

**MATH 132 Lecture notes**

# **COUNTING**

## Zoom tips

- To save the bandwidth, it is better if you turn off your cameras.
- By default, I have muted your microphones. You can still unmute them (an icon in the lower left corner), but please do not take advantage of that! Then, mute it back to reduce noise.
- Your questions are still welcome. Should you have one, either unmute your mike or “raise hand” (somewhere in the app menu). Hopefully, I will see your hand in the screen sharing mode and will know what to do!
- By default, the video switches to whoever is speaking. If you want to keep my notes on your screen, pin them (by double clicking).
- You can also use chat for questions, but, again, for the moment I don’t know if and when I see them. Let’s try together.
- I am open to your suggestions concerning the format of these meetings (lecture notes, live broadcast from my office with the whiteboard, any other suggestions).
- **Attendance is taken automatically by the system**; you don’t need to do anything but **attend**! As far as I know, everything is logged: login time, logout time, and even *the time that the Zoom window has stayed in focus!* :)

## 1. A reminder

We have learned so far:

- (1) the **Sum Rule**:  $|A \cup B| = |A| + |B|$  *provided that  $A$  and  $B$  are disjoint*;
- (2) the **Product Rule**: roughly,  $|A \times B| = |A| \cdot |B|$ ;
- (3) the **Subtraction Rule**:  $|A \cup B| = |A| + |B| - |A \cap B|$ ;
- (4) the **Division Rule**: count and divide by the overcount.

## 2. Permutations

**Definition 2.1.** A **permutation** of  $n$  **distinct** objects is an **ordered** arrangement of these objects. (In other words, a permutation of objects is a way to order them.) The number of permutations is  $P(n)$ .

More generally, an  $r$ -permutation of  $n$  **distinct** object is an ordered arrangements of  $r$  out of these objects. Notation:  $P(n, r)$ .

**Example 2.2.** The permutations of the three objects  $\{a, b, c\}$  are:

$$(2.3) \quad a, b, c; \quad a, c, b; \quad b, a, c; \quad b, c, a; \quad c, a, b; \quad c, b, a.$$

The 1-permutations are

$$(2.4) \quad a; \quad b; \quad c,$$

and the 2-permutations are

$$(2.5) \quad a, b; \quad b, a; \quad a, c; \quad c, a; \quad b, c; \quad c, b.$$

Thus, we *select and order*!

**Theorem 2.6.** If  $0 \leq r \leq n$  are integers, then

$$P(n, r) = n \cdot (n - 1) \cdot \dots \cdot (n - r + 1).$$

*Special cases:*

- $P(n, 0) = 1$ : there is **one** way to do nothing: **do nothing**!
- $P(n, 1) = n$ , cf. (2.4): we just select one out of  $n$  objects.
- $P(n) = P(n, n) = n!$ , cf. (2.3).

*Proof.* We use the **Product Rule**:

$$\begin{array}{lll} (n) \text{ ways to select the 1st object:} & 2 & \{1, \underline{2}, 3, 4, 5, 6, 7\} \\ (n-1) \text{ ways to select the 2nd object:} & 2, 6 & \{1, \underline{2}, 3, 4, 5, \underline{6}, 7\} \\ (n-2) \text{ ways to select the 3rd object:} & 2, 6, 1 & \{\underline{1}, \underline{2}, 3, 4, 5, \underline{6}, 7\} \\ & \dots\dots & \end{array}$$

$$(n-r+1) \text{ ways to select the } r\text{-th object:} \quad 2, 6, 1, 4 \quad \{\underline{1}, \underline{2}, 3, \underline{4}, 5, \underline{6}, 7\}.$$

The product  $(n)(n-1)(n-2)\dots(n-r+1)$  is  $P(n, r)$ .  $\square$

**Corollary 2.7.** This formula can be written in a more compact way

$$\begin{aligned} P(n, r) &= n \cdot (n-1) \cdot \dots \cdot (n-r+1) \frac{(n-r)!}{(n-r)!} \\ &= \frac{n \cdot (n-1) \cdot \dots \cdot (n-r+1) \cdot (n-r) \cdot \dots \cdot 1}{(n-r)!} = \frac{n!}{(n-r)!}, \end{aligned}$$

which, however, is usually much more difficult to compute.

