Computer Algebra for Concrete Mathematics

Summer semester 2024

Carsten.Schneider@risc.jku.at

In this lecture basic skills and techniques will be elaborated which are relevant to simplify formulas related to enumeration. Special emphasis is put on tools that support the student for the analysis of algorithms (best case, worst case and average case). In particular, the participant gets acquainted to apply these computer algebra tools to non-trivial examples.
The content of the lecture can be summarized by the following key words:

- algorithmic treatment of formal power series;
- c-finite and holonomic functions/sequences;
- recurrence solving;
- basic aspects of asymptotics;
- symbolic summation.

A major emphasis of the lecture is to present the basic notions, to develop the basic ideas of the underlying algorithms and to put computer algebra into action for concrete examples.
In addition, many of the topics discussed in the lecture can be found in the books

- *Concrete Mathematics - A Foundation for Computer Science* by R.L.Graham, D.E.Knuth and O.Patashnik (Addison-Wesley, 1994),
- *The Concrete Tetrahedron* by Manuel Kauers and Peter Paule (Springer Wien, 2011).

Contents

Lecture from March 05, 2024

1 Introduction

In this lecture we will deal in strong interaction with generating functions, recurrences, asymptotics and summation. This interplay can be visualized also as follows:

$$\begin{tikzcd}
\text{generating functions} \arrow[r, leftrightarrow] \arrow[d, leftrightarrow] \arrow[dr, leftrightarrow] & \text{summation} \arrow[d, leftrightarrow] \arrow[dl, leftrightarrow] \\
\text{recurrences} \arrow[r, leftrightarrow] & \text{asymptotics}
\end{tikzcd}$$

In the introduction we will illustrate the interaction of recurrences, summation and asymptotics. The machinery of generating functions (formal power series) will be introduced in Section 3 below.

1.1 A case study for SelectionSort and summation

We start with an example of the well-known sorting algorithm SelectionSort.

Example 1.1. We apply SelectionSort to $(5, 3, 8, 2)$. This means that we find a smallest element from the list/array and move it to the beginning. Afterwards we proceed with the list/array where the first entry is ignored. In this way we get the following operation steps:

$$\begin{array}{c}
5 \quad 8 \quad 3 \quad \boxed{2} \\
\downarrow \\
2 \,\big|\, 8 \quad \boxed{3} \quad 5 \\
\downarrow \\
2 \quad 3 \,\big|\, 8 \quad \boxed{5} \\
\downarrow \\
2 \quad 3 \quad 5 \,\big|\, 8
\end{array}$$

Remark: if one deals with an array, one can move the smallest element to the right place by swapping elements accordingly.

In the following (for SelectionSort and later for QuickSort) we will estimate the time complexity by counting the number of comparisons. In this regard, the following consideration is immediate: In order to find the smallest element 2 in $(5, 8, 3, 2)$ one needs 3 comparisons; to find the smallest element 3 in $(8, 3, 5)$, one needs 2 comparisons; and to find the smallest element 5 in $(8, 5)$, one needs 1 comparison. In total

$$3 + 2 + 1 = 6$$

comparisons are needed. In general, if

$$F(n) = \text{number of pairwise comparisons to selection-sort } n \text{ elements } (n \geq 0)$$

we get

$$\begin{aligned} F(n) &= (n-1) + (n-2) + \cdots + 2 + 1 \\ &= \sum_{k=1}^{n} (n-k) \\ &\overset{k \to n-k}{=} \sum_{k=1}^{n-1} k \\ &\overset{\text{why?}}{=} \frac{n(n-1)}{2}. \end{aligned}$$

Notation 1.2. *We will use the following conventions:*

$$\begin{aligned} \mathbb{N} &:= \{0, 1, 2, 3, \dots\} \\ \mathbb{N}^* &:= \{1, 2, 3, \dots\} \\ \sum_{k=a}^{b} f(k) &:= 0 \ \textit{if } a > b \\ \prod_{k=a}^{b} f(k) &:= 1 \ \textit{if } a > b. \end{aligned}$$

One way to simplify the Gauss sum $\sum_{k=1}^{n} k$ (or to show that it equals to $\frac{n(n-1)}{2}$) is to sum it twice (in the usual and in the reversed order):

$$\begin{array}{ccccccccccc} & 1 & + & 2 & + & 3 & + & \dots & + & n & \\ + & n & + & (n-1) & + & (n-2) & + & \dots & + & 1 & \\ \hline = & (n+1) & + & (n+1) & + & (n+1) & + & \dots & + & (n+1) & = n(n+1). \end{array}$$

This gives

$$\sum_{k=1}^{n} k = 1 + 2 + \cdots + n = \frac{n(n+1}{2}.$$

Alternatively, one can consider the picture (the black balls represent the sum)

$$
\begin{array}{ccccccc}
1 & +\,2 & +\,3 & +\,4 & +\,5 & \dots & +\,\mathrm{n}
\end{array}
\qquad =\mathrm{n}(\mathrm{n}+1)
$$

$$
\underbrace{\left.\begin{array}{ccccccc}
\bullet & \bullet & \bullet & \bullet & \bullet & \dots & \bullet\\
\circledast & \bullet & \bullet & \bullet & \bullet & \dots & \bullet\\
\circledast & \circledast & \bullet & \bullet & \bullet & \dots & \bullet\\
\circledast & \circledast & \circledast & \bullet & \bullet & \dots & \vdots\\
\circledast & \circledast & \circledast & \circledast & \bullet & \dots & \bullet\\
\circledast & \circledast & \circledast & \circledast & \circledast & \dots & \bullet\\
\circledast & \circledast & \circledast & \circledast & \circledast & \dots & \circledast
\end{array}\right\} n+1}_{n}
$$

in order to extract the identity.

HW 1. Try to apply the Gauß-method to sum

(a) $\sum_{k=0}^{n}(2k+1)$

(b) $\sum_{k=1}^{n} k^2$

(c) $\sum_{k=1}^{n} k^3$

Find and prove a formula for (a), (b) and (c).

Note that the above proof can be also reflected with the following sum manipulations:

$$
\begin{aligned}
\sum_{k=1}^{n-1} k \overset{k\to n-k}{=} \sum_{k=1}^{n-1}(n-k) &= \sum_{k=1}^{n-1} n - \sum_{k=1}^{n-1} k\\
&= n\underbrace{\sum_{k=1}^{n-1} 1}_{n-1} - \sum_{k=1}^{n-1} k
\end{aligned}
$$

$$\Downarrow$$

$$2\sum_{k=1}^{n-1} = n(n-1).$$

Throughout this lecture the harmonic numbers will play a central role.

Definition 1.3. *For $n \in \mathbb{N}$, we define*

$$H_n = \sum_{k=1}^{n} \frac{1}{k};$$

note that with our convention from above we have $H_0 = 0$.

HW 2. Prove for all $n \in \mathbb{N}$ that

$$\sum_{k=0}^{n-1} \frac{k}{(k+1)(k+2)} = H_n - \frac{2n}{n+1}.$$

HW 3. Let $f : \mathbb{Z} \to \mathbb{C}$ and $a, b \in \mathbb{Z}$ with $a \leq b$.

1. For
$$S(a,b) := \sum_{k=a}^{b} (f(k+1) - f(k))$$
show that
$$S(a,b) = f(b+1) - f(a).$$

2. Suppose in addition that $f(k) \neq 0$ for all k with $a \leq k \leq b$. For
$$P(a,b) := \prod_{k=a}^{b} \frac{f(k+1)}{f(k)}$$
show that
$$P(a,b) = \frac{f(b+1)}{f(a)}.$$

HW 4. Use the previous homework to find a closed form for

$$a_n := \prod_{k=2}^{n} \left(1 - \frac{1}{k^2}\right).$$

BP 1. Consider the function $\exp : \mathbb{R} \to \mathbb{R}$ defined by

$$x \mapsto \sum_{n=0}^{\infty} \frac{x^n}{n!}.$$

Prove: there is no rational function $r(x) \in \mathbb{R}(x)$ (i.e., $r(x) = \frac{p(x)}{q(x)}$ for polynomials $p, q \in \mathbb{R}[x]$) such that

$$\exp(x) = r(x) \quad \forall x \in U$$

where $U \subseteq \mathbb{R}$ is some non-empty open interval.

HW 5. Given a tower of n discs, initially stacked in decreasing size on one of three pegs. Transfer the entire tower to one of the other pegs, moving only one disc at each step and never moving a larger one onto a smaller one. Find a_n, the minimal number of moves ($n \geq 0$).

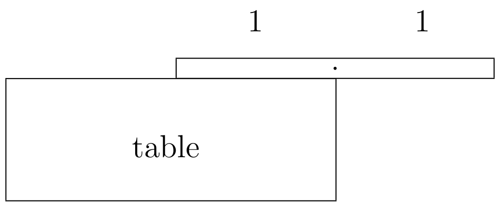
HW 6. How many slices of pizza can a person maximally obtain by making n straight cuts with a pizza knife. Let P_n ($n \geq 0$) be that number.

BP 2. Prove that there is no rational function $r(x) \in \mathbb{C}(x)$ such that

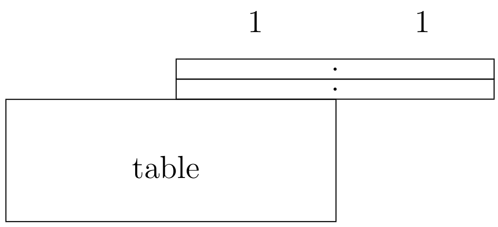
$$H_n = r(n)$$

for all $n \in \mathbb{N}$ with $n \geq \lambda$ for some $\lambda \in \mathbb{N}$.

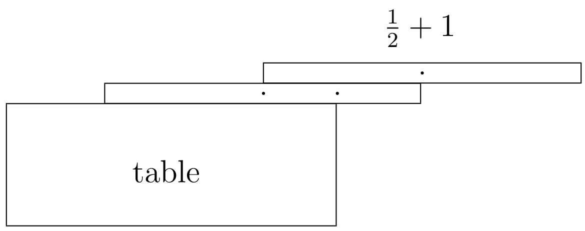
Example 1.4. What is the maximal possible overhang of n cards (beer coaster)?
Let us suppose that a card has length 2. Then with 1 card we get the overhang 1:



If we are given two cards, we start with



and observe that we cannot move the top card further. Thus we move the card below further and further away, and it is not difficult to see that the balance point is reached with the overhang $1+\frac{1}{2}=\frac{3}{2}$. Thus we get the following picture:



If we are given three cards, the balance point will be at position $1+\frac{1}{2}+\frac{1}{3}=\frac{11}{6}$.
With 4 cards the overhang will be $H_4 = 1+\frac{1}{2}+\frac{1}{3}+\frac{1}{4}=\frac{25}{12}$, which is more than one card length.
With 52 cards, we get the overhang $H_{52} = 2.27 \cdot 2$, i.e., it is twice the card length. In general, the maximal overhang of n cards is H_n.

