

BASIC PROBABILITY THEORY 2024

JUHAN ARU

1

¹Version of 2024. All kinds of feedback, including smaller or bigger typos, is appreciated - juhan.aru@epfl.ch. This is a third version of the notes. In writing previous version of these notes I have consulted notes of I. Manolescu (Fribourg), Y. Velenik (Geneva), A. Eberle (Bonn) (all on their websites) and the book by R. Dalang & D. Conus published by EPFL press.

SECTION 0

Introduction

This course is about probability theory: the mathematical framework for formalising our questions about random phenomena, and their mathematical study.

When we want to describe a random phenomena in the real world, we build a mathematical model. This is itself an interesting process and a good model involves lots of well-chosen simplifications and righteous choices - e.g. to model a coin toss, we usually discard the possibility of it landing on the edge, or without further knowledge we consider the heads and tails equiprobable, although that may not be the case for example already because of different weight distributions. But this all is not the topic of this course.

In this course we will study the general mathematical framework and formulation of such models and then discuss the mathematical tools necessary and useful to study such models. Hopefully we also have some time to discuss some interesting models.

SECTION 1

Basic framework

In this chapter we discuss some basic but important notions of probability theory:

- Probability space
- Random variables
- Independence

1.1 Probability space

Our first aim is to motivate the notion of a probability space or a probabilistic model. To do this let us consider two examples:

- (1) A random number with values in $\{1, 2, \dots, 12\}$ e.g. something that comes from a lottery.
- (2) Describing the weather in Lausanne the day after.

In describing these two random phenomena we will still use everyday vocabulary / intuitions. Thereafter we will give the mathematical definitions that will fix the vocabulary for the rest of the course.

(1) Random number. To describe a random number mathematically, we basically need three inputs:

- The set of all possible outcomes: in this case $\Omega = \{1, 2, 3, \dots, 12\}$
- The collection of yes / no questions that we can answer about the actual outcome, i.e. this random number. For example:
 - Is this number equal to 3?
 - Is this number even?
 - Is this number smaller than 4?

To each of these questions we put in correspondence the subset of outcomes that corresponds to the answer yes: $\{3\}$, $\{2, 4, 6, 8, 10, 12\}$ or $\{1, 2, 3\}$ respectively. We call each such subset an event.

- Finally, to each event $E \subseteq \Omega$ we want to assign a numerical value $\mathbb{P}(E) \in [0, 1]$ that we call the probability. This should correspond to the fraction of times an event happens if the random number is given to us many times, e.g. if the lottery is played many times. ²

Here the set of possible outcomes was easy and directly given by the problem. Also it is natural to assume that each subset $E \subseteq \Omega$ is an event - or in other words that for each E we can ask the question: is the number in E ? This means that we can take the collection of events to correspond to all subsets of Ω .

Determining the probability really depends on what we want to model - e.g. if we are trying to model the lottery, we may assume that all numbers are equally likely and then we

²In fact, one uses probabilistic models also to model phenomena that only happens once. In that case probability measures somehow our degree of belief.

rediscover the model from high-school: we set $\mathbb{P}(E) = |E|/|\Omega|$. However, if we wanted to describe the sum of two dice, we would need to choose the numbers $\mathbb{P}(E)$ very differently! ³

Now, if we want our model to correspond to the intuitive notion of probability and to predict the fraction of repeated experiments, then these choices are not quite free - we need to add some constraints. E.g. we cannot put in an arbitrary function $\mathbb{P}$: indeed, if we have two events $E_1 \subseteq E_2$ then we should have $\mathbb{P}(E_1) \leq \mathbb{P}(E_2)$ as every time E_1 happens, also E_2 happens. We should also have $\mathbb{P}(\Omega) = 1$ as something always happens and $\mathbb{P}(E \cup F) = \mathbb{P}(E) + \mathbb{P}(F)$ if E and F are disjoint (why?). Of course not all these constraints are distinct - some might imply others and when giving the definition of a probability space below we will purify and choose only some conditions that will then mathematically imply all the others.

(2) Weather in Lausanne the day after. We would again want to make the three decisions, but here the task is already harder at the very first step. What should be the state space? A natural state space could probably be all possible microscopic states of the atmosphere up to 20km of height over Lausanne...but here we of course have many arbitrary choices - why 20 km, how wide should we look over Lemman etc? And in any case, any natural state would be impossibly complicated!

Luckily, we do not actually need to worry about it - we only have to assign probabilities to all the events in the collection of events. And we have some freedom in choosing this collection events - it could be determined by our possibility to measure the states, e.g. we are able to measure the temperature up to some precision, or the density of CO_2 or water molecules to some precision and this determines some subsets of the state space.

However, as with the probability function, also for the collection of events there are some natural consistency conditions: we would assume that if one can observe if event E happened, we should be also able to measure if its complement E^c happened. Or if we are able to say if E happened or if F happened, we should be able to say if one of the two happened - i.e. $E \cup F$ should also be an event. And in fact it comes out that this is all we need!

Naturally, setting up probabilities for this model is also horribly complicated - there are no natural symmetry assumptions like the one we used for the uniform distribution. Also, even the best physicist in the world will not be able to describe the natural probability distribution of all microscopic states of the atmosphere, especially as it will heavily depend on what is happening just before! Thus, our only choice basically is to try to somehow use the combination of our knowledge about atmospheric processes together with our observations from history to set up some estimates for the model; and then naturally we will try to improve it with every next day. Luckily, this difficult task is not up to us but rather the office of meteo and the statisticians!

Remark 1.1. *Finally, before giving the mathematical definitions, let us stress again that all three components of the model - the sample space, the set of events and their probabilities - are inputs that we choose to build our model. When trying to model a real world phenomena we usually make simplifications for each of these choices. For example, for the coin toss we use only two outcomes: heads and tails, although theoretically edge is also possible. Also, we usually set probabilities to be a half, although that is not exactly true either.*

³See Exercise sheet 1.

1.2 Mathematical definition of a probability space

We are now ready to use our mathematical filter and give a mathematical definition of a probability space. In fact, we first use the mathematical purifier to come up with a definition in the restricted setting where Ω is a finite set, and then generalize it further.

Indeed, the discussions above lead us directly to:

Definition 1.2 (Elementary probability space, Kolmogorov 1933). *An elementary probability space is a triple $(\Omega, \mathcal{F}, \mathbb{P})$, where*

- Ω is a finite set, called the state or sample space or the universe.
- $\mathcal{F}$ is a set of subsets of Ω , satisfying:
 - $\emptyset \in \mathcal{F}$;
 - if $A \in \mathcal{F}$, then also $A^c \in \mathcal{F}$;
 - If $A_1, A_2, \dots \in \mathcal{F}$, then also $A_1 \cup A_2 \in \mathcal{F}$.

$\mathcal{F}$ is called the collection of events and any $A \in \mathcal{F}$ is called an event.

- And finally, we have a function $\mathbb{P} : \mathcal{F} \rightarrow [0, 1]$ satisfying $\mathbb{P}(\Omega) = 1$ and additivity for disjoint sets: if $A_1, A_2 \in \mathcal{F}$ are pairwise disjoint, then

$$\mathbb{P}(A_1 \cup A_2) = \mathbb{P}(A_1) + \mathbb{P}(A_2).$$

This function $\mathbb{P}$ is called the probability

Notice that some properties discussed above, like the fact that for events $E_1 \subseteq E_2$, we have $\mathbb{P}(E_1) \leq \mathbb{P}(E_2)$, follow directly from the definition.⁴

Now, most phenomena in the real world can be described by finite sets just because we are able to measure things only to a finite level of precision. However, like the notion of a continuous or differentiable function helps to simplify our mathematical descriptions of reality and thus improve our understanding, continuous probability spaces also make the mathematical descriptions neater, simpler and thereby also make it easier to understand and study the underlying random phenomena.

Some natural examples where infinite sample spaces come in: an uniform point on a line segment e.g. stemming from breaking a stick into several pieces; the position on the street where the first raindrop of the day falls; or the space of all infinite sequences of coin tosses. In all these cases the mathematically natural state space is even uncountable. Countably infinite state spaces can also come up: for example if we want to model the first moment that a repeated coin toss comes up heads, the value might be 1, 2, 3 or with very very small probability also 10^{10} , so a natural state space would contain all natural numbers.

So let us state the general definition:

Definition 1.3 (Probability space, Kolmogorov 1933). *A probability space is a triple $(\Omega, \mathcal{F}, \mathbb{P})$, where*

- Ω is a set, called the state or sample space or the universe.
- $\mathcal{F}$ is a set of subsets of Ω , satisfying:
 - $\emptyset \in \mathcal{F}$;
 - if $A \in \mathcal{F}$, then also $A^c \in \mathcal{F}$;
 - If $A_1, A_2, \dots \in \mathcal{F}$, then also $\bigcup_{n \geq 1} A_n \in \mathcal{F}$.

$\mathcal{F}$ is called the collection of events or a σ -algebra and any $A \in \mathcal{F}$ is called an event.

⁴See Exercise sheet 1.

- And finally, we have a function $\mathbb{P} : \mathcal{F} \rightarrow [0, 1]$ satisfying $\mathbb{P}(\Omega) = 1$ and additivity for disjoint sets: if $A_1, A_2, \dots \in \mathcal{F}$ are pairwise disjoint,

$$\mathbb{P}\left(\bigcup_{n \geq 1} A_n\right) = \sum_{n \geq 1} \mathbb{P}(A_n).$$

This function $\mathbb{P}$ is called the probability

Notice the only differences are 1) we do not assume Ω to be finite 2) we assume that the set of events is stable under countable unions 3) we assume also the additivity of the probability under countable unions.

Exercise 1.1. Show that each elementary probability space is a probability space.

In fact probability spaces are an example of a general notion of measure spaces - probability spaces are just measure spaces with total mass equal to 1.

Definition 1.4 (Measure space, Borel 1898, Lebesgue 1901-1903). A measure space is a triple $(\Omega, \mathcal{F}, \mu)$, where

- Ω is a set, called the sample space or the universe.
- $\mathcal{F}$ is a set of subsets of Ω , satisfying:
 - $\emptyset \in \mathcal{F}$;
 - if $A \in \mathcal{F}$, then also $A^c \in \mathcal{F}$;
 - If $A_1, A_2, \dots \in \mathcal{F}$, then also $\bigcup_{n \geq 1} A_n \in \mathcal{F}$.
- $\mathcal{F}$ is called a σ -algebra and any $A \in \mathcal{F}$ is called a measurable set.
- And finally, we have a function $\mu : \mathcal{F} \rightarrow [0, \infty]$ satisfying $\mu(\emptyset) = 0$ and countable additivity for disjoint sets: if $A_1, A_2, \dots \in \mathcal{F}$ are pairwise disjoint,

$$\mu\left(\bigcup_{n \geq 1} A_n\right) = \sum_{n \geq 1} \mu(A_n).$$

This function μ is called a measure. If $\mu(\Omega) < \infty$, we call μ a finite measure.

Geometrically we interpret:

- Ω as our space of points
- $\mathcal{F}$ as the collection of subsets for which our notion of volume can be defined
- μ our notion of volume: it gives each measurable set its volume.

It is important to make this link to measure theory as many properties of probability spaces directly come from there. Yet it is also good to keep in mind that probability theory is not just measure theory - as M. Kac has put it well, 'Probability is measure theory with a soul' and we adhere to this philosophical remark.

Remark 1.5. You should compare the definition of a probability space / measure space with the definition of a topological space: there also we use a collection of subsets with certain properties to attach structure to the set. A question you should ask is: why do we use exactly countable unions and intersections for the events, and not finite or arbitrary?

1.3 Some basic properties of probability spaces

We start by a few small remarks about the definition of a probability space:

Remark 1.6. *It is worth considering why ask for countable stability of the σ -algebra or countable additivity of the probability measure. Whereas this is more a meta-mathematical question, it is good to keep it in mind throughout the course. Let us here just offer two simple observations.*

First, countable sums naturally come up when we take limits of finite sums. In fact, countable additivity can be seen to be equivalent to certain form of continuity for the probability measure (see below).

