathcal{F} \) is \( (N, D) \)-rich, there exist \( N \) distinct points \( x_1, \ldots, x_N \in X \), such that

\[
\{0, 1\}^N_D := \{b \in \{0, 1\}^N : \text{wt}(b) = D\} \subseteq \mathcal{F}(x^n),
\]

where \( \text{wt}(b) \) denotes the Hamming weight of a binary string \( b \). Let \( P_X \) be the uniform distribution on \( \{x_1, \ldots, x_N\} \). Also, for each \( b \in \{0, 1\}^N_D \), let

\[
\eta_b(x_i) := \frac{1 + (2b_i - 1)h}{2}, \quad 1 \leq i \leq N.
\]

Now for each such \( b \) define a distribution \( P_b \in \mathcal{P}(X \times \{0, 1\}) \) by \( P_b = P_X \times P_{Y|X}^{(b)} \), where

\[
P_{Y|X}^{(b)}(1|x_i) = \frac{1 + (2b_i - 1)h}{2} \equiv \eta_b(x_i).
\]

In other words, the conditional distribution \( P_{Y|X = x_i}^{(b)} \) is a Bernoulli measure with bias \( \frac{1+h}{2} \) if \( b_i = 1 \) and \( \frac{1-h}{2} \) if \( b_i = 0 \). The corresponding Bayes classifier is given by \( f^*_b(x_i) = b_i \) for each \( i \), as before. Moreover, since \( \mathcal{F} \) is \( (N, D) \)-rich, for any \( b \in \{0, 1\}^N_D \) there exists at least one \( f \in \mathcal{F} \), such that \( f(x_i) = b_i = f^*_b(x_i) \) for every \( i \). Consequently,

\[
Q = \{ P_b : b \in \{0, 1\}^N_D \} \subseteq \mathcal{P}(h, \mathcal{F}).
\]
Proceeding in the same way as in the proof of Theorem 12.1, for any subset $C \subseteq \{0, 1\}_D^N$, 
\[
R_n(h, \mathcal{F}) \geq \frac{h}{2} \inf \max_{b_n \in C} \mathbf{E}_b \left\| f_{b_n}^* - f_b^* \right\|_{L_1} = \frac{h}{2N} \inf \max_{b_n \in C} \mathbf{E}_b \left[ d_H(\tilde{b}_n, b) \right].
\]

Since $\{0, 1\}_D^N$ is not the entire binary hypercube $\{0, 1\}^N$, we cannot use Assouad’s lemma. Instead, we will use Lemma 12.2 in conjunction with Birgé’s bound. In order to do that, we must first construct a nice, well-separated subset of $\{0, 1\}_D^N$. The following combinatorial result, due to P. Reynaud-Bouret, does the trick. There exists a subset $C \subset \{0, 1\}_D^N$ with the following properties:

1. $d_H(b, b') > D/2$ for any two distinct $b, b' \in C$;
2. $\log |C| \geq \kappa D \log \frac{N}{D}$, where $\kappa \approx 0.233$.

Item 1 says that this $C$ is $D/2$-separated in the Hamming distance. Thus, by Lemma 12.2,
\[
R_n(h, \mathcal{F}) \geq \frac{hD}{4N} \inf \max_{b_n \in C} \mathbf{P}_b \left( \tilde{b}_n \neq b \right) = \frac{hD}{4N} \left( 1 - \sup \min_{b_n \in C} \mathbf{P}_b \left( \tilde{b}_n \neq b \right) \right).
\]

We are now in a position to apply Birgé’s lemma:
\[
\sup \min_{b_n \in C} \mathbf{P}_b \left( \tilde{b}_n \neq b \right) \leq \alpha,
\]
where $\alpha = 0.71$, provided
\[
(12.40) \quad \bar{K} = \frac{1}{|C| - 1} \sum_{b_n \in C, b_n \neq b_0} D \left( P^n_b \parallel P^n_{b_0} \right) \leq \alpha \log |C|,
\]

where $b_0$ is some fixed but arbitrary element of $C$, and $P^n_b$ is a product of $n$ copies of $P_b$ (recall that our estimators are based on an i.i.d. sample of size $n$). So now we turn to the analysis of $\bar{K}$. For any two $b, b' \in \{0, 1\}_D^N$, we have
\[
D \left( P^n_b \parallel P^n_{b'} \right) = nD(P_b \parallel P_{b'}) = n \sum_{i=1}^{N} \sum_{y \in \{0, 1\}} P_b(x_i, y) \log \frac{P_b(x_i, y)}{P_{b'}(x_i, y)}
\]
\[
= \frac{n}{N} \sum_{i=1}^{N} \sum_{y \in \{0, 1\}} P_Y^{(b)}(y|x_i) \log \frac{P_Y^{(b)}(y|x_i)}{P_Y^{(b')}(y|x_i)}
\]
\[
= \frac{n}{N} \sum_{i=1}^{N} D \left( \text{Bernoulli} \left( \frac{1 + (2b_i - 1)h}{2} \right) \parallel \text{Bernoulli} \left( \frac{1 + (2b'_i - 1)h}{2} \right) \right),
\]

