APPENDIX B WHAT IS ...

B.1 ... A BINARY NUMBER?

We are accustomed to writing numbers using the decimal system. We use the decimal digits 0, 1, 2, 3, 4, 5, 6, 7, 8, and 9 and are comfortable with writing that a year consists of (roughly) 365 days. But why do we write down numbers using 10 digits? It is often speculated that this choice is related to the number of fingers and toes we have, which were used to perform simple calculations ("digitus" is Latin for "finger"). Nowadays, however, most numbers are processed by computers. And electrical circuits are not very well suited to represent the digits 0, 1, ..., 10. Instead, computer systems mostly use the digits 0 and 1 and can represent them by low and high voltage, for example. In a *binary system*, each number is represented using 0s and 1s. Here, the key idea is to use powers of 2. For example, we have

$$11010 = \mathbf{1} \cdot 2^4 + \mathbf{1} \cdot 2^3 + \mathbf{0} \cdot 2^2 + \mathbf{1} \cdot 2^1 + \mathbf{0} \cdot 2^0.$$

In the decimal system, this number is written as 26. For decimal numbers, we perform the same kind of calculations:

$$365 = \mathbf{3} \cdot 10^2 + \mathbf{6} \cdot 10^1 + \mathbf{5} \cdot 10^0,$$

but since we are so used to the system, we do not consciously think about this operation any more.

numeral system	
binary	decimal
0	0
1	1
10	2
11	3
100	4
101	5
110	6
111	7
1000	8
1001	9
1010	10
1011	11
1100	12
⋮	⋮

Sometimes a subscript is used to distinguish between the two systems. For example,

$$110_2 = 6_{10}.$$

It is possible, of course, to use bases other than 2 or 10. The *hexadecimal* system, for example, uses the base 16, and the *octal* system uses 8. The latter also forms the basis of a famous mathematical joke:

> Why do many mathematicians always confuse Halloween and Christmas? Because Oct 31 = Dec 25.

B.2 … A CONVERGING SEQUENCE OR SERIES?

For our purposes, a sequence $(a_n)_n := (a_n)_{n\in\mathbb{N}}$ is an infinite collection of real numbers a_n, where $n = 1, 2, \ldots$ (e.g., 1, $1/2, 1/3, 1/4, 1/5, \ldots$ if $a_n := 1/n$). Even though this sequence

never reaches 0, it comes arbitrarily close to it. The sequence defined by $a_n := (-1)^n$, in contrast, does not approach any number, since it jumps between -1 and 1. Formally, one says that a sequence $(a_n)_n$ *converges to a real number* a if for all $\varepsilon > 0$, there exists a natural number N, such that for all $n > N$, we have

$$|a_n - a| < \varepsilon.$$

That is, after some value of N, all elements of the sequence remain in an ε-band around a. We write $a = \lim_{n\to\infty} a_n$.

Some sequences consist of partial sums, which means that each a_n can be written as

$$a_n = \sum_{k=1}^{n} b_k$$

for some sequence $(b_k)_k$. These sequences are often called *series*, and if they converge, their limit is denoted by

$$\lim_{n\to\infty} a_n = \lim_{n\to\infty} \sum_{k=1}^{n} b_k =: \sum_{k=1}^{\infty} b_k.$$

As an example, consider eating a cake by always cutting the remaining piece into two equal-sized halves and eating one of them. You start by having eaten $\frac{1}{2}$ of the cake, then $\frac{1}{2} + \frac{1}{4}$, then $\frac{1}{2} + \frac{1}{4} + \frac{1}{8}$, and so on. Clearly, you never stop eating, and the amount of cake in your stomach is growing, but at the same time, you will never have eaten more than the whole cake. Mathematically, we have

$$\sum_{k=1}^{\infty} \frac{1}{2^k} = \frac{1}{2} + \frac{1}{4} + \frac{1}{8} + \cdots = 1.$$

In high school, one sometimes considers numbers of the form $0.3\bar{9}$, which should really be understood as $0.3 + \sum_{k=2}^{\infty} 9 \cdot 10^{-k} = 0.4$.