**Example 2.8.** What is the number of ways to select the 1st, 2nd, and 3rd prize winners among 100 participants?

*Solution:* Since the order (who gets what) matters, we are speaking about permutations:

*NB: Normally, there is no need to compute things like this anyway!*

$$P(100, 3) = 100 \cdot 99 \cdot 98 = 970,200 \left( = \frac{100!}{97!} : \text{cannot compute this!} \right).$$

**Example 2.9.** What is the number of ways to rearrange the letters “ABCDEFGH” if:

- (1) there are no further restrictions?
- (2) the string must contain “ABC” as a substring?
- (3) the letters ABC must stay together, but in any order?

*Solution:* (1) These are naked permutations:  $P(8) = 8! = 40,320$ .

(2) We treat the three letters ABC as a single block, thus speaking about the permutations of the *six* letters **ABC** D E F G H. (For example, in some languages **œ** is a single letter, even though it is pretty much the same as “oe”; *cf.* **cœ**re  $\approx$  coere.) Thus, the number is  $P(6) = 6! = 720$ .

(3) We solve Problem (2) first, and then rearrange the three letters **ABC** within their single block. By the **Product Rule**, the total number is  $P(6) \cdot P(3) = 6! \cdot 3! = 4,320$ .

*NB: Normally, do not compute this!*

*This trick will be used very often, on various occasions*

### 3. Combinations

**Definition 3.1.** A **combination** of  $r$  out of  $n$  **distinct** objects (or an  $r$ -**combination**) is an **unordered** selection of  $r$  out of these objects. The number is

$$C(n, r) = \binom{n}{r} = {}_nC_r = C_n^r = \dots$$

We use the blue ones; the second is pronounced “ $n$  choose  $r$ .” Another name for these numbers is **binomial coefficients** (see §4 below).

Alternatively, since combinations are *unordered*,  $C(n, r)$  is the number of  $r$ -element subsets of an  $n$ -element set.

**Example 3.2.** Here are the 2-combinations of a 3-element set  $\{a, b, c\}$

$$a, b; \quad a, c; \quad b, c$$

(cf. (2.5) for the permutations) and the 2-combinations of a 4-element set  $\{a, b, c, d\}$ :

$$a, b; \quad a, c; \quad a, d; \quad b, c; \quad b, d; \quad c, d.$$

**Theorem 3.3.** If  $0 \leq r \leq n$  are integers, then

$$C(n, r) = \frac{P(n, r)}{r!} = \frac{n!}{r!(n-r)!}.$$

*Proof.* There are  $P(n, r)$  permutations of  $r$  out of  $n$  objects. However, in this count each  $r$ -combination is counted  $P(r) = r!$  times: this is the number of ways to order the  $r$  objects selected. Hence, by the **Division Rule**, we need to divide the count by  $r!$ .  $\square$

**Example 3.4.** Here are a few special cases (remember that  $0! = 1$ ):

- $C(n, 0) = n!/(0! \cdot n!) = 1$ : there is one way to select nothing!
- $C(n, n) = n!/(n! \cdot 0!) = 1$ : there is one way to select everything!
- $C(n, 1) = n$ : there are  $n$  ways to select one out of  $n$ .
- $C(n, 2) = \frac{n(n-1)}{2}$ : just by the formula.

In general, if  $r$  is small, we usually use the expression for  $P(n, r)$  given by **Theorem 2.6**, viz.,

$$C(n, r) = \frac{n \cdot (n-1) \cdot \dots \cdot (n-r+1)}{r!},$$

followed by a number of cancellations before the multiplication. (After all, we **do** know that the result is an integer, so **everything** should cancel out!) For example,

$$C(10, 3) = \frac{10 \cdot 9 \cdot 8}{1 \cdot 2 \cdot 3} = \frac{10 \cdot 3 \cdot 4}{1 \cdot 1 \cdot 1} = 120.$$

**NB:** we do expect you to compute the combinations of reasonable size, especially if they are used further!

**NB:** a popular class of problems!

**NB:** this probably should not be computed in the exams

Another useful fact!