What happens if we stack more and more cards. Can we make the overhang arbitrarily large?

Questions like this lead immediately to asymptotic considerations.

1.2 Some basic notions for asymptotics

We start with the big-O notation.

Definition 1.5. *For*[1] $g : \mathbb{N} \to \mathbb{R}$ *we define*

$$O(g) = \{f : \mathbb{N} \to \mathbb{R} \mid \exists c_f \in \mathbb{R},\, n_0 \in \mathbb{N}\ \forall n \geq n_0 :\ |f(n)| \leq c_f\, |g(n)|\}.$$

Example 1.6. We have

$$2n \in O(n), \qquad 2n-5 \in O(n), \qquad 2^{2^{2^{2^{2^{2^{2}}}}}} \cdot n \in O(n), \qquad \frac{1}{2^{2^{2^{2^{2^{2^{2}}}}}}} \cdot n \in O(n).$$

[1]Note that the function g can be also interpreted as a the sequence $(g(n))_{n\geq 0}$ with entries from $\mathbb{R}$.

Lecture from March 12, 2024

The following theorem states that the harmonic numbers and the log-function grow similarly fast.

Theorem 1.7. *We have*

$$H_n - \log(n) - \gamma \in O(\tfrac{1}{n});$$

here $\log(n) := \ln(n)$ *denotes the natural logarithm (to the basis e) and* $\gamma = 0,5772156\dots \in \mathbb{R}$ *is Euler's constant*[2]

Proof. For a proof see the book Concrete Mathematics by Graham/Knuth/Patashnik. □

Example 1.8. Going back to Example 1.4 we conclude with

$$\lim_{n\to\infty} \log(n) = \infty$$

that the overhang can be (theoretically) arbitrary long if sufficiently many cards are available. However, the overhang grows dramatically low. E.g., suppose that the card length is 10cm (i.e., one unit corresponds to 5cm). Then we can produce an overhang of more than 100m with n cards, if

$$2000 \leq H_n \leq \log(n) + 1$$

holds. Thus $n \geq e^{1999}$, i.e., we must take around $1.429 \cdot 10^{868}$ cards; however, one estimates that there are only around 10^{80} atoms in the universe...

In particular, we can conclude with this theorem that there is a constant $c \in \mathbb{R}$ and $n_0 \in \mathbb{N}$ (actually one can choose $n_0 = 1$) such that

$$|\underbrace{H_n - \log(n) - \gamma}_{:=a_n\in\mathbb{R}}| \leq \frac{c}{n}$$

holds for all $n \geq n_0 = 1$. This implies that $(a_n)_{n\geq 0}$ converges (in the analysis sense) to 0, i.e.,

$$\lim_{n\to\infty} a_n = 0$$

$$\Updownarrow$$

$$\lim_{n\to\infty} (H_n - \log(n) - \gamma) = 0$$

$$\Updownarrow$$

$$\lim_{n\to\infty} (H_n - \log(n)) = \gamma.$$

Definition 1.9. *For* $a, b : \mathbb{N} \to \mathbb{R}$ *we define*

$$a(n) \sim b(n) \quad \Leftrightarrow \quad \lim_{n\to\infty} \frac{a(n)}{b(n)} = 1.$$

In this case, we also say that $a(n)$ *and* $b(n)$ *are asymptotically equal.*

[2]So far it is not known, if $\gamma \in \mathbb{Q}$ or if γ is irrational.

We remark that $\sim$ is an equivalence relations.

HW 7. Show that $H_n \sim \log(n)$.

Another important fact is Stirling's formula that can be stated as follows; the proof can be found again in Concrete Mathematics.

Theorem 1.10.

$$n! \sim \left(\frac{n}{e}\right)^n \sqrt{2\pi n}.$$

Note: Since $n^n = (e^{\log(n)})^n = e^{n\,\log(n)}$, we get

$$n! \sim e^{n(\log(n)-1)}\sqrt{2\pi n}.$$

1.3 A case study for QuickSort and recurrences

We turn to QuickSort and sort the array

$$44 \quad 13 \quad 9 \quad \boxed{29} \quad 71 \quad 67 \quad 5 \quad 8 \quad 15$$

with $n = 9$ elements. In each step we split the array by choosing a pivot element at random. Here we take, e.g., 29. We swap it to the right side and focus on the remaining array:

$$44 \quad 13 \quad 9 \quad 15 \quad 71 \quad 67 \quad 5 \quad 8 \,\big|\, 29.$$

Next, we split the array: all elements which are smaller than 29 are moved to the left-hand side, and all elements which are larger than 29 are moved to the right-hand side. Here the trick is to start with the corner entries.

$$\boxed{44} \quad 13 \quad 9 \quad 15 \quad 71 \quad 67 \quad 5 \quad \boxed{8} \,\big|\, 29$$

In this case, both entries are on the wrong side. Thus we swap them and get

$$8 \,\big|\, 13 \quad 9 \quad 15 \quad 71 \quad 67 \quad 5 \,\big|\, 44 \quad 29$$

Now we repeat this procedure for the remaining entries: we zoom in until we find again two bad entries. In this case,

$$8 \quad 13 \quad 9 \quad 15 \,\big|\, \boxed{71} \quad 67 \quad \boxed{5} \,\big|\, 44 \quad 29$$

and swap it:

$$8 \quad 13 \quad 9 \quad 15 \quad 5 \,\big|\, 67 \,\big|\, 71 \quad 44 \quad 29.$$

Eventually, the two lines meet and we are done: we only have to move the pivot element, which is on the right most place, to the correct position, namely at the position where the two lines meet:

$$8 \quad 13 \quad 9 \quad 15 \quad 5 \,\big|\, 29 \,\big|\, 71 \quad 44 \quad 67$$

Summarizing, we obtained our split: all elements which are smaller than 29 are left of it and all elements which are large are right to it. In total, we needed $n-1 = 8$ comparisons to obtain this split. Note that the element 29 is already at the correct position of the to be sorted array. Thus we have to repeat this tactic for the remaining sub-arrays. E.g., we obtain the following splits (applying the method recursively and choosing particular pivot elements):

$$44 \quad 13 \quad 9 \quad \boxed{29} \quad 71 \quad 67 \quad 5 \quad 8 \quad 15$$

$$\downarrow 8 \text{ comparisons}$$

$$8 \quad 13 \quad 9 \quad 15 \quad \boxed{5} \,|\, 29 \,|\, 71 \quad 44 \quad \boxed{67}$$

$$\downarrow 4{+}2{=}6 \text{ comparisons}$$

$$5 \,|\, 13 \quad \boxed{9} \quad 15 \quad 8 \,|\, 29 \,|\, 44 \,|\, 67 \,|\, 71$$

$$\downarrow 3 \text{ comparisons}$$

$$5 \,|\, 8 \,|\, 9 \,|\, \boxed{15} \quad 13 \,|\, 29 \,|\, 44 \,|\, 67 \,|\, 71$$

$$\downarrow 1 \text{ comparison}$$

$$5 \,|\, 8 \,|\, 9 \,|\, 13 \,|\, 15 \,|\, 29 \,|\, 44 \,|\, 67 \,|\, 71$$

Summarizing, we needed in total

$$8 + 6 + 3 + 1 = 18$$

comparisons to QuickSort the above array (with the particularly chosen pivot elements marked with a box).

We recall that SelectionSort needs $\frac{n(n-1)}{2}\Big|_{n=9} = 9 \cdot 4 = 36$ comparisons. So there is an improvement (as the name QuickSort suggests).

Note further that QuickSort strongly depends on the choice of the pivot elements. In particular, one can construct, e.g., a worst case scenario as follows: Take an already sorted array and apply QuickSort by choosing always the right most element. Then we obtain the worst split: the pivot element is right most and all other elements are on the left-hand side. Thus QuickSort is applied to $n-1$ elements in the next step. Applying this argument iteratively, we need in this worst case situation

$$(n-1) + (n-2) + (n-3) + \cdots + 1 = \frac{n(n-1)}{2}$$

comparisons. In other words: QuickSort behaves in the worst case like the slow algorithm SelectionSort.

In order to see (and prove) the improvement of QuickSort in contrast to, e.g., SelectionSort, we have to explore the average case. Here we assume that the pivot elements are chosen arbitrarily and that after the split it is equally likely that the pivot element is at position $1, 2, \ldots, n-1$ or n. Under this assumption, we are interested in the following counting:

$$F(n) = \text{the avarage number of pairwise comparisons to quicksort } n \text{ elements } (n \geq 0).$$

The base case of QuickSort is the empty array or an array of length 1. Here the array is already sorted and no comparisons are necessary. Thus we have

$$F(0) = F(1) = 0.$$

For an array of length $n = 2$ QuickSort will perform exactly one comparison, i.e., we can set

$$F(2) = 1.$$

More generally, if we are given an array of length n, we choose a pivot element (at random) and calculate in the divide step (of our Divide and Conquer strategy) a split. For this task we need $n - 1$ comparisons (independently of the choice of the pivot element). By our assumption it is equally likely that the pivot element will be at position 1, at position 2,..., or at position n. Thus we get

$$F(n) = \underbrace{n-1}_{\substack{\text{comparisons} \\ \text{for the split}}} + \frac{1}{n} \sum_{k=1}^{n} F_k(n);$$

here $F_k(n)$ denotes the average number of comparisons that are needed to sort the derived array where $k - 1$ elements are left to the pivot element and $n - k$ are right to the pivot element. More precisely, $F_k(n)$ is determined by the property that QuickSort is applied to each of the two subarrays: namely, the average number of comparisons are $F(k - 1)$ for the left array and the average number of comparisons are $F(n - k)$ for the right array. Thus we have

$$F_k(n) = F(k - 1) + F(n - k)$$

and in total we get

$$F(n) = n - 1 + \frac{1}{n} \sum_{k=1}^{n} (F(k - 1) + F(n - k)), \quad n \geq 1$$

Note that this formula (together with $F(0 = 0)$ allows us to compute all values of $F(n)$. E.g., we compute

n	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	...
$F(n)$	0	0	1	$\frac{8}{3}$	$\frac{29}{6}$	$\frac{37}{5}$	$\frac{103}{10}$	$\frac{472}{35}$	$\frac{2369}{140}$	$\frac{2593}{126}$	$\frac{30791}{1260}$	$\frac{32891}{1155}$	$\frac{452993}{13860}$	$\frac{476753}{12870}$	$\frac{499061}{12012}$	...