Second, allowing for arbitrary unions leads easily to power-sets, and sums of uncountably many positive terms cannot be finite (see the exercise sheet).

Exercise 1.2. *Show that the countable additivity in the axioms of a probability space can be replaced with finite additivity plus the following statement: for any decreasing sequence of events $E_1 \supseteq E_2 \supseteq E_3 \dots$ we have that $\mathbb{P}(\cap_{i=1}^n E_i) \rightarrow 0$ as $n \rightarrow \infty$.*

★ Does this hold in a general measure space?

Also we would like to remark another setting that explains well the usefulness of σ -algebras:

Remark 1.7. *Often in real life we only obtain information about the world step by step, and thus if we want to keep on working on the same probability space (which is helpful as then $\mathbb{P}$ will only need to be extended not redefined), we can consider a sequence of σ -algebras $\mathcal{F}_1 \subseteq \mathcal{F}_2 \subseteq \mathcal{F}_3 \dots$ called a filtration - each day we can ask some more yes/no questions because we already for example know what happened on the previous day and maybe also have learned something new. All possible information is contained in the power set $\mathcal{P}(\Omega)$.*

Probability spaces are usually classified in two types:

Definition 1.8 (Discrete and continuous probability spaces). *Probability spaces $(\Omega, \mathcal{F}, \mathbb{P})$ with a countable sample space Ω are called discrete probability spaces and those with an uncountable sample space are called continuous probability spaces.*

In this course we will mainly work with discrete probability spaces, as they are technically easier to deal with. However, continuous probability spaces come up naturally and we won't be able to fully avoid them either.

Their technical difference can be summoned in the following proposition, whose non-examinable proof will be left for enthusiasts.

Proposition 1.9. *Let Ω be countable and $\mathcal{F}$ a σ -algebra on Ω . Then one can find disjoint events $E_1, E_2, \dots \in \mathcal{F}$ such that for every $E \in \mathcal{F}$ we can express $E = \cup_{i \in I_E} E_i$.*

Essentially, this says that for every discrete probability space it suffices to determine $\mathbb{P}(E_i)$ for a countable collection of disjoint sets E_i , and thereafter for every other set E we can use countable additivity to extend $\mathbb{P}$. Notice that this means it is first easy to check whether a given $\mathbb{P}$ satisfies all the axioms and even more importantly it is easy to check when two probability measures are equal.

For continuous probability spaces this does not necessarily hold - the useful σ -algebras are usually more complicated. To exemplify why one doesn't want to necessarily use the power-set consider the following proposition, whose proof is in the appendix and relies on the axiom of choice:

Proposition 1.10. *There is no probability measure $\mathbb{P}$ on $([0, 1], \mathcal{P}([0, 1]))$ that is invariant under shifts, i.e. such that for any $A \in \mathcal{P}([0, 1]), \alpha \in [0, 1)$, we have that $\mathbb{P}(A + \alpha \bmod 1) =$*

$\mathbb{P}(A)$, where here we denote $A + \alpha \bmod 1 := \{a + \alpha \bmod 1 : a \in A\}$, the set obtained by shifting A by α , modulo 1.

In fact, it comes out that the only way to remedy this situation is to make the relevant σ -algebra smaller. We would still want to be able to answer yes or no to questions like: is my random number equal to $\{x\}$ or is it in an interval (a, b) ? Thanks to the fact that we have only countable additivity, this does not imply that our σ -algebra would need to be the power-set. And thanks to the properties of the σ -algebras, we can always construct at least some σ -algebra containing all our favourite sets - see the exercise sheet.

Let us now state some immediate consequences of the definitions about the σ -algebras and the probability measures:

Lemma 1.11 (Stability of the σ -algebra). *Consider a set Ω with a σ -algebra $\mathcal{F}$.*

- (1) *If $A_1, A_2, \dots \in \mathcal{F}$, then also $\bigcap_{n \geq 1} A_n \in \mathcal{F}$.*
- (2) *Then also $\Omega \in \mathcal{F}$ and if $A, B \in \mathcal{F}$, then also $A \setminus B \in \mathcal{F}$.*
- (3) *For any $n \geq 1$, if $A_1, \dots, A_n \in \mathcal{F}$, then also $A_1 \cup \dots \cup A_n \in \mathcal{F}$ and $A_1 \cap \dots \cap A_n \in \mathcal{F}$.*

Proof of Lemma 1.11. By de Morgan's laws for any sets $(A_i)_{i \in I}$, we have that

$$\bigcap_{i \in I} A_i = \left(\bigcup_{i \in I} A_i^c \right)^c.$$

Property (1) follows from this, as if $A_1, A_2, \dots \in \mathcal{F}$, then by the definition of a σ -algebra also $A_1^c, A_2^c, \dots \in \mathcal{F}$ and hence

$$\left(\bigcup_{i \geq 1} A_i^c \right)^c \in \mathcal{F}.$$

For (3), again by de Morgan laws, it suffices to show that $A_1 \cup \dots \cup A_n \in \mathcal{F}$. But this follows from the definition of a σ -algebra, as $A_1 \cup \dots \cup A_n = \bigcup_{i \geq 1} A_i$ with $A_k = \emptyset$ for $k \geq n + 1$.

Point (2) is left as an exercise. $\square$

In a similar vein, the basic conditions on the measure give rise to several natural properties:

Proposition 1.12 (Basic properties of a probability measure). *Consider a probability space $(\Omega, \mathcal{F}, \mathbb{P})$. Let $A_1, A_2, \dots \in \mathcal{F}$. Then*

- (1) *For any $A \in \mathcal{F}$, we have that $\mathbb{P}(A^c) = 1 - \mathbb{P}(A)$.*
- (2) *For any $n \geq 1$, and $A_1, \dots, A_n$ disjoint, we have finite additivity*

$$\mathbb{P}(A_1) + \dots + \mathbb{P}(A_n) = \mathbb{P}(A_1 \cup \dots \cup A_n).$$

In particular if $A_1 \subseteq A_2$ then $\mathbb{P}(A_1) \leq \mathbb{P}(A_2)$.

- (3) *If for all $n \geq 1$, we have $A_n \subseteq A_{n+1}$, then as $n \rightarrow \infty$, it holds that $\mathbb{P}(A_n) \rightarrow \mathbb{P}(\bigcup_{k \geq 1} A_k)$.*
- (4) *We have countable subadditivity (also called the union bound): $\mathbb{P}(\bigcup_{n \geq 1} A_n) \leq \sum_{n \geq 1} \mathbb{P}(A_n)$.*
- (5) *If for all $n \geq 1$, we have $A_n \supseteq A_{n+1}$, then as $n \rightarrow \infty$, it holds that $\mathbb{P}(A_n) \rightarrow \mathbb{P}(\bigcap_{k \geq 1} A_k)$.*

Proof. Properties 1, 4 and second part of 2 were included in the Exercise sheet 1. The first part of property 2 follows like in the lemma above by taking $A_{n+1} = A_{n+2} = \dots = \emptyset$ and using countable additivity.

So let us prove property 3: Write $B_1 = A_1$ and for $n \geq 2$, $B_n = A_n/A_{n-1}$. Then B_n are disjoint, $\bigcup_{n=1}^N B_n = A_N$ and $\bigcup_{n \geq 1} B_n = \bigcup_{n \geq 1} A_n$.

Thus by countable additivity

$$\mathbb{P}\left(\bigcup_{i \geq 1} A_i\right) = \mathbb{P}\left(\bigcup_{i \geq 1} B_i\right) = \sum_{i \geq 1} \mathbb{P}(B_i)$$

But $\mathbb{P}$ is non-negative, so

$$\sum_{i \geq 1} \mathbb{P}(B_i) = \lim_{n \rightarrow \infty} \sum_{i=1}^n \mathbb{P}(B_i)$$

By countable additivity again

$$\sum_{i=1}^n \mathbb{P}(B_i) = \mathbb{P}\left(\bigcup_{i=1}^n B_n\right) = \mathbb{P}(A_n)$$

and (2) follows. □

1.4 Random variables

In fact when studying a random phenomena we certainly don't want to restrict ourselves to yes and no questions. For example, in our model of a random number among $\{1, 2, \dots, 12\}$ the natural question is not 'Is this number equal to 5?' but rather 'What number is it?'. Similarly in our example of discussing the weather, it is more natural to ask 'What is the temperature?', 'How much rain will there be in the afternoon?'?

Such numerical observations about our random phenomena will be formalised under the name of random variables. In essence they give a number for each state and thus as such are just functions $X : \Omega \rightarrow \mathbb{R}$ from the state-space to real numbers. However, we may not want to include all such functions for consistency reasons. Indeed, we want to be able to ask yes / no questions about our random numbers, e.g. Is the random number equal to 3? Is the temperature more than 18? But again the answer yes / no corresponds to certain subsets of states in the universe and as such should be events in our model. Thus there is a link between the collection of events, and the collection of functions that can act as random variables. Let us without further give the general definition:

Definition 1.13 (Random variable). *Let $(\Omega, \mathcal{F}, \mathbb{P})$ be a probability space. We call a function $X : \Omega \rightarrow \mathbb{R}$ a random variable if for every interval (a, b) the set $X^{-1}((a, b)) := \{\omega \in \Omega : X(\omega) \in (a, b)\}$ is an event on the original probability space, i.e. belongs to $\mathcal{F}$.*

There is a simplification in the case of discrete probability spaces:

Lemma 1.14 (Random variables on discrete probability spaces). *Let $(\Omega, \mathcal{F}, \mathbb{P})$ be a discrete probability space. Then $X : \Omega \rightarrow \mathbb{R}$ is a random variable if and only if for every $y \in \mathbb{R}$ we have that $X^{-1}(\{y\}) \in \mathcal{F}$.*

Proof. This can be verified carefully from the definitions and will be on the exercise sheet. □

For the structurally minded the definition of a random variable might look somewhat arbitrary. And indeed, I have been hiding one piece of information - the natural collection of events on $\mathbb{R}$ that we alluded to a little bit already in the previous subsection. We will directly state it on $\mathbb{R}^n$.

Definition 1.15 (Borel σ -algebra). *The smallest σ -algebra on $\mathbb{R}^n$ that contains all open boxes of the form $(a_1, b_1) \times \cdots \times (a_n, b_n)$ is called the Borel σ -algebra. We denote it by $\mathcal{F}_B$*

Remark 1.16. *In fact this definition is even more general: given any topological space (X, τ) , the smallest σ -algebra containing all open sets is called the Borel σ -algebra. You will see on the exercise sheet that this more general definition reduces to the previous one in the case of $\mathbb{R}^n$ with its Euclidean topology.*

Based on this an equivalent, possibly more structural definition of a random variable is as follows: a function $X : \Omega \rightarrow \mathbb{R}$ is a random variable if the preimage of every set in the Borel σ -algebra under X is an event.⁵

An important notion that comes with random variables is its law:

Lemma 1.17 (The law of a random variable). *Let $(\Omega, \mathcal{F}, \mathbb{P})$ be a probability space and $X : \Omega \rightarrow \mathbb{R}$ a random variable.*

Then there is a probability measure $\mathbb{P}_X$ induced on $(\mathbb{R}, \mathcal{F}_B)$ by defining $\mathbb{P}_X(F) := \mathbb{P}(X^{-1}(F))$ for every $F \in \mathcal{F}_B$. This probability measure $\mathbb{P}_X$ is called the law (or distribution) of a random variable X .

This is a lemma and not a definition as it needs to be proved that indeed $\mathbb{P}_X$ is a probability measure on $(\mathbb{R}, \mathcal{F}_B)$.