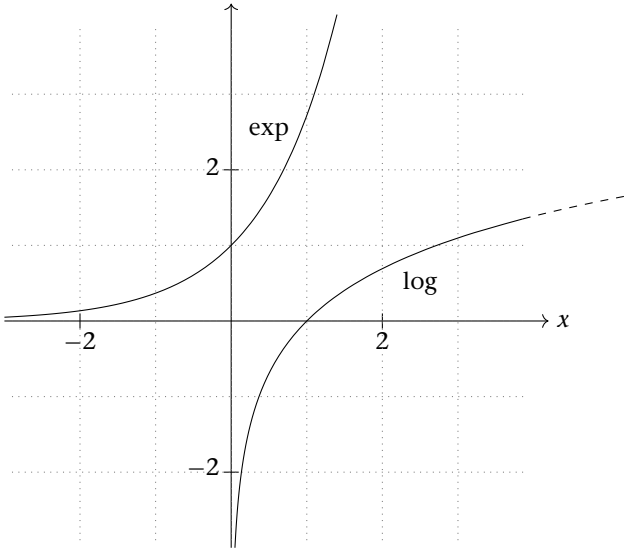
B.3 … AN EXPONENTIAL FUNCTION?

One of the most important series in mathematics defines the *exponential function* exp:

$$\exp(x) := \sum_{k=0}^{\infty} \frac{x^k}{k!}. \tag{B.1}$$

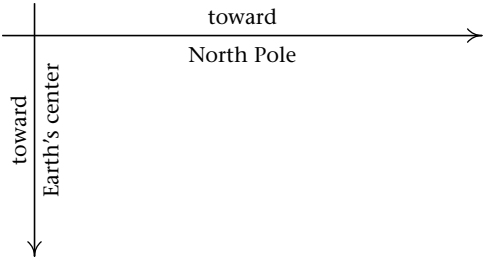
One can show that this series converges for any real number x, that is, $\exp : \mathbb{R} \to \mathbb{R}_{>0}$ is a function from $\mathbb{R}$ to strictly positive real numbers. The value $e := \exp(1) \approx 2.7182$ is the famous Euler's number.

The function exp is strictly monotonically increasing and has an inverse function, the *natural logarithm* $\log : \mathbb{R}_{>0} \to \mathbb{R}$. That is, $\log(a) = b$ if and only if $\exp(b) = a$. The graphs of the functions exp and log are shown in the following figure.



The logarithm function is strictly increasing, but the increase is slow. How slow can be experienced by doing a small experiment.

Turn this book so that the two arrows in the following figure point toward the North Pole and the center of the Earth, respectively. Open the book so that the arrow with the x on page 136 points toward the North Pole, too.



Return now to the previous figure, which shows the two graphs. Assume that you take a pencil and continue to draw the graph of the logarithm (following the dashed line). You draw over this page, leave this book, and continue to hold the pencil at the height of the corresponding value. If you go farther and farther, you will circle the Earth (passing the North Pole) and eventually, after a long time, coming back to page 146 of this book. Where will the graph meet the vertical axis on that page? The Earth's circumference (at the poles) is roughly 40,000 km, and the scale of the drawing is 1 cm. Furthermore,

$$\log(40 \cdot 10^8) \approx 22.1,$$

which means that after circling the Earth, the graph of the logarithm is only about 22 cm above the origin of the coordinate system (that is, the intersection of the two arrows)!

The logarithm and the exponential can be used to extend the exponentiation a^b to cases where the exponent b is not an integer: $a^b := \exp(b \log(a))$. This allows us to define the function $x \mapsto 2^x$, for example. In information theory (chapter 5) and coding theory (chapter 1), one usually considers logarithms to the base 2. This function is the inverse function of $x \mapsto 2^x$ and

is often denoted by $\log_2$. We have $\log_2(8) = 3$, because $2^3 = 8$. It holds that

$$\log_2(x) = \frac{\log(x)}{\log(2)}.$$

B.4 ... A BINOMIAL COEFFICIENT?

In the field of combinatorics, we count things. Often, this means counting possibilities. How many towers can I build with 4 different colored toy blocks? In how many ways can we place our 40 guests at 3 tables? How many ways are there to distribute the music parts in a string octet with 4 violins, 2 violas, and 2 cellos, if the musicians do not switch instruments?

The *binomial coefficient* is about counting subsets. Consider the group

{Anna, Bahar, Chane, Dora, Emilian},

for example. There are 10 possible ways of forming a group of size 3:

{Anna, Bahar, Chane}	{Anna, Bahar, Dora}
{Anna, Bahar, Emilian}	{Anna, Chane, Dora}
{Anna, Chane, Emilian}	{Anna, Dora, Emilian}
{Bahar, Chane, Dora}	{Bahar, Chane, Emilian}
{Bahar, Dora, Emilian}	{Chane, Dora, Emilian}.