(1)

Unfortunately, this formula (or the produced numbers) do not provide any information how good QuickSort really is.

In a preprocessing step we simplify the found recurrence further. A first observation is that the summand consists of two parts which are equal:

$$\sum_{k=1}^{n} F(k - 1) \overset{k \to n-k}{=} \sum_{k=1}^{n} F(n - k).$$

Thus we get

$$\begin{aligned}
F(n) &= n-1+\frac{1}{n}\sum_{k=1}^{n}(F(k-1)+F(n-k))\\
&= n-1+\frac{1}{n}\sum_{k=1}^{n}(F(k-1)+\sum_{k=1}^{n}F(n-k))\\
&= n-1+\frac{2}{n}\sum_{k=1}^{n}F(k-1)\\
&= n-1+\frac{2}{n}\sum_{k=0}^{n-1}F(k).
\end{aligned}$$

Second, we eliminate the indefinite sum with upper bound n (where the summand itself is free of n). This can be accomplished easily if the factor in front of the sum is also free of n. To accomplish this latter requirement, we first multiply our recurrence with n and get

$$n\,F(n) = n(n-1)+\boxed{2}\sum_{k=0}^{n-1}F(k) \quad n \geq 1.$$

Given this special form, we shift the recurrence in n, i.e., replace n by $n+1$ yielding (where the constant in front of the sum does not change!)

$$(n+1)\,F(n+1) = (n+1)n+\boxed{2}\sum_{k=0}^{n}F(k) \quad n \geq 0$$

Finally, we subtract both and obtain

$$(n+1)\,F(n+1)-nF(n) = 2n+\boxed{2}\underbrace{(\sum_{k=0}^{n}F(k)-\sum_{k=0}^{n-1}F(k))}_{=F(n)} \quad n \geq 1.$$

Summarizing, we obtained

$$(n+1)F(n+1)-(n+2)F(n) = 2n, \quad n \geq 1$$

with the initial value $F(1)=0$. One can easily check that the found recurrence is also valid for $n=0$ with $F(0)=F(1)=0$. Thus we obtain

$$\begin{aligned}
&(n+1)F(n+1)-(n+2)F(n) = 2n, \quad n \geq 0\\
&F(0) = 0.
\end{aligned} \tag{2}$$

By construction this simplified recurrence produces again the sequence $(F(n))_{n\geq 0}$ where the first values are printed in (1). More precisely, we can use the formula

$$F(n) \leftarrow \begin{cases} \frac{n+1}{n}F(n-1)+2\frac{n-1}{n} & \text{if } n \geq 1\\ 0 & \text{if } n=0. \end{cases}$$

In the following we will explore its behavior further by solving the found recurrence. For first-order linear recurrences (here $F(n)$ and $F(n+1)$ arise linearly) we can exploit the following method, also called *"variation of constants"*.

Step 1: Find a closed form for the homogeneous equation:

$$(n+1)H(n+1) - (n+2)H(n) = 0.$$

Unrolling it and proper cancellations give

$$\begin{aligned} H(n+1) &= \frac{n+2}{n+1}H(n) = \frac{n+2}{n+1} \cdot \frac{n+1}{n}H(n-1) = \dots \\ &= \frac{n+2}{\cancel{n+1}} \cdot \frac{\cancel{n+1}}{\cancel{n}} \cdot \frac{\cancel{n}}{\cancel{n-1}} \cdots \frac{\cancel{3}}{\cancel{2}} \cdot \frac{\cancel{2}}{1}H(0) = (n+2)H(0), \end{aligned}$$

and thus

$$H(n) = (n+1)H(0).$$

Using the homogeneous solution $(n+1)$ (we ignore the constant $H(0)$), we make the following ansatz in

Step 2: Find a sequence $G(n)$ such that

$$F(n) = (n+1)G(n)$$

holds for all $n \geq 0$.

As a consequence it follows that

$$0 = F(0) = G(0)$$

and

$$(n+1)\overbrace{(n+2)G(n+1)}^{=F(n+1)} - (n+2)\overbrace{(n+1)G(n)}^{=F(n)} = 2n, \quad n \geq 0$$

$$\Updownarrow$$

$$G(n+1) - G(n) = \frac{2n}{(n+1)(n+2)}, \quad n \geq 0.$$

Using telescoping (see HW 3) it follows that

$$G(n) - \underbrace{G(0)}_{=0} = \sum_{k=0}^{n-1} \frac{2k}{(k+1)(k+2)}, \quad n \geq 0$$

and with summation (HW 2) we get

$$G(n) = 2H_n - \frac{4n}{n+1}, \quad n \geq 0. \tag{3}$$

Thus

$$F(n) = (n+1)G(n) = 2(n+1)H_n - 4n, \quad n \geq 0. \tag{4}$$

Finally, we show that the average number $F(n)$ to quicksort n elements is asymptotically equal to $2n\log(n)$; as a consequence it also follows that $F(n) \in O(n\log(n))$.

Theorem 1.11.

$$F(n) \sim 2n\log(n).$$

Proof. We have

$$\begin{aligned} F(n) &= 2(n+1)H_n - 4n \\ &\sim 2(n+1)H_n \\ &\sim 2nH_n \\ &\sim 2n\log(n). \end{aligned}$$

The last equivalence follows by $H_n \sim \log(n)$; see HW 7. $\square$

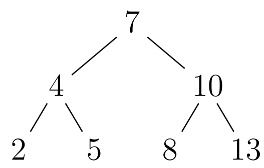
Example 1.12. For an array of length $n = 100$ SelectionSort needs $\frac{n(n-1)}{2} = 4950$ comparisons and QuickSort (in average) $2n\log(n) = 921.03$ comparisons; this looks not like a big deal. However, if we take, e.g., $n = 1000000$, then SelectionSort needs $\sim 5 * 10^{11}$ comparisons, and QuickSort $\sim 2.7631 * 10^7$ comparison; so there is the speedup factor 18095.

Lecture from March 19, 2024

1.4 A case study for Binary Search Trees (BST)

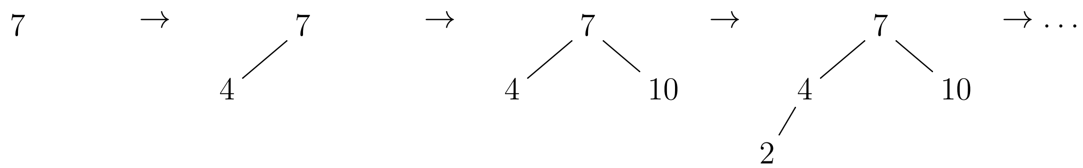
Definition 1.13. *A binary search tree is a binary tree where in each subtree with root x all the elements in its left subtree are smaller and all elements in its right subtree are larger than x.*

Example 1.14. The binary search tree



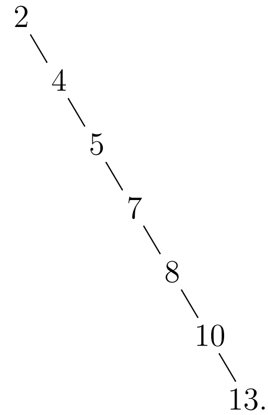
(5)

represents the set $\{2, 4, 5, 7, 8, 10, 13\}$. It can be generated by inserting step-wise the elements, e.g., in the order $7 \to 4 \to 10 \to 2 \to 5 \to 8 \to 13$:



In the tree (5) the paths $P_1 = (7)$, $P_2 = (7, 10)$, or $P_3 = (7, 4, 5)$ go from the root 7 to the root 7, to the inner node 10 or to the leaf 5 (via the inner node 4), respectively. P_1 has path length 1, P_2 has path length 2 and P_3 has path length 3.

An alternative tree can be generated by inserting step-wise the elements in the order $2 \to 4 \to 5 \to 7 \to 8 \to 10 \to 13$:



In worst case a binary search tree turns to a linked list (see the second tree in the example). Thus finding an element in such a worst case scenario requires n operations.

However, the average time complexity is much better in a randomly chosen tree. More precisely, take the set $S = \{a_1, a_2, \ldots, a_n\}$ with $a_1 < a_2 < \cdots < a_n$ and suppose that we are given a binary search trees in which the elements S are stored at random. This means that they are generated by a certain order $b_1 \to b_2 \to \cdots \to b_n$ (with $\{a_1, a_2, \ldots, a_n\} = \{b_1, b_2, \ldots, b_n\}$) where each insertion order $b_1 \to b_2 \to \cdots \to b_n$ is equally likely. E.g., the element b_1 equals the element a_1 with probability $1/n$, it equals a_2 with probability $1/n$, etc.

Now define

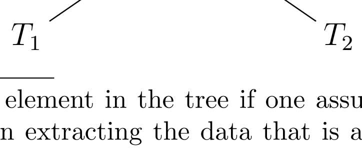
$$P(n) = \text{the avarage path length of such a binary search tree with } n \text{ nodes.}$$

As illustrated in the above example a path starts at the root and walks down a tree and stops at an inner node or a leaf; in particular, the path length is the number of nodes that are visited during the walk (including the root). Then the average cost to find an element[3] $c \in S$ (randomly chosen) in a tree (randomly generated) equals precisely $P(n)$: it is simply the average path length (the path ends at c).

Similarly to the average number of operations $F(n)$ in QuickSort, we will explore the average number $P(n)$ to find an element in a binary search tree. Obviously we have

$$P(1) = 1.$$

Next, consider the following special case: the first element that we insert in our random construction is a_{i+1} where $0 \le i < n$. After inserting randomly the remaining $n-1$ elements we obtain a tree with the following shape:



(6)

[3] It seems nonsense to search for an element in the tree if one assumes that it is in. However, c might be a data base key and one is interested in extracting the data that is attached to c. Thus one has to find the element c in the tree which is stored together with a pointer that refers to the desired data.

where the elements $S_1 = \{a_1, \dots, a_i\}$ are stored in T_1 and $S_2 = \{a_{i+1}, \dots, a_n\}$ are stored in T_2. Now consider the average path length $\delta_{a_{i+1}}$ from the root a_{i+1} to any node c randomly chosen from S. Note that $c = b_1 = a_{i+1}$ has probability $\frac{1}{n}$, $c \in S_1$ has probability $\frac{i}{n}$, and $c \in S_2$ has probability $\frac{n-i-1}{n}$. Thus we obtain three cases:

1. With probability $\frac{1}{n}$ the path length is 1 (we go from $c = a_{i+1}$ to c).
2. With probability $\frac{i}{n}$ we obtain a path of at least length two. It start at a_{i+1}, goes to another element in S_1 and from this node the average path length is $P(i)$ to end up at c. Thus the average path length equals $1 + P(i)$.
3. Analogously to case 2, we obtain with probability $\frac{n-i-1}{n}$ the average path length $1+P(n-i-1)$.