**Example 3.5.** As another example, what is the number of distinct poker hands (5 cards) can be dealt from the standard deck of 52 cards?

*Solution:* Since the order of the cards does not matter, the answer is given by combinations:

$$C(52, 5) = \frac{52 \cdot 51 \cdot 50 \cdot 49 \cdot 48}{1 \cdot 2 \cdot 3 \cdot 4 \cdot 5} = 52 \cdot 17 \cdot 10 \cdot 49 \cdot 6 = 2,598,960.$$

**Example 3.6.** The number of bit strings of length  $n$  with exactly  $r$  1's = the number of  $r$ -element subsets of an  $n$ -element set =  $C(n, r)$ .

The binomial coefficients are subject to a huge number of identities (more than in trigonometry); we will only learn half a dozen or so. Also, these identities are a very popular subject for exam questions!

The next corollary is a fundamental fact that is taken for granted in all computations! It usually goes without saying!

**Corollary 3.7** (of Theorem 3.3). For all integers  $0 \leq r \leq n$  we have

$$C(n, r) = C(n, n - r) \quad \text{or} \quad \binom{n}{r} = \binom{n}{n - r}$$

*First proof: algebraic.*

$$C(n, r) = \frac{n!}{r!(n - r)!} = \frac{n!}{(n - r)!(n - (n - r))!} = C(n, n - r) \quad \square$$

*Second proof: combinatorial.*  $C(n, r)$  is the number of  $r$ -element subsets of a certain  $n$ -element set  $U$ , whereas  $C(n, n - r)$  is the number of  $(n - r)$ -element subsets of the same  $U$ . However, the two sets are equipotent, an explicit bijection being

$$S \mapsto U - S.$$

Since  $|U - S| = n - |S|$ , we have  $|S| = r$  if and only if  $|U - S| = n - r$ :

$$S = \{2, 3, 6\} \quad \left\{ \overset{1}{\cdot} \overset{2}{\bullet} \overset{3}{\bullet} \overset{4}{\cdot} \overset{5}{\cdot} \overset{6}{\bullet} \overset{7}{\cdot} \right\} \quad U - S = \{1, 4, 5, 7\}.$$

Therefore, the numbers of  $r$ - and  $(n - r)$ -element subsets are equal.  $\square$

A *combinatorial proof* of an equality consists in counting the number of elements of the same set in two different ways and equating the results. More generally, as in the previous example, one can count the sizes of two sets  $A$  and  $B$  and establish a bijection  $A \leftrightarrow B$ , concluding that  $A$  and  $B$  are equipotent, i.e.,  $|A| = |B|$ . Often (unlike the previous example), combinatorial proof are much easier than algebraic, especially when it comes to combinatorial identities. We will see more examples.

In the previous proof:

- $A = \{r\text{-element subsets of } U\}$ , so that  $|A| = C(n, r)$ ;
- $B = \{(n - r)\text{-element subsets of } U\}$ ; so that  $|B| = C(n, n - r)$ ;
- the bijection is  $S \mapsto U - S$ .

Instead of looking at what's selected, look at what's left.

**Or:** repaint black to white and vice versa

## 4. The binomial formula

From high school:

$$(x + y)^0 = 1 \quad \text{trivial}$$

$$(x + y)^1 = x + y \quad \text{trivial}$$

$$(x + y)^2 = x^2 + 2xy + y^2 \quad \text{everyone knows this!}$$

$$(x + y)^3 = x^3 + 3x^2y + 3xy^2 + y^3 \quad \text{everyone knows this!}$$

$$(x + y)^4 = x^4 + 4x^3y + 6x^2y^2 + 4xy^3 + y^4$$

$$(x + y)^5 = x^5 + 5x^4y + 10x^3y^2 + 10x^2y^3 + 5xy^4 + y^5$$

There probably must be a “formula” for any  $(x + y)^n$ ? Yes, there is!