Proof of Lemma. We need to verify the axioms on a probability measure for a probability space:

- We have $\mathbb{P}_X(\mathbb{R}) = \mathbb{P}(\Omega) = 1$
- Similarly $\mathbb{P}_X(F) = \mathbb{P}(X^{-1}(F)) \in [0, 1]$ for all $F \in \mathcal{F}_B$
- Finally it remains to check countable additivity: let $F_1, F_2, \dots$ be disjoint sets in $\mathcal{F}_B$. Then

$$\mathbb{P}_X\left(\bigcup_{i \geq 1} F_i\right) = \mathbb{P}\left(X^{-1}\left(\bigcup_{i \geq 1} F_i\right)\right) = \mathbb{P}\left(\bigcup_{i \geq 1} X^{-1}(F_i)\right) = \sum_{i \geq 1} \mathbb{P}(X^{-1}(F_i)) = \sum_{i \geq 1} \mathbb{P}_X(F_i).$$

Here we used the definition in the first and last equality, the properties of preimages in the second equality and the fact that $X^{-1}(F_i)$ are disjoint together with countable additivity in the third equality.

□

In words we showed that each random variable X induces a probability measure on the real numbers by just forgetting about the whole context and just concentrating on the number we see. For example in the case of weather in Lausanne, the temperature will give us a random variable and by just looking at its value and nothing else we have just a random real-valued number. Or more simply, if we throw two fair coins and count the number of heads, their sum will be a random variable that takes values in the set $\{0, 1, 2\}$. Thus the notion of the law of random variable gives us a way to compare random quantities arising in very different contexts.

Definition 1.18 (Equality in law). *Let X, Y be two random variables defined possibly on different probability spaces. We say that X and Y are equal in law or equal in distribution, denoted $X \sim Y$ if for every $E \in \mathcal{F}_B$ we have that $\mathbb{P}_X(E) = \mathbb{P}_Y(E)$.*

⁵In measure theory such functions would be called measurable functions from $(\Omega, \mathcal{F})$ to $(\mathbb{R}, \mathcal{F}_B)$; notice the similarity with the definition of continuous functions in your topology course.

We stress that when looking at the law of random variable the context gets forgotten - we only concentrate on the numerical value and the initial probability space $(\Omega, \mathcal{F}, \mathbb{P})$ only helps to determine $\mathbb{P}_X$ but plays no role thereafter. This means that we can nicely connect different random phenomena between each other. For example the indicator functions of all events that have probability p , independently on which probability space they have been defined, have the same law. Or more concretely, for example the following random variables have the same law:

- Number of heads in two independent tosses
- Number of prime factors when we choose uniformly a number among $\{1, 2, 3, 4\}$.

In some sense a large part of this course will be about studying and describing probability laws of random variables.

SECTION 2

Conditional probability and independence

In general, if we learn something new about our random phenomena, this knowledge influences and often changes our predictions for the rest of the model.

- For example in the case of a uniform random number between 1 and 12, if someone tells you that this number is even, then the probability of seeing 1 will suddenly be 0, but the probability of seeing 2 will rise from $1/12$ to $1/6$.
- In the case of weather in Lausanne, if someone tells us that it rains the whole day, then it is less likely to also be above 35 degrees.

The aim of this section is to set up the vocabulary to talk about how the knowledge about some event or random variable influences the probabilities we should assign to other events. This leads us to talk about conditional probabilities and to discuss the case where events do not influence each other, giving rise to an important notion of probability theory called independence.

2.1 Conditional probability

We have already considered (in the course and on the example sheets) many unpredictable situations where several events naturally occur either at the same time or consecutively: a sequence of coin tosses or successive steps in a random walk, or different links or edges in a random graph. In all these cases, the fact that one event has happened could easily influence the others. For example, if you want to model the financial markets tomorrow, it seems rather advisable to take into account what happened today. To talk about the change of probabilities when we have observed something, we introduce the notion of conditional probability:

Definition 2.1 (Conditional probability). *Let $(\Omega, \mathcal{F}, \mathbb{P})$ be a probability space and $E \in \mathcal{F}$ with $\mathbb{P}(E) > 0$. Then for any $F \in \mathcal{F}$, we define the conditional probability of the event F given E (i.e. given that the event E happens), by*

$$\mathbb{P}(F|E) := \frac{\mathbb{P}(E \cap F)}{\mathbb{P}(E)}.$$

Recall that $E \cap F$ is the event that both E and F happen. Hence, as the denominator is always given by $\mathbb{P}(E)$, the conditional probability given E is proportional to $\mathbb{P}(E \cap F)$ for any event F . Here is the justification for dividing by $\mathbb{P}(E)$:

Lemma 2.2. *Let $(\Omega, \mathcal{F}, \mathbb{P})$ be a probability space and $E \in \mathcal{F}$ with $\mathbb{P}(E) > 0$. Then $\mathbb{P}(\cdot|E)$ defines a probability measure on $(\Omega, \mathcal{F})$, called the conditional probability measure given E .*

Proof. First, notice that $\mathbb{P}$ is indeed defined for every $F \in \mathcal{F}$. Next, $\mathbb{P}(\emptyset|E) = \mathbb{P}(\emptyset)/\mathbb{P}(E) = 0$ and $\mathbb{P}(\Omega|E) = \mathbb{P}(\Omega)/\mathbb{P}(E) = 1$. So it remains to check countable additivity.

So let $F_1, F_2, \dots \in \mathcal{F}$ be disjoint. Then also $E \cap F_1, E \cap F_2, \dots$ are also disjoint. Hence

$$\mathbb{P}\left(\bigcup_{i \geq 1} F_i | E\right) = \frac{\mathbb{P}\left(\left(\bigcup_{i \geq 1} F_i\right) \cap E\right)}{\mathbb{P}(E)} = \frac{\mathbb{P}\left(\bigcup_{i \geq 1} (F_i \cap E)\right)}{\mathbb{P}(E)} = \sum_{i \geq 1} \frac{\mathbb{P}(F_i \cap E)}{\mathbb{P}(E)} = \sum_{i \geq 1} \mathbb{P}(F_i | E),$$

and countable additivity follows. □

It should be remarked that conditional probability of an event might sometimes be similar to the initial probability (we will see more about this very soon), but it might also be drastically different. A somewhat silly but instructive example is the following:

- Conditional probability of the event E^c , conditioned on E is always zero, no matter what the original probability was;
- similarly the conditional probability of E , conditioned on E is always 1.

Or for a more senseful exercise consider the following:

Exercise 2.1 (Random walk and conditional probabilities). *Consider the simple random walk of length n .*

- *What is the probability that the walk ends up at the point n at time n ? Now, suppose that the first step was -1 . What is the probability that the walk ends up at the point n at time n now?*
- *Suppose that n is even. What is the probability that the walk ends up at the point 0 at time n ? Now, suppose that the first step was -1 . What is the probability that the walk ends up at the point 0 at time n now?*

One also has to be very careful about the exact conditioning, as two similarly sounding conditionings can induce very different conditional probabilities. In general, we need to know something extra about the relation of two events to know how the probability of one changes when conditioned on the other.

There are some cases where these relations and thus conditional probabilities are easy:

- When $E \subseteq F$, then the conditional probability of F given E is just 1.
- When $F \subseteq E^c$, then the conditional probability of F given E is just 0.
- The third case is when F and E are so called independent: in that case $\mathbb{P}(F|E) = \mathbb{P}(F)$ basically by definition (we will come back to that).

In general, there are not many tools to calculate conditional probabilities, but there is one very useful tool called the Bayes' formula or the Bayes' rule:

2.1.1 Bayes' rule

Proposition 2.3 (Bayes' rule). *Let $(\Omega, \mathcal{F}, \mathbb{P})$ be a probability space and E, F two events of positive probability. Then*

$$\mathbb{P}(E|F) = \frac{\mathbb{P}(F|E)\mathbb{P}(E)}{\mathbb{P}(F)}$$

It's not only that the statement looks innocent, but also the proof is a one-liner - by definition of conditional probability, we can write

$$\mathbb{P}(E|F)\mathbb{P}(F) = \mathbb{P}(E \cap F) = \mathbb{P}(F|E)\mathbb{P}(E).$$

Still, it is a very nice observation that allows us not only to calculate, but also is behind the framework of Bayesian statistics / Bayesian thinking about probability.

Let us here analyse a simple example.

Example 2.4. Consider the situation with three different coins: one has heads on both sides, one has tails on both sides, and one is a fair coin. Now someone picked using some procedure one of the three types of coins, told you that she tossed a coin and heads came up. Which coin did she toss?

The relevant probability space that contains the three coins and three tosses is as follows. First, the state space is pairs the product space $\{C_h, C_t, C_f\} \times \{H, T\}$ - the first coordinate describes the type of the coin, the second the result of the toss. As a σ -algebra we take the whole σ -algebra as we can ask both about what came up on top, and then which coin it was.

We know that to define $\mathbb{P}$ on a finite set with the power-set it suffices to define $\mathbb{P}$ for every element of the state-space. From the assumptions $\mathbb{P}(\{C_h, T\}) = \mathbb{P}(\{C_t, H\}) = 0$ and $\mathbb{P}(\{C_f, T\}) = \mathbb{P}(\{C_f, H\})$. If we further set $p_f = \mathbb{P}(\{\text{coin} = C_f\})$, $p_h = \mathbb{P}(\{\text{coin} = C_h\})$, $p_t = \mathbb{P}(\{\text{coin} = C_t\})$ it also has to hold that $p_f + p_t + p_h = 1$, leaving two free parameters altogether.

Let us now calculate the probabilities that we were interested in. Clearly,

$$\mathbb{P}(\{\text{coin} = C_t\}|\{\text{toss} = H\}) = 0$$

as the coin with two tails sides could not have produced heads. For the other combinations it is easiest to use Bayes' formula to calculate

$$\mathbb{P}(\{\text{coin} = c_h\}|\{\text{toss} = H\}) = \frac{\mathbb{P}(\{\text{toss} = H\}|\{\text{coin} = C_h\})\mathbb{P}(\{\text{coin} = C_h\})}{\mathbb{P}(\{\text{toss} = H\})} = \frac{\mathbb{P}(\{\text{coin} = C_h\})}{\mathbb{P}(\{\text{toss} = H\})}$$

and

$$\mathbb{P}(\{\text{coin} = c_f\}|\{\text{toss} = H\}) = \frac{\mathbb{P}(\{\text{toss} = H\}|\{\text{coin} = C_f\})\mathbb{P}(\{\text{coin} = C_f\})}{\mathbb{P}(\{\text{toss} = H\})} = \frac{\mathbb{P}(\{\text{coin} = C_f\})}{2\mathbb{P}(\{\text{toss} = H\})}.$$

Thus we see that

$$\frac{\mathbb{P}(\{\text{coin} = c_h\}|\{\text{toss} = H\})}{\mathbb{P}(\{\text{coin} = c_f\}|\{\text{toss} = H\})} = \frac{2\mathbb{P}(\{\text{coin} = c_h\})}{\mathbb{P}(\{\text{coin} = c_f\})} = 2p_h/p_f$$

and given that

$$\mathbb{P}(\{\text{coin} = c_h\}|\{\text{toss} = H\}) + \mathbb{P}(\{\text{coin} = c_f\}|\{\text{toss} = H\}) = 1$$

we conclude our estimates

$$\mathbb{P}(\{\text{coin} = c_f\}|\{\text{toss} = H\}) = \frac{p_f}{p_f + 2p_h}$$

and

$$\mathbb{P}(\{\text{coin} = c_h\}|\{\text{toss} = H\}) = \frac{2p_h}{p_f + 2p_h}.$$

What can we conclude? The first thing is maybe that without having any knowledge of how likely each coin was to begin with, we cannot say much about the final answer, as it contains that information! What we assume about the initial probability of each coin matters a lot: if we estimate that the coin with two heads was very unlikely compared to the fair coin, say $p_h = 0.000001p_f$, then after seeing heads our estimate gives $\mathbb{P}(\{\text{coin} = c_f\}|\{\text{toss} = H\}) = 0.999999$. If however we have no reason to believe that any one coin was more likely to be taken than any other, for example because the person tossing the coin just picked it randomly among the three possibilities, then we have $p_f = p_h = p_t = 1/3$ and our formula gives $\mathbb{P}(\{\text{coin} = c_f\}|\{\text{toss} = H\}) = 1/3$ and $\mathbb{P}(\{\text{coin} = c_h\}|\{\text{toss} = H\}) = 2/3$.