168
where the first line is by (12.27), while the rest follows from definitions. Now, in the above summation, the \(i\)th term is nonzero if and only if \(b_i = b'_i\), and in that case it is equal to
\[
D\left(\text{Bernoulli}\left(\frac{1 + h}{2}\right) \bigg\| \text{Bernoulli}\left(\frac{1 - h}{2}\right)\right) = h \log \frac{1 + h}{1 - h}.
\]
Consequently,
\[
D(P^n_b \bigg\| P^n_{b'}) = \frac{n}{N} h \log \left(\frac{1 + h}{1 - h}\right) \sum_{i=1}^{N} 1_{\{b_i \neq b'_i\}}
= \frac{n}{N} h \log \left(\frac{1 + h}{1 - h}\right) \cdot d_H(b, b').
\]
Now, for any two \(b, b' \in \{0, 1\}_D\), \(d_H(b, b') \leq \text{wt}(b) + \text{wt}(b') = 2D\). Moreover, using the bound \(\log t \leq t - 1\) for any \(t \geq 0\), we have
\[
h \log \frac{1 + h}{1 - h} \leq h \left(\frac{1 + h}{1 - h} - 1\right) = \frac{2h^2}{1 - h}.
\]
Therefore, for any two \(b, b' \in \mathcal{C}\),
\[
D(P^n_b \bigg\| P^n_{b'}) \leq \frac{4nh^2D}{N(1 - h)},
\]
which implies that \(\bar{K} \leq \frac{4nh^2D}{N(1 - h)}\). Using this and the fact that \(\log |\mathcal{C}| \leq \kappa D \log \frac{N}{D}\) with \(\kappa \approx 0.233\), we see that the condition (12.40) will be satisfied if we can choose some \(N \geq 4D\), so that
\[
N \log \frac{N}{D} \geq \frac{4nh^2}{\kappa(1 - h)}.
\]
A tedious calculation (see [MN06]) shows that the choice
\[
N = \left\lfloor \frac{8nh^2}{\kappa(1 - h) \left(1 + \log \frac{nh^2}{D}\right)} \right\rfloor
\]
does the job, provided \(h \geq \sqrt{D/n}\). This completes the proof.
APPENDIX A

Probability and random variables

Probability theory is the foundation of statistical learning theory. In this appendix, I will give a quick overview of the main concepts and set up the notation that will be used consistently throughout the course. This is by no means intended as a substitute for a serious course in probability; as a good introductory reference, I recommend the text by Gray and Davisson [GD04], which is geared towards beginning graduate students in electrical engineering.

Let $\Omega$ be a set. A collection $F$ of subsets of $\Omega$ is called a $\sigma$-algebra if it has the following two properties:

1. If $A \in \Omega$, then $A^c \equiv \Omega \setminus A \in F$
2. For any sets $A_1, A_2, \ldots \in F$, their union belongs to $F$: $\bigcup_{i=1}^{\infty} A_i \in F$.

In other words, any $\sigma$-algebra is closed under complements and countable unions. This implies, in particular, that the empty set $\emptyset$ and the entire set $\Omega$ are contained in any $\sigma$-algebra $F$, and that such an $F$ is closed under countable intersections. A pair $(\Omega, F)$ consisting of a set and a $\sigma$-algebra is called a measurable space. A probability measure on $(\Omega, F)$ is a function $P : F \to [0, 1]$, such that

1. $P(\Omega) = 1$
2. Given any countably infinite sequence $A_1, A_2, \ldots \in F$ of pairwise disjoint sets, i.e., $A_i \cap A_j = \emptyset$ for every pair $i \neq j$,

$$P\left(\bigcup_{i=1}^{\infty} A_i\right) = \sum_{i=1}^{\infty} P(A_i).$$

The triple $(\Omega, F, P)$ is called a probability space.