We can also count the number of combinations without writing them down explicitly. There are 5 possibilities of choosing the first person, 4 possibilities of choosing the second person, and lastly, there are 3 persons left, from which we can choose the last person. The number of combinations we obtain in this way can be written as

$$5 \cdot 4 \cdot 3 = \frac{5 \cdot 4 \cdot 3 \cdot 2 \cdot 1}{2 \cdot 1} = \frac{5!}{(5-3)!}, \tag{B.2}$$

where 5! denotes 5 factorial. Since we consider groups (sets) of people here, we do not want to distinguish between

{Emilian, Anna, Dora} and {Dora, Emilian, Anna},

for example. In equation (B.2), however, both of these combinations have been included. In fact, not only 2 versions of this set are included, but also the other 4 permutations of the set. In total, each set has been counted $6 = 3!$ times. Thus, there are

$$\binom{5}{3} := \frac{5!}{3!(5-3)!} = \frac{120}{12} = 10 \tag{B.3}$$

possibilities to form a set of 3 people out of a set of 5 people.

This derivation may seem a bit overly complex, but it generalizes to sets and subsets of arbitrary size. In general, the *binomial coefficient* is defined as

$$\binom{n}{k} := \frac{n!}{k!(n-k)!}$$

and denotes the number of possibilities of forming subsets of size k out of n distinct elements. The argument for that statement is exactly the same as the one above for $\binom{5}{3}$.

The binomial coefficient becomes important in lottery games, where participants have to guess which 6 out of 49 numbers are drawn, for example. Most of us have relatively little intuition about how many possibilities there are, but when we calculate the numbers, they are usually very large, which, unfortunately, yields very small winning probabilities, for example,

$$\binom{49}{6} = 13983816.$$

The *multinomial coefficient* is an extension of the binomial coefficient. There are

$$\binom{n}{k_1, \ldots, k_m} = \frac{n!}{k_1! \cdots k_m!}$$

possibilities to distribute n numbers into m bins of size $k_1, k_2, \ldots, k_m$ (so $k_1 + \cdots + k_m = n$). For example, given the set of 5 people mentioned above, we want to form one group of 2 people making dinner, one group of 2 people making dessert, and

one group of 1 person doing the dishes. There are

$$\binom{5}{2,2,1} = \frac{5!}{2!2!1!} = 30$$

possibilities to form such groups. Also,

$$\binom{n}{k, n-k} = \frac{n!}{k! \cdot (n-k)!} = \binom{n}{k},$$

and we recover the binomial coefficient.

B.5 … A PROBABILITY?

Probabilities of Events

We will define probabilities for sets (one can think about sets of possible outcomes), which are often called *events*. Consider a (finite) set Ω, which represents the set of possible outcomes. A *probability* is a function P that maps any subset A of Ω to a number between 0 and 1, such that the following three statements hold:

- $P(\Omega) = 1$,
- $P(A^C) = 1 - P(A)$ for all $A \subseteq \Omega$, and
- $P(A \cup B) = P(A) + P(B)$ for all $A, B \subseteq \Omega$ that are disjoint.

Here, $A^C := \Omega \setminus A$ denotes the complement of A, and A and B being disjoint means that they have no element in common: The intersection $A \cap B$ equals the empty set $\emptyset$.

Many random processes can be modeled with such probabilities. The outcome of rolling a die is a famous example and can be modeled by

$$\Omega := \{1, 2, 3, 4, 5, 6\} \text{ and } P(A) := \frac{\#A}{6},$$

where $\#A$ denotes the number of elements in A. Rolling two dice can be modeled using

$$\Omega := \{(1,1), (1,2), (1,3), \ldots, (4,6), (5,6), (6,6)\} \text{ and } P(A) := \frac{\#A}{36}.$$

For example, we have

$$P(\text{sum} = 8) = P(\{(2,6),(3,5),(4,4),(5,3),(6,2)\}) = 5/36$$

because there are 5 pairs (i, j) that yield a sum of 8.

In this book, we are often interested in the probability $P(\text{lose})$ of losing a game, for example. As in the die example, this often requires us to count the number of situations in which we lose and divide that number by the number of possible outcomes.