In total it follows that

$$\begin{aligned}\delta_{a_{i+1}} &= \tfrac{1}{n} + \tfrac{i}{n}(P(i) + 1) + \tfrac{n-i-1}{n}(P(n-i-1) + 1)\\ &= 1 + \tfrac{i}{n}P(i) + \tfrac{n-i-1}{n}P(n-i-1).\end{aligned}$$

In order to get a complete formula (recursion for $P(n)$) we note that each special case (6) with $b_1 = a_{i+1}$ for $0 \leq i < n$ is equally likely, i.e., arises with probability $\frac{1}{n}$. Thus we get

$$P(n) = \sum_{i=0}^{n-1} \frac{1}{n} \delta_{a_{i+1}}.$$

HW 8. Show that

$$P(n) = 1 + \frac{2}{n^2} \sum_{i=0}^{n-1} i\, P(i).$$

HW 9. Show that

$$n^2\, P(n) - (n-1)(n+1)P(n-1) = 2n - 1, \quad n \geq 2.$$

HW 10. Solve the recurrence in closed form (i.e., in terms of the harmonic numbers). More precisely, perform the following steps:

1. Compute a solution $H(n) \in \mathbb{Q}(n)$ of the homogeneous version
$$n^2\, H(n) - (n-1)(n+1)H(n-1) = 0.$$
2. Make the ansatz $P(n) = H(n)G(n)$ which leads to
$$G(n+1) - G(n) = r(n) \qquad r \geq l$$
for some $r(n) \in \mathbb{Q}(n)$ and $l \in \mathbb{N}$. By the telescoping trick this gives
$$G(n) - G(l) = \sum_{k=l}^{n-1} r(k)$$
with some explicitly given $G(l) \in \mathbb{Q}$ and thus
$$F(n) = H(n) \left(\sum_{k=l}^{n-1} r(k) + G(l) \right).$$

3. Simplify the sum further in term of the harmonic numbers.

Theorem 1.15.

$$
\begin{aligned}
&P(n) \in O(\log(n)),\\
&P(n) \sim 2\,\log(n).
\end{aligned}
$$

Proof. **HW 11**. □

Summarizing, given an arbitrary binary search tree with n elements, one finds an element (that occurs in the tree) in $O(\log(n))$ operations. A similar result can be derived for the case that the element is not stored and one wants to verify this fact.

2^* Recall: basic notions from algebra

In the following we repeat some basic notions and constructions from algebra that will arise in the lecture. In particular, they are useful to tackle the bonus problems stated below.

Recall 2.1. Let $\mathbb{A}$ be a set with two operations $+ : \mathbb{A} \times \mathbb{A} \to \mathbb{A}$ and $\cdot : \mathbb{A} \times \mathbb{A} \to \mathbb{A}$.
$(\mathbb{A}, +, \cdot)$ is called a *field* if the following properties hold:

1. $\forall a, b, c \in \mathbb{A} : (a + b) + c = a + (b + c)$;
2. $\forall a, b \in \mathbb{A} : a + b = b + a$;
3. $\exists 0 \in \mathbb{A}\, \forall a \in \mathbb{A} : 0 + a = a$;
4. $\forall a \in \mathbb{A}\, \exists b \in \mathbb{A} : a + b = 0$;
5. $\forall a, b, c \in \mathbb{A} : (a \cdot b) \cdot c = a \cdot (b \cdot c)$;
6. $\forall a, b \in \mathbb{A} : a \cdot b = b \cdot a$;
7. $\exists 1 \in \mathbb{A} \setminus \{0\}\, \forall a \in \mathbb{A} : 1\, a = a$;
8. $\forall a \in \mathbb{A} \setminus \{0\}\, \exists b \in \mathbb{A} \setminus \{0\} : a\, b = 1$;
9. $\forall a, b, c \in \mathbb{A} : a \cdot (b + c) = a \cdot b + a \cdot c$.

If the operations are clear from the context, one simply writes $\mathbb{A}$ for the field. Often one neglects $\cdot$ and simply writes $a\, b$ instead of $a \cdot b$.

Note: Properties (1)–(4) imply that $(\mathbb{A}, +)$ is a commutative (abelian) group, and properties (5)–(8) imply that also $(\mathbb{A} \setminus \{0\}, \cdot)$ is a commutative (abelian) group. Finally, property (9) states that the operations $+$ and $\cdot$ interact distributively.

Example 2.2. The rational numbers $(\mathbb{Q}, +, \cdot)$, the real numbers $(\mathbb{R}, +, \cdot)$ or the complex numbers the real numbers $(\mathbb{C}, +, \cdot)$ are fields with the usual operations. Furthermore, the set of rational functions $(\mathbb{Q}(n), +, \cdot)$, $(\mathbb{R}(n), +, \cdot)$ or $(\mathbb{C}(n), +, \cdot)$ (see BPs 1 and 2) form fields with the usual operations.

Often one is given algebraic structures which are equipped with operations that do not satisfy all the properties required for a field. In this lecture we deal mostly with commutative rings with 1.

Recall 2.3. Let $\mathbb{A}$ be a set with two operations $+ : \mathbb{A} \times \mathbb{A} \to \mathbb{A}$ and $\cdot : \mathbb{A} \times \mathbb{A} \to \mathbb{A}$.
$(\mathbb{A}, +, \cdot)$ is called a *commutative ring with 1* if the properties (1)–(7) and (9) from Recall 2.1 hold. If the operations are clear from the context, one simply writes $\mathbb{A}$ for the ring.

Note: a commutative ring with 1 is a field if all non-zero elements are invertible (i.e., property (8) in Recall 2.1 holds). In general, one can distinguish two types of rings.

Recall 2.4. A commutative ring $\mathbb{A}$ with 1 is called *integral domain* if the following holds:

$$\forall a, b \in \mathbb{A} : a \cdot b = 0 \Rightarrow a = 0 \vee b = 0.$$

If the ring is not an integral domain, one finds two such elements $a, b \in \mathbb{A} \setminus \{0\}$ with $a \cdot b = 0$. Such elements are also called zero-divisors. In this case, $\mathbb{A}$ is also called a *a commutative ring with 1 and zero-divisors*.

Note that a commutative ring with 1 which contains zero-divisors cannot be a field. Contrary, an integral domain (i.e., a commutative ring with 1 and without zero-divisors) might be a field. Even better, if it is an integral domain but not a field yet, one can build the set of quotients. Then this extended set forms a field and contains $\mathbb{A}$ as subring. More precisely, one can carry out the following construction.

Recall 2.5. Let $(\mathbb{A}, +, \cdot)$ be an integral domain and define the set of quotients

$$Q(\mathbb{A}) = \left\{ \frac{a}{b} \,\middle|\, a \in \mathbb{A}, b \in \mathbb{A} \setminus \{0\} \right\}.$$

Since $\mathbb{A}$ is an integral domain, it follows that for any $b_1, b_2 \in \mathbb{A} \setminus \{0\}$ we have $b_1 \cdot b_2 \neq 0$. Thus we can define the operation $\oplus : Q(\mathbb{A}) \times Q(\mathbb{A}) \to Q(\mathbb{A})$ defined by

$$\frac{a_1}{b_1} \oplus \frac{a_2}{b_2} = \frac{a_1 \cdot b_2 + a_2 \cdot b_1}{b_1 \cdot b_2} \tag{7}$$

and the operation $\odot : Q(\mathbb{A}) \times Q(\mathbb{A}) \to Q(\mathbb{A})$ defined by

$$\frac{a_1}{b_1} \odot \frac{a_2}{b_2} = \frac{a_1 \cdot a_2}{b_2 \cdot b_2}. \tag{8}$$

One can verify that $(Q(\mathbb{A}), \oplus, \odot)$ is a field (i.e., all 9 properties in Recall 2.1 hold). $Q(\mathbb{A})$ is also called the *quotient field of* $\mathbb{A}$. *Note that* $\mathbb{A}$ *is contained in* $Q(\mathbb{A})$ *by identifying* $a \in \mathbb{A}$ *with* $\frac{a}{1} \in Q(\mathbb{A})$. *In particular, for any* $a, b \in \mathbb{A}$ *we have* $a \oplus b = a + b$ *and* $a \odot b = a \cdot b$. *This means that the ring* $\mathbb{A}$ *is contained in the field* $Q(\mathbb{A})$. *Usually, one reuses for* $Q(\mathbb{A})$ *again the operations* $+$ *and* $\cdot$ *from the integral domain* $\mathbb{A}$.

Example 2.6. The set of integers $\mathbb{Z}$ forms a ring with the usual addition and multiplication. The ring is an integral domain, i.e., for any $a, b \in \mathbb{Z} \setminus \{0\}$ we have $a \cdot b \neq 0$. The set of quotients $Q(\mathbb{Z})$ is nothing else than $\mathbb{Q}$. Together with the operations (7) and (8) one obtains a field, also called the field of rational numbers. Obviously, $\mathbb{Z}$ is contained in $\mathbb{Q}$ by identifying $\frac{a}{1} \in \mathbb{Q}$ with $a \in \mathbb{Z}$.
A ring with zero divisors cannot be turned to a field: one can find at least two denominators whose multiplication turns to zero. Such "exotic" rings will arise in the next section.

Sometimes one is faced with a commutative (abelian) group $(\mathbb{A}, +)$, i.e., with an operation $+ : \mathbb{A} \times \mathbb{A} \to \mathbb{A}$ with the properties (1)-(4) from Recall 2.1, but a multiplication $\cdot : \mathbb{A} \times \mathbb{A} \to \mathbb{A}$ with the properties of a ring or a field does not exist. However, in many cases one can determine a field $\mathbb{K}$ together with a scalar operation $* : \mathbb{K} \times \mathbb{A} \to \mathbb{A}$ yielding a vector space.