**Theorem 4.1** (The Binomial Theorem; Newton). *For any integer  $n \geq 0$ :*

$$\begin{aligned} (x + y)^n &= \sum_{r=0}^n \binom{n}{r} x^{n-r} y^r \\ &= \binom{n}{0} x^n y^0 + \binom{n}{1} x^{n-1} y + \dots + \binom{n}{n-1} x y^{n-1} + \binom{n}{n} x^0 y^n. \end{aligned}$$

In all such formulas, we let  $x^0 = 1$  no matter what: even  $0^0 = 1$ . Forget Calculus! Or, as in Calculus:  $\lim_{x \rightarrow 0} x^0 = 1$ .

*Combinatorial proof.* We have

$$\begin{aligned} (x + y)^n &= \underbrace{(x + y) \cdot (x + y) \cdot \dots \cdot (x + y)}_{n \text{ factors}} \\ &= \underbrace{\dots + \underbrace{(x \text{ or } y) \cdot (x \text{ or } y) \cdot \dots \cdot (x \text{ or } y)}_{n \text{ factors}} + \dots}_{2^n \text{ summands}} \end{aligned}$$

For  $x^{n-r} y^r$ , we need to select  $r$  (out of  $n$ ) places for  $y$ ; the rest are  $x$ 's. For example:

$$6x^2y^2 = yyxx + yxyx + yxxy + xyxy + xyyx + xxyy.$$

This is the same as  $r$ -element subsets (the positions of the  $y$ 's) of the  $n$ -element set of factors.  $\square$

An algebraic proof (by induction) is to be found later.

**Example 4.2.** What is the coefficient of  $x^{12}y^{13}$  in  $(2x - 3y)^{25}$ ?

*Solution:*  $(2x - 3y)^{25} = ((2x) + (-3y))^{25}$ ; hence, the term with  $x^{12}y^{13}$  is

$$\binom{25}{12} (2x)^{12} (-3y)^{13} = \left( -\frac{25!}{12! 13!} 2^{12} 3^{13} \right) x^{12} y^{13}.$$

**Remark 4.3** (Digression). Later, we will say that  $(x + y)^N$  is the so-called *generating function* for the sequence  $a_n := C(N, n)$ : in a sense, this simple expression “knows” everything about the complicated sequence of numbers!

**Corollary 4.4** (**another fundamental fact**). For each integer  $n \geq 0$ :

$$\sum_{r=0}^n \binom{n}{r} = 2^n.$$

*First proof: algebraic.*

$$2^n = (1 + 1)^n = \sum_{r=0}^n \binom{n}{r} 1^{n-r} 1^r = \sum_{r=0}^n \binom{n}{r}. \quad \square$$

*Second proof: combinatorial.* Let us consider the  $n$ -element universe  $U = \{1, \dots, n\}$  and count the number of subsets of  $U$ :

$$C(n, 0) = \#\{\text{0-element subsets of } U\}$$

$$C(n, 1) = \#\{\text{1-element subsets of } U\}$$

$$C(n, 2) = \#\{\text{2-element subsets of } U\}$$

.....

$$C(n, r) = \#\{\text{r-element subsets of } U\}$$

.....

$$C(n, n) = \#\{\text{n-element subsets of } U\}$$

---


$$\sum C(n, r) = \#\{\text{all subsets of } U\} = |\mathcal{P}(U)| = 2^n. \quad \square$$

**Remark 4.5.** Together with the independent algebraic proof, the combinatorial one gives us yet another proof of the formula  $|\mathcal{P}(U)| = 2^{|U|}$ .

**Corollary 4.6** (**there are lots of others like this**). For each integer  $n \geq 0$ :

$$\sum_{r=0}^n 2^r \binom{n}{r} = 3^n.$$

*Proof.*

$$3^n = (1 + 2)^n = \sum_{r=0}^n \binom{n}{r} 1^{n-r} 2^r = \sum_{r=0}^n 2^r \binom{n}{r}. \quad \square$$

**Corollary 4.7** (**this one is important**). For each integer  $n \geq 1$ :

$$\sum_{r=0}^n (-1)^r \binom{n}{r} = 0.$$

In other words, the sum of all “even” binomial coefficients  $C(n, 2k)$  equals the sum of all “odd” ones  $C(n, 2k + 1)$ . This statement clearly does **not** hold for  $n = 0$  ( $1 \neq 0$ ). Why?