However, an important point is that independently of the initial probabilities, we can say how the probabilities or rather the ratios of probabilities changed - our guess that it was the coin was heads/heads went up two times w.r.t. to the fair coin. In fact, as you will see on the exercise sheet if we could follow more tosses we would become more and more knowledgeable which coin it was, independently of our possibly bad initial estimate. This is also the idea behind Bayesian approach to probability models - we may not know all the parameters to begin with, but we can then just fill them with guesses and as we observe more and more about the world, we can a posteriori improve on these guesses and make our models better.

2.1.2 Law of total probability

Although conditional probabilities are often tricky, they are necessary to deal with and even useful. For example, they help to decompose the probability space. Indeed, the following result is a generalization of the following intuitive result: if you know that exactly one of three events E_1, E_2, E_3 happens, then to understand the probability of any other event F , it suffices to understand the conditional probabilities of this event, conditioned on each of E_i , i.e. the probabilities $\mathbb{P}(F|E_i)$.

Proposition 2.5 (Law of total probability). *Let $(\Omega, \mathcal{F}, \mathbb{P})$ be a probability space. Further, let I be countable and $(E_i)_{i \in I}$ be disjoint events with positive probability $\Omega = \bigcup_{i \in I} E_i$. Then for any $F \in \mathcal{F}$, we can write*

$$\mathbb{P}(F) = \sum_{i \in I} \mathbb{P}(F|E_i)\mathbb{P}(E_i).$$

Proof. As $\Omega = \bigcup_{i \in I} E_i$ we have $\mathbb{P}(F) = \mathbb{P}(F \cap (\bigcup_{i \in I} E_i))$.

Now rewrite $F \cap (\bigcup_{i \in I} E_i) = \bigcup_{i \in I} (F \cap E_i)$. Because $(E_i)_{i \in I}$ are disjoint, so are $(F \cap E_i)_{i \in I}$. Hence again by countable additivity for disjoint sets

$$\mathbb{P}(F) = \mathbb{P}\left(\bigcup_{i \in I} (F \cap E_i)\right) = \sum_{i \in I} \mathbb{P}(F \cap E_i).$$

Now, by definition $\mathbb{P}(F \cap E_i) = \mathbb{P}(F|E_i)\mathbb{P}(E_i)$ and the proposition follows. □

Remark 2.6. *In fact pretty much the same proof works if E_i don't cover the full space, but we only know that $\mathbb{P}(\Omega \setminus (\bigcup_i E_i)) = 0$. This generalisation is left as an exercise.*

2.2 Independence of events

Conditional probabilities are of course not at all difficult when the probability of an event does not change under conditioning - i.e. when $\mathbb{P}(E|F) = \mathbb{P}(E)$. Such pairs of events are called independent. In fact the rigorous definition is slightly different:

Definition 2.7 (Independence for two events). *Let $(\Omega, \mathcal{F}, \mathbb{P})$ be a probability space. We say that two events E, F are independent if $\mathbb{P}(E \cap F) = \mathbb{P}(E)\mathbb{P}(F)$.*

Observe that when $\mathbb{P}(F) > 0$, then we get back to the intuitive statement of independence, i.e. that $\mathbb{P}(E|F) = \mathbb{P}(E)$. Indeed, if E and F are independent we can write

$$\mathbb{P}(E|F) = \frac{\mathbb{P}(E \cap F)}{\mathbb{P}(F)} = \frac{\mathbb{P}(E)\mathbb{P}(F)}{\mathbb{P}(F)} = \mathbb{P}(E).$$

We have chosen the other definition, as then we automatically also include the case where possibly $\mathbb{P}(F) = 0$.

Example 2.8. Consider our model of a uniform random number among $\{1, 2, 3, \dots, 12\}$ and the events $E_1 := \{\text{the number is equal to 1}\}$, $E_2 := \{\text{the number is divisible by 2}\}$, $E_3 := \{\text{the number is divisible by 3}\}$. Which of these are independent?

From a direct calculation, we have $\mathbb{P}(E_1) = 1/12$, $\mathbb{P}(E_2) = 1/2$ and $\mathbb{P}(E_3) = 1/3$. But also we can directly calculate that $\mathbb{P}(E_1 \cap E_2) = \mathbb{P}(E_1 \cap E_3) = 0$ and $\mathbb{P}(E_2 \cap E_3) = \mathbb{P}(\{\text{the number is divisible by 6}\}) = 1/6$. We conclude that E_2, E_3 are independent, but E_1 and E_2 are not, neither are E_1, E_3 .

Already in this examples we actually had three events and one could also ask if there is some sort of notion of joint independence that generalises to more events. And indeed there are two different ways to generalize independence to several events:

- mutual or joint independence
- and pairwise independence

The stronger and more important notion is that of mutual independence.

Definition 2.9 (Mutual independence). Let $(\Omega, \mathcal{F}, \mathbb{P})$ be a probability space and let I be an index set. Then the events $(E_i)_{i \in I}$ are called mutually independent if for any finite subsets $I_1 \subseteq I$ we have that

$$\mathbb{P}\left(\bigcap_{i \in I_1} E_i\right) = \prod_{i \in I_1} \mathbb{P}(E_i).$$

Sometimes one does not have the full mutual independence or at least does not know it holds, and just pairwise independence can be asserted. There are similar notions of k -wise independence too.

Definition 2.10 (Pairwise independence). Let $(\Omega, \mathcal{F}, \mathbb{P})$ be a probability space and let I be an index set. Then the events $(E_i)_{i \in I}$ are called pairwise independent if for any $i \neq j \in I$ the events E_i and E_j are independent.

It is important to notice that, whereas mutual independence clearly implies pairwise independence, the opposite is not true in general:

Exercise 2.2 (Pairwise independent but not mutually independent). Consider the probability space for two independent coin tosses. Let E_1 denote the event that the first coin comes up heads, E_2 the event that the second coin comes up heads and E_3 the event that both coin come up on the same side. Show that E_1, E_2, E_3 are pairwise independent but not mutually independent.

Finally, one can also talk about independence of collections of events. This will be important when we try to generalize the notion of independence from events to random variables

Definition 2.11 (Mutual independence of collections of events). Consider two collections events $(E_i)_{i \in I}$ and $(F_j)_{j \in J}$ all defined on the same probability space. We say that they are independent if for all $i \in I, j \in J$:

$$\mathbb{P}(E_i \cap F_j) = \mathbb{P}(E_i)\mathbb{P}(F_j).$$

In case of several different collections of events $(E_{j,i})_{i \in I_j}$ for $j = 1 \dots$, we say that these collections are mutually independent if for any finite subset $J_1 \subseteq J$ and any events E_{j,i_j} with $j \in J_1$, it holds that

$$\mathbb{P} \left(\bigcap_{j \in J_1} E_{j,i_j} \right) = \prod_{j \in J_1} \mathbb{P}(E_{j,i_j}).$$

Equivalently, we ask any subset of events E_{j,i_j} from different collection to be mutually independent.

Before going to the independence of random variables, here are some basic properties of independence for events:

Lemma 2.12 (Basic properties). *Let $(\Omega, \mathcal{F}, \mathbb{P})$ be a probability space.*

- *If E is an event with $\mathbb{P}(E) = 1$ then it is independent of all other events.*
- *If E, F are independent, then also E^c and F are independent. In particular every event with $\mathbb{P}(E) = 0$ is independent of all other events.*
- *Finally, if an event is independent of itself, then $\mathbb{P}(E) \in \{0, 1\}$.*

Proof. This is on the example sheet. □

2.3 Independence of random variables

We now formalise the notion of independence for random quantities, i.e. random variables. Recall that (the law of) a random variable X is characterized by all events $\{X \in (a, b)\}$ for intervals (a, b) . The mutual independence of random variables is then defined as mutual independence of these sets of events. More precisely,

Definition 2.13 (Mutually independent random variables). *Let I be an index set and $(X_i)_{i \in I}$ a family of random variables defined on the same probability space $(\Omega, \mathcal{F}, \mathbb{P})$. We say that these random variables are mutually independent if for every finite set $J \subseteq I$ and all set of intervals $((a_j, b_j))_{j \in J}$ we have that*

$$\mathbb{P} \left(\bigcap_{j \in J} \{X_j \in (a_j, b_j)\} \right) = \prod_{j \in J} \mathbb{P}(X_j \in (a_j, b_j)).$$

Remark 2.14. *The more structurally sound definition would use instead as the collection all Borel sets $E_j \in \mathcal{F}_{\mathcal{B}}$. However, that is impractical, and in fact turns out (via some non-trivial measure theory) to be equivalent to the condition above.*

There are naturally more equivalent conditions. For example, a useful one as we see later is the following:

Exercise 2.3. *Consider random variables $X_1, X_2, \dots$ defined on the same probability space $(\Omega, \mathcal{F}, \mathbb{P})$. Then $X_1, X_2, \dots$ are mutually independent if and only if for every $m \geq 2$ and all pairs $a_j \in \mathbb{R}$ we have that*

$$\mathbb{P} \left(\bigcap_{1 \leq j \leq m} \{X_j \leq a_j\} \right) = \prod_{1 \leq j \leq m} \mathbb{P}(X_j \leq a_j).$$

Further, we again have a very nice and simple condition for random variables defined on discrete probability spaces.

Lemma 2.15 (Independence on the discrete probability space). *Let $X_1, \dots, X_n$ be defined on a discrete probability space. Then $X_1, \dots, X_n$ are mutually independent if and only if for every $s_1, \dots, s_n \in \mathbb{R}$, we have that*

$$\mathbb{P}\left(\bigcap_{i=1}^n \{X_i = s_i\}\right) = \prod_{i=1}^n \mathbb{P}(X_i = s_i).$$

*The same holds more generally if $X_1, \dots, X_n$ are defined on any probability space but each take only a discrete number of values with full probability, i.e. for each of them there is some countable set S_i such that $\mathbb{P}(X_i \in S_i) = 1$.*⁶

Proof. This is left as an exercise. □

As a sanity check it is now simple to see that the indicator events E, F of two events are independent if and only if E, F are independent as events: indeed $\mathbb{P}(\{1_E = x\}\{1_F = y\})$ is equal to

$$1_{x=1}1_{y=1}\mathbb{P}(E)\mathbb{P}(F) + 1_{x=1}1_{y=0}\mathbb{P}(E)\mathbb{P}(F^c) + 1_{x=0}1_{y=1}\mathbb{P}(E^c)\mathbb{P}(F) + 1_{x=0}1_{y=0}\mathbb{P}(E^c)\mathbb{P}(F^c)$$

which in turn can be rewritten as

$$(1_{x=1}\mathbb{P}(E) + 1_{x=0}\mathbb{P}(E^c))(1_{y=1}\mathbb{P}(F) + 1_{y=0}\mathbb{P}(F^c)) = \mathbb{P}(\{1_E = x\})\mathbb{P}(\{1_F = y\}).$$

Exercise 2.4 (Simple symmetric random walk). *Prove that for a simple random walk of length n all the increments of the walk, i.e. $\Delta_i = S_i - S_{i-1}$ for $i = 1 \dots n$, are mutually independent random variables.*

The notion of independent random variables is very important and widely used - often also just because otherwise it is very difficult to do any calculations!