Recall 2.7. Let $(\mathbb{K}, +, \cdot)$ be field and let $\mathbb{A}$ be a set with two operations $+ : \mathbb{A} \times \mathbb{A} \to \mathbb{A}$ and $* : \mathbb{K} \times \mathbb{A} \to \mathbb{A}$.
$(\mathbb{A}, +, *)$ is called a vector space over $\mathbb{K}$ if properties (1)–(4) from Recall 2.1 hold and in addition the following properties hold:

1. $\forall a \in \mathbb{A}\ \ \forall \lambda, \mu \in \mathbb{K} :\ (\lambda \cdot \mu) * a = \lambda * (\mu * a)$;
2. $\forall a \in \mathbb{A} :\ 1 * a = a$ (here 1 is the neutral element in $\mathbb{K}$);
3. $\forall a, b \in \mathbb{A}\ \ \forall \lambda \in \mathbb{K} :\ \lambda * (a + b) = \lambda * a + \lambda * b$;
4. $\forall a \in \mathbb{A}\ \forall \lambda, \mu \in \mathbb{K} :\ (\lambda + \mu) * a = \lambda * a + \mu * a$.

$*$ is also called a *scalar multiplication.*

Example 2.8. $\mathbb{R}^3$ is a vector space over $\mathbb{R}$. E.g.,

$$(1, 0, 0) + (-1) * (0, 1, 0) = (1, 0, 0) + (0, -1, 0) = (1, -1, 0).$$

More generally take any field $\mathbb{K}$ and $n \in \mathbb{N}^*$. Then $\mathbb{K}^n$ (the set of vectors of length n with entries from $\mathbb{K}$) forms a vector space over $\mathbb{K}$.

Lecture from April 9, 2024

3 Generating functions and formal power series

In this lecture we will often deal with sequences $(a_n)_{\geq 0}$ (see, e.g., (1) with $a_n = F(n)$). As we will see later, it is often more convenient to work with a generating function

$$(a_n)_{n\geq 0} \mapsto \sum_{n=0}^{\infty} a_n\, x^n.$$

For instance, the generating function of $a_n = 1$ with $n \geq 0$ yields

$$(a_n)_{n\geq 0} \mapsto \boxed{\sum_{n=0}^{\infty} x^n = \frac{1}{1-x}. \qquad (GS)}$$

In analysis the identity (GS) can be interpreted as follows by considering the functions

- $f : \mathbb{R} \setminus \{1\} \to \mathbb{R}$ defined by $f(x) = \frac{1}{1-x}$;
- $g : (-1, 1) \to \mathbb{R}$ defined by $g(x) = \lim_{N\to\infty} \sum_{n=0}^{N} x^n$; by the ratio test the power series $g(x)$ has the convergence radius $r = 1$.

Then (GS) in analysis means

$$g(x) = f(x) \qquad \forall x \in (-1, 1).$$

In algebra the interpretation will be elaborated in Example 3.12 below.

Definition 3.1. *(including notations)*
$\mathbb{K}$ denotes a field containing the rational numbers $\mathbb{Q}$ as subfield; typical examples are $\mathbb{K} = \mathbb{Q}$, the rational function field $\mathbb{K} = \mathbb{Q}(n)$ with rational coefficients (like $\frac{n^3+1}{2n^2+3}$), $\mathbb{K} = \mathbb{R}$ or the rational function field $\mathbb{K} = \mathbb{R}(n)$ with real coefficients (like $\frac{n^3+\sqrt{2}}{2n^2+\pi}$).
The set of sequences with entries from $\mathbb{K}$ is denoted by

$$\mathbb{K}^{\mathbb{N}} := \{(a_n)_{n\geq 0} \mid a_n \in \mathbb{K}\}.$$

In the following we will explore step-wise more and more operations that can be applied to the set $\mathbb{K}^{\mathbb{N}}$. We start with the following simple versions.

Definition 3.2. *For $(a_n)_{n\geq 0}, (b_n)_{n\geq 0} \in \mathbb{K}^{\mathbb{N}}$ and $\lambda \in \mathbb{K}$ we define*

$$(a_n)_{n\geq 0} + (b_n)_{n\geq 0} := (a_n + b_n)_{n\geq 0},$$
$$\lambda * (a_n)_{n\geq 0} := (\lambda a_n)_{n\geq 0}.$$

Example 3.3. We have

$$(1, 0, 0, 0, \dots) + (-1) * (0, 1, 0, 0, \dots) = (1, 0, 0, 0, \dots) + (0, -1, 0, 0, \dots) = (1, -1, 0, 0, \dots).$$

Lemma 3.4. *$(\mathbb{K}^{\mathbb{N}}, +, *)$ is a vector space over $\mathbb{K}$.*

Proof. **BP 3**. $\square$

Remark 3.5. For $m \in \mathbb{N}^*$ set

$$\tilde{K}_m = \{(a_n)_{n\geq 0} \in \mathbb{K}^{\mathbb{N}} \mid a_l = 0 \;\; \forall l \geq m\}.$$

Then $\tilde{K}_m$ and $\mathbb{K}^m$ are isomorphic as vector spaces, i.e., up to renaming of the objects (taking only the first m entries from each element of $\tilde{K}_m$)

$$(a_0, a_1, \dots, a_{m-1}, 0, 0, 0, \dots) \mapsto (a_0, a_1, \dots, a_{m-1})$$

they are the same. Summarizing, the vector space $\mathbb{K}^{\mathbb{N}}$ contains $\tilde{K}_m$ and thus $\mathbb{K}^m$ as a special case ($\mathbb{K}^m$ is the well known vector space known from linear algebra; it is a subspace of $\mathbb{K}^{\mathbb{N}}$).

Example 3.6. For $\mathbb{K} = \mathbb{R}$ and $m = 3$ we conclude that

$$\tilde{\mathbb{R}}_3 = \{(a_n)_{n\geq 0} \in \mathbb{R}^{\mathbb{N}} \mid a_l = 0 \, \forall l \geq 3\}$$

and $\mathbb{R}^3$ are isomorphic. For instance, we identify $(1, -1, 0, 0, \dots) \in \tilde{\mathbb{R}}_3$ with $(1, -1, 0) \in \mathbb{R}^3$.

In contrast to the scalar multiplication $*$ for $\mathbb{K}^{\mathbb{N}}$, one can define more flexible operations for $\mathbb{K}^{\mathbb{N}}$. As will be seen later, the Cauchy product can be considered as a generalization of the scalar multiplication.

Definition 3.7. *For $(a_n)_{n\geq 0}, (b_n)_{n\geq 0} \in \mathbb{K}^{\mathbb{N}}$ we define the* Hadamard product $\odot : \mathbb{K}^{\mathbb{N}} \times \mathbb{K}^{\mathbb{N}} \to \mathbb{K}^{\mathbb{N}}$ by

$$(a_n)_{n\geq 0} \odot (b_n)_{n\geq 0} := (a_n \, b_n)_{n\geq 0}$$

and the Cauchy product $\cdot : \mathbb{K}^{\mathbb{N}} \times \mathbb{K}^{\mathbb{N}} \to \mathbb{K}^{\mathbb{N}}$ by

$$(a_n)_{n\geq 0} \cdot (b_n)_{n\geq 0} := (c_n)_{n\geq 0}$$

where

$$c_n = \sum_{k=0}^{n} a_k \, b_{n-k}.$$

Example 3.8. Consider $(a_n)_{n\geq 0}$ with $a_n = 1$ for $n \geq 0$ and $(b_n)_{n\geq 0}$ with $b_0 = 1$, $b_1 = -1$ and $b_n = 0$ for $n \geq 2$. Then

$$(a_n)_{n\geq 0} \odot (b_n)_{n\geq 0} = (1, 1, 1, 1, \dots) \odot (1, -1, 0, 0, \dots) = (1, -1, 0, 0, \dots)$$

and

$$(a_n)_{n\geq 0} \cdot (b_n)_{n\geq 0} = (1, 1, 1, 1, \dots) \cdot (1, -1, 0, 0, \dots) = (c_0, c_1, c_2, \dots)$$

with

$$c_n = \sum_{k=0}^{n} a_k \, b_{n-k}.$$

More precisely,

$$\begin{aligned}
c_0 &= 1 \cdot 1 = 1\\
c_1 &= a_0\, b_1 + a_1\, b_0 = -1 + 1 = 0\\
c_2 &= a_0\, b_2 + a_1\, b_1 + a_2\, b_0 = 0 + -1 + 1 = 0\\
c_3 &= a_1\, b_3 + a_1\, b_2 + a_2\, b_1 + a_3\, b_0 = 0 + 0 - 1 + 1 = 0\\
&\vdots\\
c_l &= 0 \quad \forall l \geq 1.
\end{aligned}$$

Thus

$$(a_n)_{n\geq 0} \cdot (b_n)_{n\geq 0} = (1,1,1,1,\dots) \cdot (1,-1,0,0,\dots) = (1,0,0,0,\dots). \tag{9}$$

Theorem 3.9. $(\mathbb{K}^{\mathbb{N}}, +, \odot)$ *is a commutative ring with*[4] 1*, but not an integral domain.*

Proof. **BP 4**. $\square$

Recall: A ring R with 1 is an integral domain if

$$\forall a, b \in R : a \cdot b = 0 \Rightarrow a = 0 \vee b = 0$$

If there are two elements $a, b \in R$ with $a \neq 0 \neq b$ and $a\, b = 0$, then and a and b are called zero divisors. Obviously, R is an integral domain if and only if it has no zero-divisors.

Example 3.10. $(\mathbb{K}^{\mathbb{N}}, +, \odot)$ contains zero-divisors: $(a_n)_{n\geq 0} = (1,0,1,0,1,0,\dots)$ and $(b_n)_{n\geq 0} = (0,1,0,1,0,1,\dots)$ are not the zero-sequence but their Hadamard product produces the zero-sequence:

$$(a_n)_{n\geq 0} \odot (b_n)_{n\geq 0} = (1,0,1,0,1,0,\dots) \odot (0,1,0,1,0,1,\dots) = (0,0,0,0,0,\dots).$$

Theorem 3.11. $(\mathbb{K}^{\mathbb{N}}, +, \cdot)$ *is a commutative ring with*[5] 1*, it is even an integral domain.*

Proof. **BP 5**: Show that $(\mathbb{K}^{\mathbb{N}}, +, \cdot)$ is a commutative ring with 1.
HW 12: Show that it is even an integral domain[6]. $\square$

Notation. For $(a_n)_{n\geq 0} \in \mathbb{K}^{\mathbb{N}}$ we also write

$$(a_n)_{n\geq 0} =: \sum_{n=0}^{\infty} a_n\, x^n = a(x)$$

with x an indeterminate (variable).
For $(\mathbb{K}^{\mathbb{N}}, +, \cdot)$ we shall write $(\mathbb{K}[[x]], +, \cdot)$ or $\mathbb{K}[[x]]$ for short and will call it also the *ring of formal power series over* $\mathbb{K}$.
Note: $(1,0,0,0,\dots) = 1\, x^0 + 0\, x^1 + 0\, x^2 + 0\, x^3 + \cdots = 1$ is the 1-element in $\mathbb{K}[[x]]$. If it is clear from the context, we simply write $a\, b$ instead of $a \cdot b$.