Independence

We say that two events are *independent* if the probability that both events happen is the product of the probabilities of each event happening. Formally, we say $A, B \subseteq \Omega$ are independent if and only if

$$P(A \cap B) = P(A) \cdot P(B).$$

Intuitively, this means that the occurrence of event A does not tell you anything about the occurrence of event B. Consider, for example, the event A: "sum of the two dice is divisible by 3" and event B: "second die shows a 6." Using the above probability model, this can be written as

$$A := \{(1,2),(1,5),(2,1),(2,4),(3,3),(3,6),(4,2),(4,5),(5,1),(5,4),(6,3),(6,6)\} \text{ and}$$

$$B := \{(1,6),(2,6),(3,6),(4,6),(5,6),(6,6)\}.$$

Clearly, we have

$$P(A \cap B) = P(\{(3,6),(6,6)\}) = \frac{2}{36} = \frac{12}{36} \cdot \frac{6}{36} = P(A) \cdot P(B).$$

The events A: "sum of the two dice equals 11" and B: "second die shows a 6," however, are not independent.

B.6 … AN EXPECTATION?

As in appendix B.5, we start with a (finite) set Ω of possible outcomes and a probability P that maps any subset $A \subseteq \Omega$ to the interval $[0, 1]$. Sometimes, any outcome can be attached to a number that we are particularly interested in. In the example of rolling two dice, for example, we may be particularly interested in the sum of the two dice. This can be achieved by considering the map $X : \Omega \to \mathbb{R}$, with $(i, j) \mapsto i + j$. Such maps X are called *random variables*. Rather than looking at events, we can then compute probabilities involving random variables directly. In the die example, we can write the term $P(\text{sum} = 8)$ as $P(X = 8)$.

Given a set Ω of possible outcomes, a probability P, and a random variable X, we can now compute the *expectation* of X. It is defined as

$$\mathbf{E}X := \sum_x xP(X = x).$$

Here, the sum is over all values that the random variable X can take. For example, for the sum of two dice, we have:

$$\mathbf{E}X = 2 \cdot \frac{1}{36} + 3 \cdot \frac{2}{36} + 4 \cdot \frac{3}{36} + \cdots + 11 \cdot \frac{2}{36} + 12 \cdot \frac{1}{36} = 7.$$

There are two intuitive interpretations of that statement. First, the expectation is the "best guess" for the outcome of X.[1] Second, the convergence to the expectation tells us that when we average a large number of rolls of two dice, the average will be roughly 7 (this is usually referred to as the "law of large numbers").

In chapter 4 on page 65, we considered a random variable for counting mistakes and argued that

$$P(\text{mistakes} = 1) \geq 1 - \frac{1}{p}.$$

1. More formally, we have for all $a \in \mathbb{R}$ that $\mathbf{E}[(X - \mathbf{E}X)^2] \leq \mathbf{E}[(X - a)^2]$, if $\mathbf{E}X^2 < \infty$.

This clearly implies that

$$\mathrm{E}(\text{mistakes}) \geq 1 - \frac{1}{p}.$$

B.7 … A MATRIX?

A matrix is a collection of numbers organized into rows and columns. For example,

$$A = \begin{pmatrix} 5 & -\pi & 2 \\ 0 & 3 & 3 \end{pmatrix}$$

is called a 2×3 matrix, since it has 2 rows and 3 columns. We often write $A \in \mathbb{R}^{2\times 3}$.

The matrix multiplication of two matrices A and B in general is defined if A has as many columns as B has rows. Then the entry (k, j) of the product AB is calculated by "overlaying" row k of matrix A with the jth column of B and summing up the pairwise entries as

$$(AB)_{k,j} = \sum_{\ell} A_{k,\ell} B_{\ell,j}, \tag{B.4}$$

where the index ℓ in the sum runs over all values of ℓ from 1 to the number of columns of A.

A special but important case of a matrix-matrix multiplication is the matrix-vector multiplication. Writing out equation (B.4), we obtain

$$\begin{pmatrix} a_1 & a_2 & a_3 \\ b_1 & b_2 & b_3 \\ c_1 & c_2 & c_3 \end{pmatrix} \begin{pmatrix} v_1 \\ v_2 \\ v_3 \end{pmatrix} = \begin{pmatrix} a_1 v_1 + a_2 v_2 + a_3 v_3 \\ b_1 v_1 + b_2 v_2 + b_3 v_3 \\ c_1 v_1 + c_2 v_2 + c_3 v_3 \end{pmatrix},$$

which we use in section 7.3, for example.