Remark 2.16 (i.i.d. random variables). *Often one talks about collection of i.i.d. random variables $(X_j)_{j \in J}$ - this means that $(X_j)_{j \in J}$ are mutually independent (first 'i') and all have the same probability law, i.e. are identically distributed (the 'i.d.'). Intuitively, this corresponds to repeating the very same random situation or experiment over and over again.*

Now, we started the course by constructing probability spaces and then defining random variables on it. However, there are natural cases where one would like to go in the opposite direction - we know from observation or experience that we would like to study a bunch of independent random variables and our question is how to construct a probability space where they live? This might sound somewhat silly, but in fact mathematically it is not an easy question! We will partly deal with this question in the next subsection.

2.4 Independence and product probability spaces

Whereas independence is a probabilistic concept, it comes out that it is related also to a structure in measure spaces.

Let us consider an example to see this.

Example 2.17 (The space for n fair coin tosses). *We have seen that the probability space for n fair coin tosses can be modelled by taking the state space Ω to be the set of all n -tuples*

⁶Such random variables are called discrete random variables, as we will see soon.

$\{x_1, \dots, x_n\}$ of length n with each $x_i \in \{H, T\}$, then taking $\mathcal{F}$ to be the power set and finally setting the probability of each singleton, i.e. each n -tuple, to be 2^{-n} .

Now, let us look at this as follows:

- Each n -tuples is just an element of the product space $\{H, T\} \times \dots \times \{H, T\}$, so we can use as Ω the product space. Let's denote also by $\Omega_0 = \{H, T\}$ the state spaces for the coordinates.
- The power-set is the smallest σ -algebra containing all sets of the form $E_1 \times \dots \times E_n$ with each E_i in the power-set of a single coordinate $\{H, T\}$
- The uniform probability measure on Ω satisfies by definition

$$\mathbb{P}(E_1 \times \dots \times E_n) = \mathbb{P}_0(E_1) \dots \mathbb{P}_0(E_n),$$

where $\mathbb{P}_0$ is the uniform probability measure on the space of a single toss.

- Finally the fact that the tosses are independent comes down to the following: all events $F_1, \dots, F_n$ of the form $F_i = \Omega_0 \times \dots \times E_i \times \dots \times \Omega_0$ with $E_i \in \mathcal{F}_i$ are mutually independent: indeed for $i \neq j$ we have for example

$$\mathbb{P}(\Omega_0 \times \Omega_0 \times \dots \times E_i \times \dots \times \Omega_0 \cap \Omega_0 \times \Omega_0 \times \dots \times E_j \times \dots \times \Omega_0) = \mathbb{P}(\Omega_0 \times \Omega_0 \times E_i \times \Omega_0 \dots \times E_j \times \Omega_0 \dots \times \Omega_0)$$

which by above equals $\mathbb{P}_0(E_i) \times \mathbb{P}_0(E_j)$ which again by above is equal to the product of $\mathbb{P}(\Omega_0 \times \Omega_0 \times \dots \times E_i \times \dots \times \Omega_0)$ and $\mathbb{P}(\Omega_0 \times \Omega_0 \times \dots \times E_j \times \dots \times \Omega_0)$.

So we see that in some sense the product structure goes in hand with independence. And indeed, this is the general rule - mutual independence of random variables is naturally linked to products of probability spaces.

Let us follow this through mathematically, by first discussing product spaces in general and then looking at the construction of probability spaces for independent random variables.

2.4.1 Construction of product spaces

So let us have a brief look at the construction of product spaces. Consider probability spaces $(\Omega_i, \mathcal{F}_i, \mathbb{P}_i)$ for $i = 1, 2, \dots$. Then to construct the product probability space we need a product σ -algebra and a product measure.

- (1) The product σ -algebra $\mathcal{F}_\Pi$ is simple and natural: it is the smallest σ -algebra containing all $E_{i_1} \times \dots \times E_{i_n}$ with $E_{i_j} \in \mathcal{F}_{i_j}$ for all $j = 1 \dots n$ and $\{i_j\}_{j=1 \dots n}$ a finite subset of $\mathbb{N}$.
- (2) The product probability measure $\mathbb{P}_\Pi$ of $\mathbb{P}_1, \mathbb{P}_2, \dots$ on $(\Pi_{i \geq 1} \Omega_i, \mathcal{F}_\Pi)$ also sounds simple: it is the only probability measure such that

$$\mathbb{P}(E_{i_1} \times \dots \times E_{i_n}) = \prod_{j=1}^n \mathbb{P}_i(E_{i_j})$$

for all $E_{i_1} \times \dots \times E_{i_n}$ with $E_{i_j} \in \mathcal{F}_{i_j}$ for $j = 1 \dots n$. However, its construction and uniqueness even in the case of finite products is technical for general probability spaces and out of the scope of this course.

Thus we will state the following theorem without proof, which you will see in the measure theory or the third year probability course:

Theorem 2.18 (Product measure // admitted). *For $i \in \mathbb{N}$, let $(\Omega_i, \mathcal{F}_i, \mathbb{P}_i)$ be probability spaces. Then there exists a unique probability measure $\mathbb{P}_\Pi$ on $(\Pi_{i \in \mathbb{N}} \Omega_i, \mathcal{F}_\Pi)$ such that for any*

finite subset $J \subset \mathbb{N}$ and any event E of the form $E = \prod_{i \in \mathbb{N}} F_i$ with $F_i = \Omega_i$ for $i \notin J$ and $F_i = E_i \in \mathcal{F}_i$ for $i \in J$, we have that

$$(2.1) \quad \mathbb{P}_\Pi(E) = \prod_{i \in J} \mathbb{P}_i(E_i).$$

We call such a measure the product measure of the collection $((\Omega_i, \mathcal{F}_i, \mathbb{P}_i))_{i \geq 1}$.

It is rather easy to see the existence and uniqueness in the case of a finite number of discrete probability spaces, so let us do that. Below, we state it in the case where the σ -algebras are equal to the power set, but as discussed before (see Proposition 1.9, this essentially encompasses the case of general σ -algebras on discrete spaces.

Lemma 2.19 (Discrete product spaces). *Let $(\Omega_i, \mathcal{P}(\Omega_i), \mathbb{P}_i)$ for $i = 1 \dots n$ be discrete probability spaces. Then the product probability $\mathbb{P}_\Pi$ measure on $(\prod_{i=1}^n \Omega_i, \mathcal{F}_\Pi)$ exists and is unique.*

Proof. On the example sheet

□

2.4.2 Probability spaces for independent random variables

We will now follow through the philosophy alluded to above:

- if we are given some laws of random variables and we want to construct a common probability space on which all of these random variables are defined and are moreover mutually independent, then we should use product spaces.

We will again state this proposition in a larger generality than we prove it.

Theorem 2.20 (Existence of probability spaces with independent random variables // partly admitted). *Consider random variables $(X_i)_{i \geq 1}$. Then we can find a common probability space $(\Omega, \mathcal{F}, \mathbb{P})$ and random variables $(\tilde{X}_i)_{i=1 \geq 1}$ defined on $(\Omega, \mathcal{F}, \mathbb{P})$ such that*

- For all $i \geq 1$, $\tilde{X}_i$ has the law of X_i
- Moreover, the random variables $(\tilde{X}_i)_{i \geq 1}$ are mutually independent.

Example 2.21. *Suppose you have a coin that is not fair, but comes up heads with probability $p \in (0, 1)$. How would you model the sequence of independent n such tosses?*

The assumption of all sequences being equally likely does not make sense any longer (e.g. think of the case when p is near 1, then certainly the sequence of all zeros and all ones cannot have the same probabilities). However, the assumption of mutual independence and its relation to product measures are useful.

Indeed, we can define the probability space as follows:

- we take the product space of n copies of $(\{0, 1\}, \mathcal{P}(\{0, 1\}), \mathbb{P}_p)$, where $\mathbb{P}_p$ such that it gives 1 with probability p and 0 with probability $1 - p$.

Notice that in this probability space, the probability of a fixed sequence of n tosses with m heads and tails $n - m$ is exactly $p^m(1 - p)^{n-m}$. If we further want to calculate the probability that we have exactly m heads we have to sum over all sequences with m heads and we get $\binom{n}{m} p^m(1 - p)^{n-m}$. Check that $\sum_{m=0}^n \binom{n}{m} p^m(1 - p)^{n-m} = 1$!

Let us now give the proof of the theorem in the case when all the random variables are defined on discrete probability spaces. For a slightly more natural statement, see the exercise sheet

Proof of Theorem 2.20, case of finite products of random variables on discrete spaces. Suppose we have discrete probability spaces $(\Omega_i, \mathcal{P}(\Omega_i), \mathbb{P}_i)$ and random variables $X_i : \Omega_i \rightarrow \mathbb{R}$.

By the Lemma 2.19 above, we can construct the product probability space corresponding to these probability spaces, denoted $(\Omega_\Pi = \prod_{i=1}^n \Omega_i, \mathcal{F}_\Pi, \mathbb{P}_\Pi)$.

Now, define $\tilde{X}_i(\omega_1, \dots, \omega_n) := X_i(\omega_i)$. One can check that $\tilde{X}_i$ thus defined are all random variables and they are defined to have the same law as X_i . Indeed, by the definition of $\tilde{X}_i$ and the product measure

$$\mathbb{P}_{\tilde{X}_i}(E) = \mathbb{P}_\Pi(\Omega_1 \times \Omega_2 \cdots \times X_i^{-1}(E) \times \dots \times \Omega_n) = \mathbb{P}_{X_i}(E).$$

Finally, we need to check that the random variables $(\tilde{X}_i)_{i=1 \dots n}$ are mutually independent on the space $(\prod_{i=1}^n \Omega_i, \mathcal{F}_\Pi, \mathbb{P}_\Pi)$. From the identity

$$\{w : \Omega_\Pi : \tilde{X}_j(\omega) \in E_j\} = \{\Omega_1 \times \cdots \times X_i^{-1}(E) \times \cdots \times \Omega_n\}$$

we have that:

$$\mathbb{P}_\Pi\left(\bigcap_{i=1 \dots n} \{\tilde{X}_i \in E_i\}\right) = \mathbb{P}_\Pi(\prod_{i=1}^n X_i^{-1}(E_i)).$$

By the definition of product measure this equals $\prod_{i=1}^n \mathbb{P}_{X_i}(E_i)$, which in turn equals $\prod_{i=1}^n \mathbb{P}_{\tilde{X}_j}(E_j)$ by equality in law. The last expression is equal to $\prod_{i=1}^n \mathbb{P}_\Pi(\tilde{X}_i \in E_i)$ by definition and we conclude. $\square$

Let us finish this section by playing with an important example.

2.4.3 Erdős-Renyi random graph

Our aim in this section is to describe and study random graphs. Graphs are simple mathematical structures that help to describe networks like social networks, or logistic networks or why not the network of neurons in the brain.

Definition 2.22 (Simple graph). *Let $n \in \mathbb{N}$. A simple graph is a pair $G = (V, E)$ where V is a set of points $V = \{v_1, \dots, v_n\}$, called vertices, and E is a subset of $\{\{v_i, v_j\} : (v_i, v_j) \in V \times V, v_i \neq v_j\}$, i.e. a set of unordered pairs of distinct vertices, called edges.*

You can imagine the graph as drawing all the n points $v_1, \dots, v_n$ on the plane and then drawing a line between v_i and v_j to say they are connected if and only if $\{v_i, v_j\} \in E$.

If the networks are very big, like the brain or the social network in Facebook, it is both impractical and unfeasible to describe them in all detail. Moreover, it comes out that usually they start resembling certain random networks. Thus in order to understand properties of these real world networks, one often studies the simplified models of random networks.

The easiest model of a random network, or in our mathematical language of a random graph, is the Erdős-Renyi random graph where we include each edge with probability $p > 0$.

Example 2.23 (Erdős-Renyi random graph). *For $n \in \mathbb{N}$ consider a set of vertices V of size n and let E be the set of all undirected edges between these vertices.*

The Erdős-Renyi random graph $G_{n,p}$ of size n and edge parameter $p \in [0, 1]$ is then defined by including each possible edge independently with probability p .