[4] Note: $(0,0,0,\dots)$ is the zero element and $(1,1,1,1,\dots)$ is the 1 element.
[5] Note: $(0,0,0,\dots)$ is the zero element and $(1,0,0,0,\dots)$ is the 1 element.
[6] Hint: To prove that the ring is integral, we show that it has no zero divisors. Namely, suppose that $(a_n)_{n\geq 0}$ and $(b_n)_{n\geq 0}$ are both not the zero-sequence (as warm up example suppose that $a_0 \neq 0 \neq b_0$). Then show that at least one entry in $(a_n)_{n\geq 0} \cdot (b_n)_{n\geq 0}$ is not zero.

Example 3.12. Rewriting (9) in its formal power series notation gives

$$\left(\sum_{n=0}^{\infty} x^n\right)(1-x) = 1.$$

In summary, the interpretation of (GS) in the algebra sense means that $1-x$ and $\sum_{n=0}^{\infty} x^n$ are the multiplicative inverses to each other, i.e., $\sum_{n=0}^{\infty} x^n$ multiplied by $1-x$ equals the 1-element. In short,

$$(1-x)^{-1} = \frac{1}{1-x} = \sum_{n=0}^{\infty} x^n.$$

Remark 3.13. We define

$$\mathbb{K}[x] = \left\{ \sum_{n=0}^{\infty} a_n\, x^n \in \mathbb{K}[[x]] \mid a_k = 0 \text{ for all } k \geq \delta \text{ for some } \delta \in \mathbb{N} \right\} \subseteq \mathbb{K}[[x]]$$

and call it the set of polynomials. Take two such polynomials $a(x) = \sum_{n=0}^{m_1} a_n\, x^n$ and $b(x) = \sum_{n=0}^{m_2} b_n\, x^n$ from $\mathbb{K}[x]$ (we define $a_k = 0$ for $k > m_1$ and $b_k = 0$ for $k > m_2$). Then the Cauchy product simplifies to

$$a(x) \cdot b(x) = \sum_{n=0}^{m_1+m_2} c_n x^n$$

with $c_n = \sum_{k=0}^{n} a_k\, b_{n-k}$. In Mathematica the multiplication $a(x), b(x) \in \mathbb{Q}[x]$ can be carried out, e.g., by `Expand[a*b]`. Note that $(\mathbb{K}[x], +, \cdot)$ itself is a ring with $1 \in \mathbb{K}[x]$ called the *polynomial ring over* $\mathbb{K}$. *This follows from the fact that for all* $a, b \in \mathbb{K}[x]$ *we have that* $a + b \in \mathbb{K}[x]$ *and* $a \cdot b \in \mathbb{K}[x]$ *i.e.,* $(\mathbb{K}[x], +, \cdot)$ *is a subring of* $(\mathbb{K}[[x]], +, \cdot)$. *Furthermore, since* $\mathbb{K}[[x]]$ *has no zero divisors, also its subset* $\mathbb{K}[x]$ *has no zero-divisors. In other words,* $(\mathbb{K}[x], +, \cdot)$ *itself is an integral domain.*

Remark 3.14. Take $\lambda \in \mathbb{K} \subseteq \mathbb{K}[[x]]$ and $b(x) = \sum_{n=0}^{\infty} b_n x^n \in \mathbb{K}[[x]]$ and consider the Cauchy product

$$\lambda \cdot b(x) := (\lambda, 0, 0, \dots) \cdot (b_0, b_1, b_2, \dots) = (c_n)_{n \geq 0}$$

with

$$c_n = \sum_{k=0}^{n} a_k b_{n-k}$$

with $a_0 = \lambda$ and $a_l = 0$ for $l \geq 1$. Then $c_n = \lambda\, b_n$ and hence

$$\lambda \cdot b(x) = (\lambda b_0, \lambda b_1, \lambda b_2, \dots) = \sum_{n=0}^{\infty} (\lambda\, b_n) x^n.$$

In other words, restricting $\cdot : \mathbb{K}[[x]] \times \mathbb{K}[[x]] \to \mathbb{K}[[x]]$ to $\cdot : \mathbb{K} \times \mathbb{K}[[x]] \to \mathbb{K}[[x]]$ yields precisely our scalar multiplication $* : \mathbb{K} \times \mathbb{K}[[x]] \to \mathbb{K}$ introduced in Definition 3.2 and by Lemma 3.4 it follows that $(\mathbb{K}[[x]], +, \cdot)$ with $\cdot : \mathbb{K} \times \mathbb{K}[[x]] \to \mathbb{K}[[x]]$ is a vector space over $\mathbb{K}$.

Lemma 3.15. *Take* $\lambda \in \mathbb{K}$, $m \in \mathbb{N}$ *and* $a(x) = \sum_{n=0}^{\infty} a_n x^n \in \mathbb{K}[[x]]$. *Then*

$$(\lambda\, x^m) \cdot \left(\sum_{n=0}^{\infty} a_n x^n \right) = \sum_{n=0}^{\infty} \lambda a_n x^{n+m} = \sum_{n=m}^{\infty} \lambda a_{n-m} x^n.$$

Proof. **HW 13**. □

Definition 3.16. *(coefficient functional)*
For $k \in \mathbb{N}$ *we define*

$$[x^k]\sum_{n=0}^{\infty} a_n x^n = a_k.$$

As shortcut we write

$$a(0) := [x^0]a(x) = a_0.$$

Lemma 3.17. *For* $k \in \mathbb{N}$ *and* $a(x), b(x) \in \mathbb{K}[[x]]$,

$$\begin{aligned}[x^k](a(x) + b(x)) &= [x^k]a(x) + [x^k]b(x),\\ [x^k](\lambda\, a(x)) &= \lambda[x^k]a(x).\end{aligned}$$

Proof. **HW 14**. □

Lecture from April 16, 2024

Remark 3.18. By the properties from Lemma 3.17 it follows that for a fixed $k \in \mathbb{N}$ the map

$$[x^k] : \mathbb{K}[[x]] \to \mathbb{K}$$

is a linear map.

HW 15. In $(\mathbb{K}[x], +, \cdot)$ prove

1. $\left(\sum_{n=0}^{\infty} c^n x^n\right)(1 - cx) = 1 \qquad (c \in \mathbb{K})$
2. $\left(\sum_{n=0}^{\infty} \frac{1}{n!}x^n\right)\left(\sum_{k=0}^{\infty} \frac{(-1)^n}{n!}x^n\right) = 1.$

Definition 3.19. *Let* R *be a commutative ring with* 1 *containing* $\mathbb{Q}$. *For* $r \in R$ *and* $k \in \mathbb{N}$ *we define the* falling factorial

$$\begin{aligned}&r^{\underline{k}} = r(r-1)(r-2)\cdots(r-k+1), \quad k \geq 1\\ &r^{\underline{0}} = 1\end{aligned}$$

and the *raising factorial*

$$\begin{aligned}&r^{\bar{k}} = r(r+1)(r+2)\cdots(r+k-1), \quad k \geq 1\\ &r^{\bar{0}} = 1.\end{aligned}$$

In addition, for $r \in R$ and $k \in \mathbb{Z}$ we define the *binomial coefficient with*

$$\binom{r}{k} := \begin{cases} \frac{r^{\underline{k}}}{k!} & k \geq 0\\ 0 & k < 0.\end{cases}$$

HW 16. Show for all $z \in \mathbb{C}$ and $k \in \mathbb{Z}$ that

$$\binom{z+1}{k} = \binom{z}{k} + \binom{z}{k-1}.$$

Definition 3.20. *The following formal power series deserve a short-cut notation:*

$$\begin{aligned}
exp(x) &:= \sum_{n=0}^{\infty} \frac{1}{n!} x^n \in \mathbb{K}[[x]], \\
exp(-x) &:= \sum_{n=0}^{\infty} \frac{(-1)^n}{n!} x^n \in \mathbb{K}[[x]], \\
\log(1+x) &:= \sum_{n=1}^{\infty} \frac{(-1)^{n+1}}{n} x^n \in \mathbb{K}[[x]], \\
\log(1-x) &:= -\sum_{n=1}^{\infty} \frac{1}{n} x^n \in \mathbb{K}[[x]].
\end{aligned}$$

Remark 3.21. From HW 15 we know that

$$\exp(x) \cdot \exp(-x) = 1,$$

i.e., $\exp(-x)$ is the multiplicative inverse of $\exp(x)$:

$$\exp(x)^{-1} := \exp(-x).$$

Remark 3.22. In analysis we know that

$$\frac{d}{dx} \log(1-x) = -\sum_{n=1}^{\infty} \frac{1}{n} n x^{n-1} = -\sum_{n=1}^{\infty} x^{n-1} = -\frac{1}{1-x}$$

with $|x| < 1$.

The last two remarks motivate us to consider the operations differentiation and division also in our formal ring $\mathbb{K}[[x]]$ in more details.

3.1 Differentiation and division

Definition 3.23. *Let $(R, +, \cdot)$ be a commutative ring with* 1 *(containing $\mathbb{Q}$ as a subring). Let $D : R \to R$ be a function such that*

$$\begin{aligned}
D(a+b) &= D(a) + D(b) \\
D(a \cdot b) &= D(a) \cdot b + a \cdot D(b)
\end{aligned}$$

for all $a, b \in R$. Then D is called a (formal) derivative on *R, and the pair (R, D) is called a* differential ring.

Lemma 3.24. *Consider $D_x : \mathbb{K}[[x]] \to \mathbb{K}[[x]]$ with*

$$D_x\Big(\sum_{n=0}^{\infty} a_n x^k\Big) = \sum_{n=0}^{\infty} a_{n+1}(n+1)x^n.$$

Then $(\mathbb{K}[[x]], D_x)$ is a differential ring.

Proof. **HW 17**. □

Example 3.25.

$$D_x \sum_{n=0}^{\infty} \frac{1}{n!}x^n = \sum_{n=0}^{\infty} \frac{1}{(n+1)!}(n+1)x^n = \sum_{n=0}^{\infty} \frac{1}{n!}.$$

This motivates the notation from above: for $\exp(x) := \sum_{n=0}^{\infty} \frac{1}{n!}x^n$ we have $D_x \exp(x) = \exp(x)$.