*Proof.*

$$0 = 0^n = (1 - 1)^n = \sum_{r=0}^n \binom{n}{r} 1^{n-r} (-1)^r = \sum_{r=0}^n (-1)^r \binom{n}{r}. \quad \square$$

Because of the symmetry of the binomial coefficients, see [Corollary 3.7](#), [Corollary 4.7](#) is obvious when  $n$  is odd:

$$1 - 1 = 0 \quad (n = 1),$$

$$1 - 3 + 3 - 1 = 0 \quad (n = 3),$$

$$1 - 5 + 10 - 10 + 5 - 1 = 0 \quad (n = 5),$$

$$1 - 7 + 21 - 35 + 35 - 21 + 7 - 1 = 0 \quad (n = 7).$$

However, it is somewhat more mysterious when  $n$  is even:

$$1 - 2 + 1 = 0 \quad (n = 2),$$

$$1 - 4 + 6 - 4 + 1 = 0 \quad (n = 4),$$

$$1 - 6 + 15 - 20 + 15 - 6 + 1 = 0 \quad (n = 6),$$

$$1 - 8 + 28 - 56 + 70 - 56 + 28 - 8 + 1 = 0 \quad (n = 8).$$

**Corollary 4.8** (of [Corollaries 4.4](#) and [4.7](#)). For each integer  $n \geq 1$ ,

$$\sum_{k=0}^{\lfloor n/2 \rfloor} \binom{n}{2k} = \sum_{k=0}^{\lfloor (n-1)/2 \rfloor} \binom{n}{2k+1} = 2^{n-1}.$$

## 5. Pascal's identity

**Theorem 5.1** (Pascal's identity). *For all integers  $n \geq 0$  and  $r$ , one has*

$$\binom{n+1}{r} = \binom{n}{r-1} + \binom{n}{r}.$$

**Remark 5.2.** For this and many other identities, we extend the numbers  $C(n, r)$  to all integers  $r$  (still,  $n \geq 0$ ) by letting

$$C(n, r) = 0 \quad \text{whenever } r < 0 \text{ or } r > n.$$

This agrees both with the combinatorial interpretation (there is no way to select  $< 0$  or  $> n$  objects) and algebraic formulas (correctly understood).

*Algebraic proof.*

$$\begin{aligned} \binom{n}{r-1} + \binom{n}{r} &= \frac{n! \cdot r}{(r-1)! \cdot r \cdot (n-r+1)!} + \frac{n! \cdot (n-r+1)}{r!(n-r)! \cdot (n-r+1)} \\ &= (\text{common denominator } r!(n-r+1)!) = \frac{n!(r + (n-r+1))}{r!(n-r+1)!} \\ &= \frac{n! \cdot (n+1)}{r!(n-r+1)!} = \frac{(n+1)!}{r!((n+1)-r)!} = \binom{n+1}{r}. \quad \square \end{aligned}$$

*Combinatorial proof.* The left hand side counts the number of  $r$ -element subsets in an  $(n+1)$ -element universe  $U$ . Let us pick a distinguished element  $* \in U$ , so that  $U' := U - \{*\}$  has  $n$  elements (*cf. our inductive proof of  $|\mathcal{P}(U)| = 2^{n+1}$* ):

$$U = \{ \underbrace{\cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot}_{n \text{ elements of } U} * \}$$

Then, an  $r$ -element subset  $S \subseteq U$  either does or does not contain  $*$ :

$$\begin{aligned} * \in S: & \quad \{ \underbrace{\cdot \odot \cdot \odot \cdot \odot \cdot \odot \cdot \odot \cdot \odot}_{(r-1) \text{ elements of } S} * \} \quad \text{the count is } C(n, r-1) \text{ (was } 2^n) \\ * \notin S: & \quad \{ \underbrace{\cdot \odot \cdot \odot \cdot \odot \cdot \odot \cdot \odot \cdot \odot}_{r \text{ elements of } S} * \} \quad \text{the count is } C(n, r) \text{ (was } 2^n) \end{aligned}$$

In the former case,  $S$  is described by the  $(r-1)$ -element subset  $S - \{*\}$  of the  $n$ -element set  $U - \{*\}$ , and the count is  $C(n, r-1)$ .