To define the relevant probability space we let

- The state space should include all possible graphs with the vertex set V . We observe that this can be done by determining the edge set. So we let $\Omega = \{0,1\}^E$ be the set of all possible edge configurations on n vertices - we interpret 1 to mean that an edge is present.
- We assume that we can check for any edge if it is present or not, and thus set $\mathcal{F} = \mathcal{P}(\Omega)$
- Finally, we set each edge to be present with probability p independently of others. In other words for each $\omega \in \Omega$ we set

$$\mathbb{P}_p(\{\omega\}) := p^{|\omega|}(1-p)^{n-|\omega|},$$

where $\omega \in \Omega$ is an edge configuration and $|\omega|$ is the number of edges in this configuration.

Finally, we can identify each element ω also with the resulting graph $G_{n,p}(\omega) = (V, E(\omega))$.

What are some questions that we would like to look at? Roughly we would like to answer how the graph looks like when n is very large, i.e. tending to infinity. Of course sometimes one could be also interested in n small, but then one could actually explicitly describe the probability of each possible graph and picture it.

Now to describe how the graph looks like we could consider the following questions:

- (1) How many edges are present?
- (2) Is the graph connected, i.e. can one find for each $v, w \in V$ a set of edges $e_1, \dots, e_n$ such that each e_i, e_{i-1} share a vertex and e_1 is connected to v and e_n connected to w ?
- (3) If yes, what is the maximal distance between two vertices?
- (4) If no, how many different connected components are there?
- (5) What is the biggest connected component?
- (6) ...

Each of these questions is about a single graph, i.e. a single configuration ω . Thus in the random graph model they correspond either to an event or random variable, whose probability or law we can study.

For example, $N_E : \Omega \rightarrow \mathbb{N}$ given by $N_E(\omega) := |\omega|$ attaches to each ω its number of edges and thus corresponds to the first question. Similarly the event $F := \{\omega \text{ is connected}\}$ corresponds to the second question. Of course there are also more complex questions, which arise when one considers several questions at the same time.

One is interested in both how the probability of these events behaves for $p \in [0, 1]$ fixed and $n \rightarrow \infty$, but also how this behaviour changes when we change p . Notice that a priori p does not need to be constant, we can also easily consider a sequence of graphs $G_{n,p(n)}$ where $p(n)$ is a function of n .

Studying the properties of Erdős-Renyi random graphs was and still is a very active research topic, with hundreds if not thousands of papers written about them. We will try to just get a very small taste of this research.

Let us concentrate on one notion, that of connectivity and look at some scenarios. Notice that when $p = 1$ then the graph is connected with probability 1 and when $p = 0$ it is disconnected with probability 1. We will try to get a grasp what happens with $p_n \in (0, 1)$ possibly changing with n .

Claim 2.24. *Let $p \in (0, 1)$ be fixed. Then as $n \rightarrow \infty$ the probability of the graph being connected converges to 1 almost surely.*

This is maybe not so surprising as with fixed probability p we will have lots of edges: indeed, if you think of edges as coin tosses, you would expect to have a proportion p of all edges to be present, which makes $pn(n-1)/2$ edges!

Proof. We will prove that $\mathbb{P}_p(\{G_{n,p} \text{ is not connected}\}) \rightarrow 0$ as $n \rightarrow \infty$. First notice that

$$\{G_{n,p} \text{ is not connected}\} = \cup_{v \neq w \in V} \{v, w \text{ not connected by a path}\}.$$

Thus by the union bound

$$\mathbb{P}_p(\{G_{n,p} \text{ is not connected}\}) \leq 1/2 \sum_{v \neq w \in V} \mathbb{P}_p(\{v, w \text{ not connected by a path}\}),$$

where the $1/2$ comes from the fact that we count each edge twice in the sum. But because of symmetry of the model, each pair of edges is equivalent, so we can write the right hand side as $n(n-1)/4 \mathbb{P}_p(\{v, w \text{ not connected by a path}\})$.

Thus we want to bound the probability that v and w are not connected by a path. First, just looking at the edge $\{v, w\}$ is not enough - this edge is absent with probability $1-p$, which doesn't go to zero. However, there are many other ways to connect these two vertices.

One way is to use an intermediate vertex z : then v and w are not connected if and only if there is no vertex z such that both $\{z, w\}$ and $\{z, v\}$ belong to the edge set. Thus we can write

$$\mathbb{P}_p(\{v, w \text{ not connected by a path}\}) \leq \prod_{z \in V \setminus \{v, w\}} \mathbb{P}_p(\{\{v, z\} \notin E\} \cup \{\{w, z\} \notin E\}).$$

But now $\mathbb{P}_p(\{\{v, z\} \notin E\} \cup \{\{w, z\} \notin E\}) = 1 - \mathbb{P}_p(\{\{v, z\} \in E\} \cap \{\{w, z\} \in E\}) = 1 - p^2$ and hence

$$\mathbb{P}_p(\{v, w \text{ not connected by a path}\}) \leq (1 - p^2)^{n-2}.$$

This clearly goes to zero as $n \rightarrow \infty$ and thus any two fixed vertices will be connected with probability going to 1.

We now come back to our initial probability of all pairs being connected and bound:

$$\mathbb{P}_p(\{G_{n,p} \text{ is not connected}\}) \leq n(n-1)(1 - p^2)^{n-2}/4.$$

This is also nicely goes to zero!

□

In fact, if we look at the proof more carefully we see that the claim is true as long as $p = p(n)$ goes to zero with n sufficiently slowly. In other words the exact same proof gives us

Claim 2.25. *Let $(p_n)_{n \geq 1}$ be a sequence of numbers in $[0, 1]$ satisfying $p_n \geq n^{-1/4}$. Then as $n \rightarrow \infty$ the probability of the graph being connected converges to 1 almost surely.*

Proof. We follow the proof above and notice that for $1 \geq p_n \geq n^{-1/4}$ we still have that

$$n(n-1)(1 - p_n^2)^{n-2}/4 \rightarrow 0$$

as $n \rightarrow \infty$.

□

On the other hand, we have that

Claim 2.26. *Let $(p_n)_{n \geq 1}$ be a sequence of numbers in $[0, 1]$ such that $p_n \leq n^{-2}$. Then as $n \rightarrow \infty$ the probability of the graph being connected converges to 0 almost surely.*

This will be on the exercise sheet. But notice the interesting phenomena: there seems to be a sort of threshold effect. If p_n decays very fast, the probability of connectedness goes to 0; if decays slowly enough it goes to 1. Why doesn't it go to some other number between 0 and 1? Where is the exact threshold? It is a non-trivial theorem that says this threshold is exactly at $p_n = \frac{\log n}{n}$!

SECTION 3

Random variables and random vectors

In this chapter, we will look more closely into random variables and n -tuples of random variables, called random vectors.

3.1 The cumulative distribution function of a random variable

Recall that we call two random variables equal in law, when the probability measures they induce on $(\mathbb{R}, \mathcal{F}_B)$ are equal - this allowed us to compare random variables defined on different probability spaces, coming up in different contexts.

Our first aim is to see how to classify and compare random variables more easily. Indeed, for now one has to actually determine. We already saw that the law of each random variable is described by the probability over all possible events, but this is a description that is very difficult to deal with.

It comes out that all the information about the law of a random variable can be uniquely encoded using what is called a cumulative distribution function.

Definition 3.1 (Cumulative distribution function). *We call a function $F : \mathbb{R} \rightarrow [0, 1]$ a (cumulative) distribution function (abbreviated c.d.f.) if it satisfies the following conditions:*

- (1) F is non-decreasing;
- (2) $F(x) \rightarrow 0$ as $x \rightarrow -\infty$ and $F(x) \rightarrow 1$ as $x \rightarrow \infty$;
- (3) F is right-continuous, i.e. for any $x \in \mathbb{R}$ and any sequence $(x_n)_{n \geq 1} \in [x, \infty)$ such that $x_n \rightarrow x$, we have that $F(x_n) \rightarrow F(x)$.

Given a random variable X , we define its cumulative distribution function as follows:

Proposition 3.2 (Cum.dist. function of a random variable). *For each random variable X (defined on some probability space $(\Omega, \mathcal{F}, \mathbb{P})$), the function $F_X(x) := \mathbb{P}_X((-\infty, x])$ defines a cumulative distribution function (c.d.f.).*

Proof. Set $F_X(x) = \mathbb{P}(X \in (-\infty, x])$. Then as $(-\infty, x] \subseteq (-\infty, y]$ for $x \leq y$, we have by (1) of Proposition 1.12 that F is non-decreasing.

Let us next check right-continuity of F . So let $(x_n)_{n \geq 1}$ be any sequence in $[x, \infty)$ converging to x . Then setting $A_n := \cap_{1 \leq k \leq n} (-\infty, x_k]$ we get that $\bigcap_{n \geq 1} A_n = (-\infty, x]$. By continuity of $\mathbb{P}$, i.e. (5) of Proposition 1.12, it follows that $\mathbb{P}_X(A_n) \rightarrow \mathbb{P}_X((-\infty, x])$. But now notice that as $y_n \rightarrow y$, we have that $\{-\infty, y_n\} \subseteq A_{m_n}$ for some subsequence m_n with $m_n \rightarrow \infty$ as $n \rightarrow \infty$. It follows that $F_X(y) \leq F_X(y_n) \leq \mathbb{P}_X(A_{m_n})$ and we conclude that $F_X(y_n) \rightarrow F_X(y)$ as $n \rightarrow \infty$.

The final two claims are on the example sheet. □

In fact, it comes out the conversely each cumulative distribution function gives rise to a unique law of a random variable.

Theorem 3.3 (Laws of random variable are uniquely determined by c.d.f. // admitted). *Each cumulative distribution function F gives rise to a unique law of a random variable X such that $F_X(x) = \mathbb{P}_X((-\infty, x])$. In other words c.d.f.s are in one to one correspondence with probability measures $\mathbb{P}$ on $(\mathbb{R}, \mathcal{F}_B)$.*

We admit this theorem in the general case, but will again prove the discrete case. Let us look at a simple example:

Example 3.4. Let us calculate the c.d.f of the so called Bernoulli random variable X that takes value 1 with probability p and 0 with probability $1-p$. Notice that all indicator functions of events correspond to such random variables with $\mathbb{P}(E) = p$.

We have $F_X(x) = (1-p)1_{x \geq 0} + p1_{x \geq 1}$. More generally for a random variable that takes only finite number of values $x_1, \dots, x_n$ with probabilities $p_1, \dots, p_n$, we have $F_X(x) = \sum_{i=1 \dots n} p_i 1_{x \geq x_i}$. (Why?)

Thus we see that F_X encodes the behaviour of X rather naturally. Let us now look at this relation between the cumulative distribution function F_X and the random variable X more closely. By $F(x-)$ we denote the limit of $F(x_n)$ with $(x_n)_{n \geq 1} \rightarrow x$ from below, i.e. by numbers $x_n < x$.

Lemma 3.5 (C.d.f vs r.v.). Let X be a random variable on some probability space $(\mathbb{P}, \Omega, \mathcal{F})$ and F_X its cumulative distribution function. Then for any $x < y \in \mathbb{R}$

- (1) $\mathbb{P}(X < x) = F(x-)$
- (2) $\mathbb{P}(X > x) = 1 - F(x)$
- (3) $\mathbb{P}(X \in (x, y)) = F(y-) - F(x)$.
- (4) $\mathbb{P}(X = x) = F(x) - F(x-)$.

Proof. This is on exercise sheet. □

Example 3.6. Let us also exhibit the c.d.f. of the uniform random variable U taking values uniformly in $[0, 1]$. It is given by $F_U := x1_{x \in [0, 1]} + 1_{x > 1}$. By the proposition above we can see that for any interval $(a, b) \subseteq [0, 1]$, $\mathbb{P}(U \in (a, b)) = b - a$.