Let $(X, B)$ be some other measurable space. A random variable on $\Omega$ with values in $X$ is any function $X : \Omega \to X$ with the property that, for any $B \in B$, the set

$$X^{-1}(B) := \{\omega \in \Omega : X(\omega) \in B\}$$

lies in $F$ (in fancy language, $X$ is a measurable mapping from $(\Omega, F)$ into $(X, B)$). Together, $X$ and $P$ induce a probability measure $P_X$ on $(X, B)$ by setting

$$P_X(B) := P\left(X^{-1}(B)\right) \equiv P\left(\{\omega \in \Omega : X(\omega) \in B\}\right),$$

which is called the distribution of $X$. (A good character-building exercise is to try and prove that $P_X$ is indeed a valid probability measure.) Once $P_X$ is defined, we can forget all about $(\Omega, F, P)$ and just work with $P_X$. Here are two standard examples to keep in mind. One is when $X$ is a finite set, in which case we can take the $\sigma$-algebra consisting of all subsets of $X,
let $P_X$ be the probability mass function (pmf) of $X$, and then for any $B \subseteq X$ we will have

$$P_X(B) = \sum_{x \in B} P_X(x).$$  \hfill (A.1)

The other is when $X$ is the real line $\mathbb{R}$ (with the so-called Borel $\sigma$-algebra, which at this point you don’t have to worry about), and $P_X$ has a probability density function (pdf) $p_X$, giving

$$P_X(B) = \int_B p_X(x)\,dx.$$  \hfill (A.2)

for any (measurable) set $B \subseteq \mathbb{R}$. We will use a more abstract notation that covers these two cases (and much more besides):

$$P_X(B) = \int_B P_X(\,dx), \quad \forall B \in \mathcal{B}. \hfill (A.3)$$

When seeing something like (A.3), just think of (A.1) or (A.2).

If $f : X \to \mathbb{R}$ is a real-valued function on $X$, the expected value of $f(X)$ is

$$\mathbb{E}[f(X)] = \int_X f(x) P_X(\,dx);$$

again, think of either

$$\mathbb{E}[f(X)] = \sum_{x \in X} f(x) P_X(x)$$

in the case of discrete $X$, or

$$\mathbb{E}[f(X)] = \int_{\mathbb{R}} f(x) p_X(x)\,dx$$

in the case of $X = \mathbb{R}$ and a random variable with a pdf $p_X$.

For any two jointly distributed random variables $X \in X$ and $Y \in X$, we have their joint distribution $P_{XY}$, the marginals

$$P_X(A) := P_{XY}(A \times Y) \equiv \int_{A \times Y} P_{XY}(dx, dy)$$

$$P_Y(B) := P_{XY}(X \times B) \equiv \int_{X \times B} P_{XY}(dx, dy)$$

for all measurable sets $A \subseteq X, B \subseteq Y$, and the conditional distribution

$$P_{Y|X}(B|A) := \frac{P_{XY}(A \times B)}{P_X(A)}$$

of $Y$ given that $X \in A$. Neglecting technicalities and considerations of rigor, we can define the conditional distribution of $Y$ given $X = x$, denoted by $P_{Y|X}(\cdot|x)$, implicitly through

$$P_{XY}(A \times B) = \int_A P_X(dx) \left(\int_B P_{Y|X}(dy|x)\right).$$

Here, it is helpful to think of the conditional pmf

$$P_{Y|X}(y|x) = \frac{P_{XY}(x,y)}{P_X(x)}.$$
in the discrete case, and of the conditional pdf
\[ p_{Y|X}(y|x) = \frac{p_{XY}(x,y)}{p_X(x)} \]
in the continuous case. The conditional expectation of any function \( f : X \times Y \to \mathbb{R} \) given \( X \), denoted by \( \mathbb{E}[f(X,Y)|X] \), is a random variable \( g(X) \) that takes values in \( \mathbb{R} \), such that\(^1\)
\[ \mathbb{E}[f(X,Y)] = \mathbb{E}[g(X)] = \mathbb{E}[\mathbb{E}[f(X,Y)|X]]. \]
This is known as the law of iterated expectations. Once again, think of
\[ \mathbb{E}[f(X,Y)|X = x] = \sum_{y \in Y} f(x,y)P_{Y|X}(y|x) \]
if both \( X \) and \( Y \) are discrete sets, and of
\[ \mathbb{E}[f(X,Y)|X = x] = \int_Y f(x,y)p_{Y|X}(y|x) dy \]
if both \( X \) and \( Y \) are subsets of \( \mathbb{R} \).

\(^1\)As usual, I am being rather cavalier with the definitions here, since the choice of \( g \) is not unique; one typically speaks of different versions of the conditional expectation, which, properly speaking, should be defined w.r.t. the \( \sigma \)-algebra generated by \( X \). Again, this will not be an issue in this course.
Bibliography