Definition 3.26. *We define the formal integration $\int_x : \mathbb{K}[[x]] \to \mathbb{K}[[x]]$ by*

$$\int_x \sum_{n=0}^{\infty} a_n\, x^n \mapsto \sum_{n=1}^{\infty} \frac{a_{n-1}}{n} x^n.$$

Remark 3.27. In analysis this formal integration is equivalent to the integration of a power series from 0 to x.

The action of D_x and $\int_x$ on the sequence representation of a formal power series is nothing else than the shift of the sequence (up to some normalizing factor) to the left or right:

$$D_x(a_0, a_1, a_2, a_3, \dots) = (1\,a_1, 2\,a_2, 3\,a_3, \dots)$$
$$\int_x (a_0, a_1, a_2, \dots) = (0, \tfrac{a_0}{1}, \tfrac{a_1}{2}, \tfrac{a_2}{3}, \dots).$$

This yields

Theorem 3.28. *For all $a(x) \in \mathbb{K}[[x]]$ we have*

1. $D_x \int_x a(x) = a(x)$ *"Fundamental Theorem of Calculus I"*
2. $\int_x D_x a(x) = a(x) - a(0)$ *"Fundamental Theorem of Calculus II"*
3. $[x^n]a(x) = \frac{1}{n!}\left((D_x)^n a(x)\right)|_{x=0}$ *"Taylor's formula"*

Proof. With

$$D_x \int_x (a_0, a_1, a_2, \dots) = D_x(0, \tfrac{a_0}{1}, \tfrac{a_1}{2}, \tfrac{a_2}{3}, \dots) = (a_0, a_1, a_3, \dots)$$

property 1 follows. With

$$\int_x D_x(a_0, a_1, a_2, a_3, \dots) = \int_x (1\,a_1, 2\,a_2, 3\,a_3, \dots) = (0, a_1, a_2, a_3, \dots)$$

and

$$\begin{aligned} a(x) = (a_0, a_1, a_2, a_3, \dots) =& (a_0, 0, 0, 0, \dots) + (0, a_1, a_2, a_3, \dots) \\ &= (a_0, 0, 0, 0, \dots) + \int_x D_x(a_0, a_1, a_2, a_3, \dots) \\ &= a(0) + \int_x D_x a(x) \end{aligned}$$

property 2 is established. Finally, observe that

$$\begin{aligned}
(D_x)^n(a_0, a_1, a_2, a_3, a_4, a_5, \dots) &= (D_x)^{n-1} D_x(a_0, a_1, a_2, a_3, a_4, a_5, \dots) \\
&= (D_x)^{n-1}(1\, a_1, 2\, a_2, 3\, a_3, 4\, a_4, 5\, a_5, \dots) \\
&= (D_x)^{n-2} D_x(1\, a_1, 2\, a_2, 3\, a_3, 4\, a_4, 5\, a_5, \dots) \\
&= (D_x)^{n-2}(1 \cdot 2\, a_2, 2 \cdot 3\, a_3, 3 \cdot 4\, a_4, 4 \cdot 5\, a_5 \dots) \\
&= (D_x)^{n-3} D_x(1 \cdot 2\, a_2, 2 \cdot 3\, a_3, 3 \cdot 4\, a_4, 4 \cdot 5\, a_5 \dots) \\
&= (D_x)^{n-3}(1 \cdot 2 \cdot 3\, a_3, 2 \cdot 3 \cdot 4\, a_4, 3 \cdot 4 \cdot 5\, a_5, \dots) \\
&= \cdots = (n! a_n, \tfrac{n!}{1!} a_{n+1}, \tfrac{n!}{2!} a_{n+2}, \tfrac{n!}{3!} a_{n+3}, \dots)
\end{aligned}$$

which gives $(D_x)^n(a_0, a_1, a_2, a_3, \dots)|_{x=0} = n! a_n = n! [x^n] a(x)$, and thus proves property 3. $\square$

The following property is particular strong: one can invert a formal power series if and only if the constant term does not vanish.

Theorem 3.29. *[multiplicative inverse] Let $a(x) \in \mathbb{K}[[x]]$. Then:*

$$\boxed{\text{There exists a } b(x) \in \mathbb{K}[[x]] \text{ with } a(x) \cdot b(x) = 1} \quad \Leftrightarrow \quad \boxed{a(0) \neq 0}.$$

Proof. Let $a(x) = \sum_{n=0}^{\infty} a_n\, x^n$.
$\Rightarrow$: Suppose that there is a $b(x) = \sum_{n=0}^{\infty} b_n\, x^n$ with

$$a(x) \cdot b(x) = 1.$$

Then by the definition of the Cauchy product,

$$a_0\, b_0 = 1$$

and thus, since $\mathbb{K}$ is a field, $a(0) = a_0 \neq 0$.
$\Leftarrow$ Suppose that $a_0 \neq 0$. We construct $b(x) = b_n\, x^n$ such that

$$1\, x^0 + 0\, x^1 + 0\, x^2 + \cdots = 1 = a(x) \cdot b(x) = \left(\sum_{n=0}^{\infty} a_n\, x^n \right) \cdot \left(\sum_{n=0}^{\infty} b_n\, x^n \right) = \sum_{n=0}^{\infty} x^n \sum_{k=0}^{n} a_k\, b_{n-k}. \quad (10)$$

By coefficient comparison in equation (10) at $[x^0]$ we get $a_0\, b_0 = 1$ and thus with $a_0 \neq 0$ we get (in the field $\mathbb{K}$)

$$\boxed{b_0 = \frac{1}{a_0},} \quad (11)$$

i.e., b_0 is determined. Furthermore, by coefficient comparison in equation (10) at $[x^n]$ with $n \geq 1$ we get

$$0 = \sum_{k=0}^{n} a_k\, b_{n-k} = a_0\, b_n + \sum_{k=1}^{n} a_k\, b_{n-k}$$

and hence

$$\boxed{b_n = -\frac{1}{a_0} \sum_{k=1}^{n} a_k\, b_{n-k}.} \quad (12)$$

Summarizing,

- given a_0, we can determine b_0 with (11),
- given a_0, a_1 and b_0 we can use the formula in (12) to determine b_1,
- given a_0, a_1, a_2 and b_0, b_1, we can use the formula in (12) to determine b_2,
- ...

and thus all b_n can be determined iteratively for $a(x) = \sum_{n=0}^{\infty} a_n x^n$. □

Lecture from April 23, 2024

Note 1: If the standard operations in $\mathbb{K}$ are computable and if the coefficients $a_0, a_1, \dots, a_l$ ($a_0 \neq 0$) are given explicitly (can be computed by an algorithm), also the first coefficients $b_0, b_1, \dots, b_l$ ($b_0 \neq 0$) can be computed. In particular, we get

$$\left(\sum_{n=0}^{l} a_l\right)\left(\sum_{n=0}^{l} b_l\right) = \boxed{1} + \underbrace{0\,x^1 + 0\,x^2 + \cdots + 0\,x^l}_{=0} + c_{l+1}x^{l+1} + c_{l+2}x^{l+2}$$

where $c_{l+1}, c_{l+2}, \dots$ are error terms (which arise since we only considered the first $l+1$ coefficients of $a(x)$ and $b(x)$).

Note 2: Let $b(x), \tilde{b}(x) \in \mathbb{K}[[x]]$ such that

$$a(x) \cdot b(x) = 1 = a(x) \cdot \tilde{b}(x).$$

Then $b(x) \cdot (a(x) \cdot b(x)) = b(x) \cdot (a(x) \cdot \tilde{b}(x))$ and thus

$$\begin{aligned} b(x) &= (a(x) \cdot b(x)) \cdot b(x) = (b(x) \cdot a(x)) \cdot b(x) \\ &= \boxed{b(x) \cdot (a(x) \cdot b(x)) = b(x) \cdot (a(x) \cdot \tilde{b}(x))} \\ &= (b(x) \cdot a(x)) \cdot \tilde{b}(x) = (a(x) \cdot b(x)) \cdot \tilde{b}(x) = \tilde{b}(x), \end{aligned}$$

i.e., $b(x) = \tilde{b}(x)$. Consequently, if $a(x)$ has a multiplicative inverse $b(x)$ (i.e., if $a(x) \neq 0$), then it is unique and motivates the following notation.

Notation. Let $a(x) \in \mathbb{K}[[x]]$ with $a(0) \neq 0$. Then for the multiplicative inverse $b(x) \in \mathbb{K}[[x]]$ of $a(x)$ (determined, e.g., by the above theorem) we also write

$$a^{-1}(x) := b(x) \text{ or } \frac{1}{a(x)} := b(x).$$

Example. We have $(1-x) \cdot \sum_{n=0}^{\infty} x^n = 1$, i.e., the multiplicative inverse of $1-x$ is $\sum_{n=0}^{\infty} x^n$ and we write

$$(1-x)^{-1} = \frac{1}{1-x} = \sum_{n=0}^{\infty} x^n.$$

Furthermore, the multiplicative inverse of $\sum_{n=0}^{\infty} x^n$ is $(1-x)$ and we write

$$\left(\sum_{n=0}^{\infty} x^n\right)^{-1} = \frac{1}{\sum_{n=0}^{\infty} x^n} = 1 - x.$$

Example. By HW. 15 we have $\exp(x) \cdot \exp(-x) = 1$. Thus $\exp(-x)$ is the multiplicative inverse of $\exp(x)$, i.e.,

$$\exp(x)^{-1} = \frac{1}{\exp(x)} = \exp(-x);$$

furthermore, $\exp(x)$ is the multiplicative inverse of $\exp(-x)$, i.e.,

$$\exp(-x)^{-1} = \frac{1}{\exp(-x)} = \exp(x).$$

HW 18. Let $\exp(c\,x) := \sum_{n=0}^{\infty} \frac{c^n}{n!} x^n$. For $a, b \in \mathbb{K}$ show:

$$\exp(a\,x)\exp(b\,x) = \exp((a+b)x).$$

Hint for possible solutions of the HWs below: Compute the first coefficients b_n and use Sloan's database `https://oeis.org` to find a closed form.

HW 19. Find a closed form for the coefficients in the multiplicative inverse of $(1-2x)^2 \in \mathbb{K}[[x]]$.

HW 20. Find a closed form for the coefficients in the multiplicative inverse of $(1-x)^3 \in \mathbb{K}[[x]]$.

HW 21. Find a closed form for the coefficients in the multiplicative inverse of $\exp(2x) \in \mathbb{K}[[x]]$.

3.2 Finding closed forms for generating functions

Example Find a closed form for

$$H(x) = \sum_{n=0}^{\infty} H_n x^n \in \mathbb{K}[[x]]$$

where H_n denote the harmonic numbers ($H_0 = 0$).