From above we see that all jumps of F_X correspond to points where $\mathbb{P}_X(X = x) > 0$. In fact there can be only countably many of them.

Lemma 3.7. A cumulative distribution function F_X of a random variable X has at most countably many jumps.

Proof. Let S_n be the set of jumps that are larger than $1/n$ and $\hat{S}_n$ any finite subset of S_n . Then $\hat{S}_n$ is measurable and $1 \geq \mathbb{P}(X \in S_n) \geq |\hat{S}_n|n^{-1}$. Thus it follows that $|\hat{S}_n| \leq n$. As this holds for any finite subset of S_n , we deduce that $|S_n| \leq n$ and in particular S_n is finite.

Now the set of all jumps can be written as a union $\bigcup_{n \geq 1} S_n$. Hence as each S_n is finite and a countable union of finite sets is countable, we conclude. □

These jumps of a c.d.f. F_X are sometimes called atoms of the law of X . More precisely, we call $s \in \mathbb{R}$ an atom for the law of X if and only if $\mathbb{P}(X = s) > 0$.

In the extreme case F_X increases only via jumps, i.e. is piece-wise constant changing value at most countable times. Precisely:

Definition 3.8 (Piece-wise constant with at most countable jumps). We say that $f : \mathbb{R} \rightarrow [0, \infty)$ is piece-wise constant with countably many jumps iff there is some countable set S and some real numbers $c_s > 0$ for $s \in S$ such that $\sum_{s \in S} c_s < \infty$ and

$$f(x) = \sum_{s \in S} c_s 1_{x \geq s}.$$

Notice that this set S could be dense, like the set of rational numbers, making it hard to imagine as a staircase function!

In the other extreme F_X could also be everywhere continuous. These observations help us separate out two classes of random variables.

3.1.1 Classification of random variables

Definition 3.9 (Discrete vs continuous random variables). *A random variable is called discrete if its c.d.f. F_X is piece-wise constant changing value at most countable many times. It is called continuous if its c.d.f. F_X is continuous.*

These definitions look a bit abstract / non-telling from the probabilistic perspective and a priori differs from the definition we gave on the example sheet! But no need to worry, it does give the same object:

Exercise 3.1 (Discrete vs random variables ver 2). *Consider a random variable X . Prove that*

- *X is discrete, i.e. its cumulative distribution function F_X is piece-wise constant, if and only if there is a countable set $S \subseteq \mathbb{R}$ with $\mathbb{P}(X \in S) = \mathbb{P}_X(S) = 1$.*
- *X is continuous if and only if for every $y \in \mathbb{R}$, $\mathbb{P}(X = y) = \mathbb{P}_X(\{y\}) = 0$.*

Notice that not every random variable is either discrete or continuous, there could be also mixtures of the two, e.g. one could imagine a c.d.f. given by $F(x) = 0.51_{x \geq 0} + 0.5x1_{x \in [0,1)} + 1_{x \geq 1}$ (What does it correspond to?).

The following proposition says, the c.d.f. of any random variable can be written as a convex combination of c.d.f-s of a discrete and continuous random variable.

Proposition 3.10. *Any cumulative distribution function F can be written uniquely as convex combination of a continuous c.d.f F_c and a piece-wise constant c.d.f. with countably many jumps F_j i.e. for some $a \in [0, 1]$ we have that $F = aF_j + (1 - a)F_c$.*

Moreover, in a later the exercise sheet you will see how to interpret this as saying that each random variable can be written as a random sum of a continuous and discrete random variable.

Proof. If F is either continuous or piece-wise constant with countably many jumps, the existence of such writing is clear. So suppose that F is neither. Write S for the countable set of jumps of F . Define

$$\hat{F}_j(x) = \sum_{s \in S} 1_{x \geq s}(F(s) - F(s-)),$$

which is piece-wise continuous with countably many jumps.

We claim that $\hat{F}_c := F - \hat{F}_j$ is continuous. Indeed, by definition both F and $\hat{F}_j$ both right-continuous, and thus is also their difference. Moreover, both are continuous at any continuity point x of F , i.e. when $x \notin S$ as by definition then $F(x) = F(x^-)$ and one can check the same for $\hat{F}_j$. Finally, when $s \in S$, then again by definition of $\hat{F}_j$, we have that

$$F(s) - F(s-) = 1_{s \geq s}(F(s) - F(s-)) = \hat{F}_j(s) - \hat{F}_j(s-)$$

and thus $\hat{F}_c$ is continuous at such s too.

Now, as F is neither continuous nor piece-wise constant increasing with jumps, we have that $0 < \widehat{F}_j(\infty) < 1$ and $0 < \widehat{F}_c(\infty) < 1$. Hence, we can define

$$F_j(x) := \frac{\widehat{F}_j(x)}{\widehat{F}_j(\infty)}$$

and

$$F_c(x) := \frac{\widehat{F}_c(x)}{\widehat{F}_c(\infty)}.$$

By definition both of those are non-decreasing, right-continuous satisfying the correct limits at $\pm\infty$ and hence are c.d.f-s for random variables. As F_j increases only via jumps and F_c is continuous, we have the desired writing with $a = \widehat{F}_j(\infty)$ and $1 - a = \widehat{F}_c(\infty)$.

Uniqueness is left as an exercise. To see the uniqueness of the decomposition, suppose that one can write

$$F_X = aF_{Y_1} + (1 - a)F_{Y_2} = bF_{Z_1} + (1 - b)F_{Z_2},$$

where both Y_1 and Z_1 are discrete and Y_2, Z_2 continuous random variables. Then $aF_{Y_1} - bF_{Z_1}$ has to be continuous, but also piecewise constant with countably many jumps. As $aF_{Y_1}(-\infty) - bF_{Z_1}(-\infty) = 0$, the only possibility is that it is constantly zero. As $F_{Y_1}(\infty) = 1 = F_{Z_1}(\infty)$, it follows that $a = b$ and $F_{Y_1} = F_{Z_1}$. Thus also $F_{Y_2} = F_{Z_2}$ and the proposition follows. □

3.2 Examples of discrete random variables

There are several families of laws of discrete random variables that come up again and again. As we will see, sometimes these laws also have very nice mathematical characterizations.

Recall that to characterise the law of a random variable, we can either give the value of $\mathbb{P}_X(F)$ for a sufficiently large set of F (e.g. all intervals) or give the c.d.f. For a discrete random variable it suffices to just determine the support S and determine $\mathbb{P}_X(X = s)$ for each $s \in S$ (why?).

Bernoulli random variable

As mentioned already, a random variable that takes only values $\{0, 1\}$, taking value 1 with probability p is called a Bernoulli random variable of parameter p . It is named after the Swiss mathematician Bernoulli, who also thought that all sciences need mathematics, but mathematics doesn't need any. Leaving you to judge, let us see that these examples come up very often.

Namely, on every probability space $(\Omega, \mathcal{F}, \mathbb{P})$, every indicator function of an event, i.e. 1_E gives rise to a Bernoulli random variable and the parameter p is equal to the probability of the event. Indeed for any event E in a probability space $(\Omega, \mathcal{F}, \mathbb{P})$ the indicator function $1_E : (\Omega, \mathcal{F}) \rightarrow (\mathbb{R}, \mathcal{F})$ is measurable and hence a random variable. Moreover, it is $\{0, 1\}$ valued by definition and $\mathbb{P}(\{1_E = 1\}) = \mathbb{P}(E) = p$.

Sometimes one talks about Bernoulli random variables more generally whenever there are two different outcomes, e.g. also when the values are $\{-1, 1\}$. We then call it the Bernoulli

random variable with values $\{-1, 1\}$.

Uniform random variable

Any random variable that takes values in a finite set $S = \{x_1, \dots, x_n\}$, each with equal probability $1/n$ is called the uniform random variable on S . We call the law of this random variable the uniform law. Its c.d.f is given by simply $F_X(x) = n^{-1} \sum_{i=1}^n 1_{x \geq x_i}$.

Examples are - a fair die, the outcome of roulette, taking the card from the top of a well-mixed pack of cards etc... Concretely, for a trivial example is that if we model a fair die on $\Omega = \{1, 2, 3, 4, 5, 6\}$, $\mathcal{F} = \mathcal{P}(\Omega)$ and $\mathbb{P}(i) = 1/6$, then the random variable $X(\omega) := \omega \in \mathbb{R}$ gives rise to a uniform random variable.

We use this family of random variables every time we have no a priori reason to prefer one outcome over the other. A fancy mathematical way of saying this would be to say that the uniform law is the only probability law on a finite set that is invariant under permutations of this set. We will also see on the example sheet that this is the so called maximum entropy probability distribution with values in a finite set S .

Binomial random variable

A random variable that takes values in the set $\{0, 1, \dots, n\}$, and takes each value k with probability

$$p^k(1-p)^{n-k} \binom{n}{k}$$

is called a binomial random variable of parameters $n \in \mathbb{N}$ and $0 \leq p \leq 1$ (why do the probabilities sum to one?). We denote the law of such a binomial random variable by $Bin(n, p)$.

Notice that for $n = 1$, we have the Bernoulli random variable. Bernoulli random variable comes up naturally in models of independent coin tosses, random graphs, or models of random walks. The reason why it comes up so often is that it always describes the following situation - we have a sequence of independent indistinguishable events and we count the number of those who occur. Or in other words, the Binomial random variable $Bin(n, p)$ can be seen as a sum of n independent $Ber(p)$ random variables.

Exercise 3.2 (Binomial r.v. is the number of occurring events). *Suppose we have n mutually independent events $E_1, \dots, E_k$ of probability p on some probability space $(\Omega, \mathcal{F}, \mathbb{P})$. Consider the random number of events that occurs: $X = \sum_{i=1}^n 1_{E_i}$. Prove that X is a random variable and has the law $Bin(n, p)$.*

For a concrete lively example, let's go back to the Erdos-Renyi random graph on n vertices, where each edge is independently included with probability p . We can then fix some vertex v and consider the random variable M_v giving the number of vertices adjacent to v , i.e. linked to v by an edge. The exercise above shows that this random variable has law $Bin(n-1, p)$.

Geometric random variable

A random variable that takes values in the set $\mathbb{N}$, each value k with probability $p(1-p)^{k-1}$ for some $0 < p \leq 1$ is called a geometric random variable of parameter p . We denote the law of a geometric random variable by $Geo(p)$. One should again check that this even defines a random variable, by seeing that the probabilities do sum to one.

A geometric random variable describes the following situation: we have independent events $E_1, E_2, \dots$ each of success probability p and we are asking for the smallest index k such that the event E_k happens. For example, $Geo(1/2)$ describes the number of tosses needed to get a first heads. This will be made precise on the exercise sheet.

There is also a nice property that characterizes the geometric r.v.:

Lemma 3.11 (Geometric r.v. is the only memoryless random variable). *We say that a random variable X with values in $\mathbb{N}$ is memoryless if for every $k, l \in \mathbb{N}$ we have that $\mathbb{P}_X(X > k + l | X > k) = \mathbb{P}_X(X > l)$. Every geometric random variable is memoryless, and in fact these are the only examples of memoryless random variables on $\mathbb{N}$.*

Proof. Let us start by proving that the geometric random variable satisfies the memoryless property. First, notice that if $\mathbb{P}(X = 1) = 1$, then X is a degenerate geometric random variable with $p = 1$. So we can suppose that we work in the case $\mathbb{P}(X > 1) > 0$.

Let us check that a geometric r.v. is memoryless. First, it is easy to check that for a geometric random variable X , we have that $\mathbb{P}(X > l) = (1 - p)^l$ for some $p \in (0, 1]$. As by the definition of conditional probability

$$\mathbb{P}(X > k + l | X > k) = \frac{\mathbb{P}(X > k + l)}{\mathbb{P}(X > k)},$$

it follows that $\mathbb{P}(X > k + l | X > k) = (1 - p)^{k+l-k} = (1 - p)^l = \mathbb{P}(X > l)$ as desired.