Many maps that appear in practice have such a form. For example, for a 3×5 matrix A, we can consider the map

$$\begin{array}{ccc} \mathbb{R}^5 & \to & \mathbb{R}^3 \\ v & \mapsto & Av. \end{array}$$

This is often called a *linear map*, because we have the following two properties: first, $A \cdot 0 = 0$, and second, for all $\lambda \in \mathbb{R}$ and v, $w \in \mathbb{R}^5$, we have $A(\lambda v + w) = \lambda Av + Aw$. In general, an $n \times m$ matrix A defines a linear map $\mathbb{R}^m \to \mathbb{R}^n$.

The *transpose* $A^\top$ of a matrix A is obtained by simply turning around rows and columns:

$$A = \begin{pmatrix} 5 & -\pi & 2 \\ 0 & 3 & 3 \end{pmatrix} \quad \Longrightarrow \quad A^\top = \begin{pmatrix} 5 & 0 \\ -\pi & 3 \\ 2 & 3 \end{pmatrix}.$$

B.8 … A COMPLEX NUMBER?

Complex numbers are, unlike their name suggests, not particularly difficult. One way to think about them is to consider the real numbers $\mathbb{R}$ and to "add" a whole bunch of other numbers. But why would we want to do that? The real numbers have a lot of nice properties, but they are not *complete*. If we consider the following polynomial f,

$$f(x) = x^2 - 2x - 3,$$

then f has two roots: $x = -1$ and $x = 3$. That is, $f(-1) = 0 = f(3)$. In fact, you can write

$$f(x) = (x + 1)(x - 3),$$

which makes it even more obvious what the roots are. But what about a polynomial g with

$$g(x) = x^2 - 2x + 3?$$

We do not find any real number x that satisfies $g(x) = 0$. It somehow feels it should be possible to write

$$g(x) = (x - r)(x - s),$$

but what are r and s? These are complex numbers.

Formally, a complex number $z \in \mathbb{C}$ can be written as

$$z = a + i \cdot b,$$

for $a, b \in \mathbb{R}$. We call a the *real part* and b the *imaginary part* of z. As for real numbers, we can add, substract, multiply, and divide complex numbers, but similarly to when we first learned how to add two ratios, we also need to learn the rules for adding complex numbers. Let

$$z_1 = a_1 + i \cdot b_1,$$
$$z_2 = a_2 + i \cdot b_2.$$

We then define

$$z_1 + z_2 := (a_1 + b_1) + i \cdot (b_1 + b_2),$$
$$z_1 - z_2 := (a_1 - b_1) + i \cdot (b_1 - b_2),$$
$$z_1 \cdot z_2 := (a_1 a_2 - b_1 b_2) + i \cdot (a_1 b_1 + a_2 b_2).$$

Dividing two complex numbers is possible, too, but that is not so important for our book.

The 'i' is really just a symbol, but if you think of it as the famous $\sqrt{-1}$, you may find it easier to memorize the multiplication rule, because you can then simply multiply out and collect terms:

$$\begin{aligned} z_1 \cdot z_2 &= a_1 a_2 + i a_1 b_1 + i a_2 b_2 + i^2 b_1 b_2 \\ &= (a_1 a_2 - b_1 b_2) + i \cdot (a_1 b_1 + a_2 b_2). \end{aligned}$$

What about our polynomial g from above? This polyonomial indeed has two roots. If you like, you can convince yourself that

$$g(1 + i \cdot 2) = 0 \text{ and } g(1 - i \cdot 2) = 0. \tag{B.5}$$

This allows us to write

$$g(x) = (x - 1 - i \cdot 2)(x - 1 + i \cdot 2),$$

which yields the values of r and s we were looking for.

In fact, there is a famous theorem stating that any polynomial g of degree n can be written as

$$g(x) = (x - z_1) \cdot (x - z_2) \cdot \cdots \cdot (x - z_n)$$

with z_is that are not necessarily real but may be complex.

As in equation (B.5), complex numbers often appear in pairs: If

$$z = a + i \cdot b$$

satisfies a certain property, then often $a - i \cdot b$ does, too. We therefore write

$$\bar{z} = a - i \cdot b$$

and call this the *complex conjugate* of z.