$\boxed{\text{TACTIC:}}$ Find a (functional) equation for $H(x)$.

A) by using the recurrence for H_n:

$$H_{n+1} = H_n + \frac{1}{n+1}$$

with $H_0 = 0$.
Note: we stay in $\mathbb{K}[[x]]$ (no analysis!)
Using the recurrence (in the second line) we get

$$\begin{aligned}
H(x) &= \sum_{n=0}^{\infty} H_n\, x^n = \sum_{n=1}^{\infty} H_n\, x^n = \sum_{n=0}^{\infty} H_{n+1}\, x^{n+1} \\
&= \sum_{n=0}^{\infty} \left(H_n + \frac{1}{n+1} \right) x^{n+1} \\
&= x \sum_{n=0}^{\infty} H_n\, x^n + \sum_{n=0}^{\infty} \frac{x^{n+1}}{n+1} \\
&= xH(x) - \log(1-x)
\end{aligned}$$

and thus

$$\boxed{H(x) = -\frac{1}{1-x} \log(1-x).} \tag{13}$$

Note 1: Here we use that $(1-x)\frac{1}{1-x} = 1$.

Note 2: We consider $-\frac{1}{1-x}\log(1-x)$ as a closed form for $H(x)$ since it is the product of well known formal power series which we gave already special names:

- the geometric series $\frac{1}{1-x} = \sum_{n=0}^{\infty} x^n$;
- the logarithmic power series $\log(1-x) = -\sum_{n=1}^{\infty} \frac{x^n}{n}$; see also Definition 3.20.

B) by using an extra lemma (which we will use later again)

Lemma 3.30. *We have*[7]

$$\sum_{n=0}^{\infty} x^n \left(\sum_{k=0}^{n} a_k \right) = \frac{1}{1-x} \sum_{n=0}^{\infty} a_n\, x^n$$

or equivalently (by multiplying with $1-x$)

$$(1-x) \sum_{n=0}^{\infty} x^n \left(\sum_{k=0}^{n} a_k \right) = \sum_{n=0}^{\infty} a_n x^n.$$

[7] The Cauchy product of $\frac{1}{1-x}$ with a formal power series $a(x) = \sum_{n=0}^{\infty} a_n\, x^n$ yields a formal power series whose coefficients are $\sum_{k=0}^{n} a_k$.

Proof.

$$
\begin{aligned}
\text{LHS} &= (1-x)\sum_{n=0}^{\infty} x^n \left(\sum_{k=0}^{n} a_k\right) \\
&= \underbrace{\sum_{n=0}^{\infty} x^n \left(\sum_{k=0}^{n} a_k\right)}_{x^0\, a_0 + \sum_{n=1}^{\infty} x^n \left(\sum_{k=0}^{n} a_k\right)} - \underbrace{\sum_{n=0}^{\infty} x^{n+1} \left(\sum_{k=0}^{n} a_k\right)}_{\sum_{n=1}^{\infty} x^n \left(\sum_{k=0}^{n-1} a_k\right)} \\
&= x_0\, a_0 + \sum_{n=1}^{\infty} x^n \left(\underbrace{\sum_{k=0}^{n} a_k - \sum_{k=0}^{n-1} a_k}_{a_n}\right) \\
&= \sum_{n=0}^{\infty} a_n x^n = \text{RHS}.
\end{aligned}
$$

□

Remark: The special case of the above lemma with

$$
a_k = \begin{cases} 1 \text{ if } k = 0 \\ 0 \text{ if } k \geq 1 \end{cases}
$$

gives

$$
(1-x)\sum_{n=0}^{\infty} x^n = 1.
$$

Another special case can be used for $H(x)$:

$$
\begin{aligned}
H(x) &= \sum_{n=0}^{\infty} x^n \sum_{k=0}^{n} a_k \quad \text{where } a_k = \begin{cases} 0 \text{ if } k = 0 \\ \frac{1}{k} \text{ if } k \geq 1 \end{cases} \\
&= \frac{1}{1-x}\sum_{n=0}^{\infty} a_n x^n \\
&= \frac{1}{1-x}\left(0 + \sum_{n=1}^{\infty} \frac{x^n}{n}\right) \\
&= -\frac{1}{1-x}\log(1-x).
\end{aligned}
$$

HW 22. Consider the formal power series $f(x) = \frac{1}{(1-x)^2}\log(1-x) \in \mathbb{Q}[[x]]$. Express the coefficients $f_n \in \mathbb{Q}$ of $f(x) = \sum_{k=0}^{\infty} f_n x^n$ in terms of the harmonic numbers H_n.

4 Application: binary trees

We will apply the tools from the previous section in order to explore binary trees.

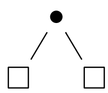
Definition 4.1. *A binary tree is*

- *a single external node (denoted by* $\square$*)*
- *or an internal node (denoted by* $\bullet$*) that is connected to two binary trees: a left and a right subtree.*

To warm up, we consider all trees with n external nodes for $n = 1, 2, 3, 4$.
For $n = 1$ we get:

t_0

For $n = 2$ we get:

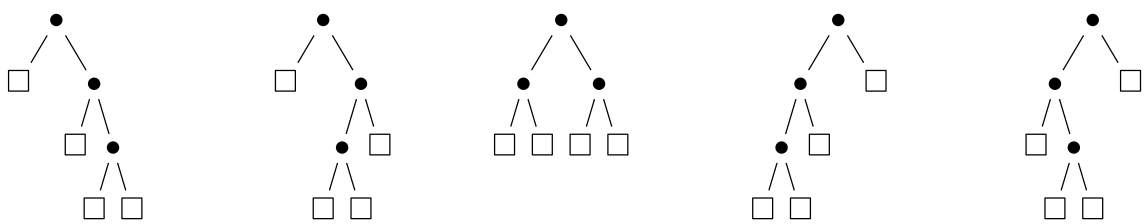


$t_1 = t_0\, t_0$

For $n = 3$ we get:

$t_2 = \quad t_0\, t_1 \quad + \quad t_1\, t_0$

And for $n = 4$ we get:



$t_3 = \quad t_0\, t_2 \quad + \quad t_1\, t_1 \quad + \quad t_2\, t_0$

In the following we want to explore

$$\boxed{t_n := \text{the number of binary trees with } n+1 \text{ external nodes.}}$$

Looking at the above enumeration we get

n	0	1	2	3	…	n	…
t_n	1	1	2	5	…	?	…

The main goal is to produce a general formula for t_n. Note that we can produce all trees with $n+1$ external nodes by considering all trees of the form

	$\bullet$	
a binary tree with $k+1$ external nodes		a binary tree with $n-k$ external nodes

with $k = 0, 1, 2, \ldots, n-1$. Summarizing, we get

$$\begin{aligned} t_0 &= 1 \\ t_n &= \sum_{k=0}^{n-1} t_k \, t_{n-k-1}. \end{aligned} \tag{14}$$

For instance,

$$\begin{aligned} t_1 &= t_0 \, t_0 = 1 \\ t_2 &= t_0 \, t_1 + t_1 \, t_0 = 1 + 1 = 2 \\ t_3 &= t_0 \, t_2 + t_1 \, t_1 + t_2 \, t_0 = 2 + 1 + 2 = 5; \end{aligned}$$

note that this formula is also reflected in the graphical enumeration from above.

In general, we can now calculate any value t_n with $n \in \mathbb{N}$ using this recursion formula. But we can do much better!

After this preparation step we can activate our formal power series engine by defining the generating function

$$t(x) = \sum_{n=0}^{\infty} t_n \, x^n \in \mathbb{Q}[[x]].$$

Hence

$$\begin{aligned} t(x) &= t_0 \, x^0 + \sum_{n=1}^{\infty} x^n \sum_{k=0}^{n-1} t_k \, t_{n-1-k} \\ &= 1 + \sum_{n=0}^{\infty} x^{n+1} \sum_{k=0}^{n} t_k \, t_{n-k} \\ &= 1 + x \sum_{n=0}^{\infty} x^n \sum_{k=0}^{n} t_k \, t_{n-k} \end{aligned}$$

and by the Cauchy product we get

$$= 1 + x \, t(x)^2.$$

Summarizing, we obtain the following functional equation:

$$\boxed{x \, t(x)^2 - t(x) + 1 = 0.} \tag{15}$$

As it turns out, the following trick makes our life easier: multiply the equation with x. This gives

$$x^2\, t(x)^2 - x\, t(x) + x = 0.$$

Thus if we define

$$T(x) := x\, t(x) \in \mathbb{Q}[[x]]$$

we get

$$\begin{gathered} T(x)^2 - T(x) + x = 0 \\ || \\ \underbrace{T(x)^2 - 2T(x)\cdot\tfrac{1}{2} + \left(\tfrac{1}{2}\right)^2}_{=\left(T(x)-\frac{1}{2}\right)^2} - \tfrac{1}{4} + x \end{gathered}$$

which is equivalent to

$$\begin{gathered} (T(x) - \tfrac{1}{2})^2 = \tfrac{1}{4}(1-4x). \\ \Updownarrow \\ (2T(x)-1)^2 = 1-4x. \end{gathered}$$

Lemma 4.2. *Let $g(x) \in \mathbb{K}[[x]]$ with $g(0) = 1$. Then there is a unique $f(x) \in \mathbb{K}[[x]]$ with $f(x)^2 = g(x)$ and $f(0) = 1$. In addition, there is exactly one other solution which is $-f(x)$.*

Proof. **HW 23** (Hint: adapt the proof of Theorem 3.29). □

With this lemma it follows that we can take $f(x) \in \mathbb{K}[[x]]$ with $f(0) = 1$ such that

$$f(x)^2 = 1 - 4x. \tag{16}$$

In particular, we get

$$\begin{gathered} 2T(x) - 1 = \pm f(x) \\ \Updownarrow \\ T(x) = \frac{1}{2} \pm \frac{1}{2} f(x). \end{gathered}$$

In the following we will write for the unique $f(x) \in \mathbb{Q}[[x]]$ with $f(0) = 1$ and $f(x)^2 = 1 - 4x$ also

$$\sqrt{1-4x} := f(x).$$

Thus we get

$$T(x) = \frac{1}{2} \pm \frac{1}{2}\sqrt{1-4x};$$

Looking at the constant term on both sides shows that

$$T(x) = \frac{1}{2} - \frac{1}{2}\sqrt{1-4x};$$

the plus version would have given $[x^0](\frac{1}{2} + \frac{1}{2}\sqrt{1-4x}) = 1$, but we have $[x^0]T(x) = 0$.