Now, let us show that each random variable satisfying the memoryless property has the law of a geometric random variable. Again if $\mathbb{P}(1) = 1$, we are done. Otherwise we can write

$$\mathbb{P}(X > 1 + l | X > 1) \mathbb{P}(X > 1) = \mathbb{P}(X > 1 + l).$$

As for a memoryless random variable $\mathbb{P}(X > l) = \mathbb{P}(X > 1 + l | X > 1)$, we obtain

$$\mathbb{P}(X > l) \mathbb{P}(X > 1) = \mathbb{P}(X > l + 1).$$

Thus inductively $\mathbb{P}(X > l) = \mathbb{P}(X > 1)^l$ and hence X is a geometric random variable of parameter $p = 1 - \mathbb{P}(X > 1)$. $\square$

Poisson random variable

Poisson was a French mathematician who has famously said that the life is good for only two things - mathematics and teaching mathematics. His random variables come up quite often.

The Poisson random variable is a discrete random variable with values in $\{0\} \cup \mathbb{N}$ and taking the value k with probability

$$e^{-\lambda} \frac{\lambda^k}{k!}$$

for some $\lambda > 0$. We denote this distribution by $Poi(\lambda)$. Poisson random variables describe occurrences of rare events over some time period, where events happening in any two consecutive time periods are independent. For example, it has been used to model

- The number of visitors at a small off-road museum.
- More widely, the number of stars in a unit of the space.

- Or more darkly, it was used to also model the number of soldiers killed by horse kicks in the Prussian army.

One way we see the Poisson r.v. appearing is via a limit of the Binomial distribution if the success probability p scales like $1/n$:

Lemma 3.12 (Poisson random variable as the limit of Binomials). *Consider the Binomial distribution $\text{Bin}(n, \lambda/n)$. Prove that as $n \rightarrow \infty$ it converges to $\text{Poi}(\lambda)$ in the sense that for every $k \in \{0\} \cup \mathbb{N}$, we have that*

$$\mathbb{P}(\text{Bin}(n, \lambda/n) = k) \rightarrow e^{-\lambda} \frac{\lambda^k}{k!}.$$

Proof. By definition, for any fixed $n \in \mathbb{N}$ and $k \in \{0\} \cup \mathbb{N}$, we have

$$\mathbb{P}(\text{Bin}(n, \lambda/n) = k) = \binom{n}{k} \frac{\lambda^k}{n^k} \left(1 - \frac{\lambda}{n}\right)^{n-k}.$$

Using

$$\binom{n}{k} = \frac{n!}{(n-k)!k!} = \frac{n(n-1) \cdots (n-k+1)}{k!}.$$

we can write

$$\mathbb{P}(\text{Bin}(n, \lambda/n) = k) = \frac{\lambda^k}{k!} \left(1 - \frac{\lambda}{n}\right)^n \frac{n(n-1) \cdots (n-k+1)}{n^k} \left(1 - \frac{\lambda}{n}\right)^{-k}.$$

But now as $n \rightarrow \infty$

$$\left(1 - \frac{\lambda}{n}\right)^n \rightarrow e^{-\lambda}.$$

Moreover, for any fixed $t > 0$ also $\frac{n-t}{n} \rightarrow 1$ as $n \rightarrow \infty$ and hence

$$\frac{n(n-1) \cdots (n-k+1)}{n^k} \rightarrow 1$$

and

$$\left(1 - \frac{\lambda}{n}\right)^{-k} = \left(\frac{n-\lambda}{n}\right)^{-k} \rightarrow 1,$$

proving the lemma. □

To connect this to the occurrences of rare events described before, one could think as follows. Suppose we try to model the number of arrivals over time window $[0, 1]$, say one year in a distant location. We then cut a time-window $[0, 1]$ into n equal time-segments of length $1/n$ with n large, say into 365 days, so that we can suppose that at each time-segment, say each day, there is at most one arrival. In this case we can describe the arrival or non-arrival using $\text{Ber}(p)$ or 1_E for some event E . If we further suppose that all days are alike, we can take this parameter p to be the same for all time-segments of the same length, e.g. for all days. Moreover, if we suppose that an arrival in one time-segment does not influence arrivals in other time-intervals, we can assume that all events E corresponding to different time intervals are mutually independent. Hence the total number of arrivals is the number of independent events happening, when the event probability is p - we saw above that this gives a $\text{Bin}(n, p)$ random variable. But now, if you check carefully the proof above, you see that if p is not of the form λ/n for some $\lambda > 0$, then in fact the number of events will either

go to infinity or go to zero - i.e. to have a non-trivial random variable in the limit $n \rightarrow \infty$, we are forced to set $p = \lambda/n$.

Poisson random variables also behave very well under taking independent copies and taking random subsets of them:

Exercise 3.3 (Poisson random variables). *Let $X_1 \sim \text{Poi}(\lambda_1)$ and $X_2 \sim \text{Poi}(\lambda_2)$ be two independent random variables defined on the same probability space.*

- *Prove that then $X_1 + X_2$ is also a Poisson random variable with parameter $\lambda_1 + \lambda_2$.*
- *Let now $Y_1, Y_2, \dots$ be independent $\text{Ber}(p)$ random variables defined on the same probability space. Prove that $X := \sum_{i=1}^{X_1} Y_i$ also has the law of $\text{Poi}(p\lambda)$ and $X_1 - X$ has the law of $\text{Poi}((1-p)\lambda)$ and is independent of X .*

3.2.1 How to choose my distribution - the maximum entropy principle

We have now seen several examples of discrete random variables with special properties, which may or may not have sounded relevant and were a bit different for each of the examples. A generic question is the following. Suppose we want to model some statistical phenomena using a random variable. From the experiments or theory we can deduce some weak constraints on the probability distribution of the variable - for example the support of the distribution, i.e. which values it takes, and maybe some other parameters obtained from repeated experiments like some sort of average. The question is: which probability distribution should we choose as our model under these constraints?

Intuitively, we would like to choose a distribution that takes into account these constraints and nothing more. Already Laplace used such an argument: his principle of insufficient reason says that if we only know that we have n outcomes, we should assign each the probability $1/n$. It comes out that somehow the right generalization of this principle of insufficient reason is the principle of maximum entropy - we should choose the probability distribution with maximal entropy, given the constraints. This feels at least intuitively natural, as we are then maximizing our surprise or uncertainty about what is happening. The principle of maximum entropy was introduced by E. T. Jaynes in the 1950s.

To state this, let us first introduce the concept of entropy in the realm of discrete random variables. This rich concept is also interesting in itself and I believe you have already met it in your course of computer science as introduced by Shannon, although its origins go back much further in thermodynamics. In essence the entropy of a random variable is a way to formalise the notion of information content that we learn by observing an outcome.

Definition 3.13 (Discrete (Shannon) entropy). *For a discrete random variable X with outcome set S we define the entropy*

$$H(X) := - \sum_{s \in S} \mathbb{P}(X = s) \log \mathbb{P}(X = s).$$

We also call it the entropy of the probability distribution $\mathbb{P}$.

The mentioned link to information content can be thought of in two steps:

- First, to each event E , and in particular to each outcome $\{X = s\}$ we assign a measure of information content or surprise: $-\log \mathbb{P}(E)$. We like this precise measure more than just $\mathbb{P}(E)$ basically because $\log$ is additive under products and hence the information content of two independent events adds up.

- Then to measure the information content over all outcomes we take the weighted average of $-\log \mathbb{P}(X = s)$ as in the definition above. Such a weighted average is called the mathematical expectation, as we will shortly see.

Remark 3.14. *Often in computer science / information theory one rather uses $\log_2$ instead of $\log$ - this in some sense is just a choice of units for the information content.*

Example 3.15. *One can directly check that for the uniform distribution on n points the entropy is $H = \log n$. Indeed then $\mathbb{P}(X = s) = 1/n$ for any s and the claim follows.*

Notice that although we defined the discrete entropy for a random variable, it does not depend on the exact values of the random variable - only on how many values with which probability it takes. In particular for example it is direct to see the following Lemma.

Lemma 3.16. *For any real-valued discrete random variable we have that $H(X) = H(aX+b)$.*

Further, the reason of choosing the logarithm in the definition, boils down to the following facts:

Lemma 3.17. *The entropy is non-negative: $H(X) \geq 0$. Moreover, for independent discrete random variables X, Y , we have that $H(X, Y) = H(X) + H(Y)$.*

Proof. The first part is evident from the fact that $-p \log p \geq 0$ for all $p \in [0, 1]$ ⁷ The proof is a direct computation on the example sheet. $\square$

There are many ways to give mathematical characterisations of entropy, i.e. to give a set of intuitive conditions for a measure of information content such that they uniquely characterise the entropy functional. We will not do this in our course, but rather explain a property that makes entropy appear - asymptotic equipartition property.

In this respect, consider i.i.d. non-trivial discrete random variables $X_1, X_2, \dots, X_n$ taking each of the values $s \in S$ with positive probability. Then for each sequence of outcomes $(s_1, s_2, \dots, s_n)$ we can calculate the probability $\mathbb{P}(X_1 = s_1, \dots, X_n = s_n)$. By independence, this is given by $\prod_{i=1}^n \mathbb{P}(X_i = s_i)$. As each of $\mathbb{P}(X_1 = s) \in (0, 1)$, these probabilities decay exponentially with n , i.e. should be roughly of the form $\exp(cn)$. Is this the case, and how does this $c > 0$ behave? For a given sequence, this will clearly depend on the exact sequence $(s_1, s_2, \dots, s_n)$, so one cannot expect an answer in full generality.

However, one can determine this exponent for a typical outcome sequence and it is given by the entropy of X_1 :

Theorem 3.18 (Asymptotic equipartition property). *Let $X_1, X_2, \dots$ be i.i.d. non-trivial discrete random variables, taking values $s \in S$ with positive probability. Denote by $p(s_1, s_2, \dots, s_n)$ the probability of the sequence of outcomes $(s_1, s_2, \dots, s_n)$. Then $\mathbb{P}(|-\frac{1}{n} \log p(X_1, \dots, X_n) - H(X_1)| > \epsilon)$ converges to 0.*

We will be able to give a simple proof and even a stronger statement of this result towards the end of the course, but I encourage you already to try it out now - this maybe also helps to understand how the notion we are about to introduce simplify our thinking.

As said, entropy has many contexts and many uses, but for us the aim was to help select probability laws on discrete sets. Here are two results in this direction.

⁷If you wish we take the convention that $0 \log 0 = 0$, which of course also makes a lot of sense by taking $x > 0$ and letting it tend to 0.

Lemma 3.19 (Uniform distribution has maximum entropy). *Consider all probability distributions on n points. Among such distributions, the uniform distribution is the unique maximum entropy distribution.*

Proof. Let $Q = (q_i)_{i=1\dots n}$ denote a probability distribution on n points. We want to prove that

$$H(Q) = - \sum_{i=1}^n q_i \log_2 q_i \leq \log_2 n.$$

We use the fact that $\log x$ is concave on $[0, 1]$. Thus we have that

$$H(Q) = \sum_{i=1}^n (q_i \log_2 \frac{n}{q_i}) - \log_2 n \leq \log_2 (\sum_{i=1}^n \frac{q_i n}{q_i}) = \log_2 n^2 - \log_2 n = \log_2 n,$$

where we also used that $\sum_{i=1}^n q_i = 1$. Moreover, the equality holds only if $q_i = 1/n$ for all i , so in fact the uniform distribution is the unique maximum entropy distribution $\square$

Similarly we can single out the geometric random variable among all distributions with outcomes in $\mathbb{N}$, however with one extra constraint. Namely, it is maximum entropy distribution on $\mathbb{N}$ among those distributions for which the so called mean or expectation is finite: $\sum_{n \geq 1} n \mathbb{P}(X = n) < \infty$.