In the latter case,  $S$  is described by the  $r$ -element subset  $S$  of the same  $n$ -element set  $U - \{*\}$ , and the count is  $C(n, r)$ .

Since each subset is either one or the other, but never both, by the **Sum Rule** the total count is the sum  $C(n, r-1) + C(n, r)$ , *i.e.*, the right hand side of the identity.  $\square$

Selecting a point  
is a useful trick!  
We did this  
before!

**Remark 5.3.** If we set the *initial conditions*

$$C(n, 0) = C(n, n) = 1 \quad \text{for all integers } n \geq 0,$$

**Theorem 5.1** will let us compute all binomial coefficients *recursively*, using addition only (instead of a lot of multiplications). In fact, taking into account **Remark 5.2**, it suffices to set  $C(0, 0) = 1$ .

This computation can be organized in the shape of *Pascal's triangle*:

$$\begin{array}{rcl}
 n = 0: & & 1 \quad \leftarrow \text{the vertex is } (0, 0) \\
 n = 1: & & 1 \quad 1 \\
 n = 2: & & 1 \quad 2 \quad 1 \\
 n = 3: & 0 & 1 \quad 3 \quad 3 \quad 1 \\
 n = 4: & 1 & 4 \quad 6 \quad 4 \quad 1 \\
 n = 5: & 1 \quad 5 \quad 10 \quad 10 \quad 5 \quad 1 \\
 n = 6: & 1 \quad 6 \quad 15 \quad 20 \quad 15 \quad 6 \quad 1 \\
 n = 7: & 1 \quad 7 \quad 21 \quad 35 \quad 35 \quad 21 \quad 7 \quad 1 \\
 n = 8: & 1 \quad 8 \quad 28 \quad 56 \quad 70 \quad 56 \quad 28 \quad 8 \quad 1 \\
 r: & 0 \quad 1 \quad 2 \quad 3 \quad \cdots & \text{constant along slopes}
 \end{array}$$

*Algebraic proof of the Binomial Theorem 4.1.* We can use induction.

*Basic step.* The formula obviously holds for  $n = 0$ : we get  $1 = 1$ . *Just in case, you can also check  $n = 1$ :*

$$(x + y)^1 = 1 \cdot x + 1 \cdot y = \binom{1}{0} x^1 y^0 + \binom{1}{1} x^0 y^1. \quad \checkmark$$

*Inductive step.* Assume the formula for  $n = k$  and consider  $n = k + 1$ . The crucial ingredient is Pascal's identity:

$$\begin{aligned}
 (x + y)^{k+1} &= (x + y)(x + y)^k \stackrel{\text{IH}}{=} (x + y) \sum_{r=0}^k \binom{k}{r} x^{k-r} y^r \\
 &\quad \text{multiply out and collect equal powers of } y \\
 &= \sum_{s=0}^{k+1} \left( \binom{k}{s} + \binom{k}{s-1} \right) x^{k+1-s} y^s \\
 &\stackrel{\text{Pascal}}{=} \sum_{s=0}^{k+1} \binom{k+1}{s} x^{k+1-s} y^s \quad \square
 \end{aligned}$$

## 6. More combinatorial identities

**Theorem 6.1** (Vandermonde's identity). *For all integers  $m, n \geq 0$  and  $r$ , one has*

$$\binom{m+n}{r} = \sum_{k=0}^r \binom{m}{r-k} \binom{n}{k}.$$

**Remark 6.2.** With our conventions (see [Remark 5.2](#)), Pascal's identity is a special case ( $m = 1$ ) of [Theorem 6.1](#). Indeed,

$$\binom{1}{r-k} = \begin{cases} 1, & \text{if } k = r \text{ or } r-1, \\ 0, & \text{otherwise,} \end{cases}$$

and we have but two terms left. In fact, the proof is a direct generalization of our combinatorial proof of Pascal's identity.

*Combinatorial proof.* This time, we consider an  $(m+n)$ -element universe  $U$  and represent it as a disjoint union of an  $m$ -element set  $A$  (dots) and an  $n$ -element set  $B$  (stars):

$$U = \left\{ \underbrace{\cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot}_{m \text{ elements of } A} \underbrace{* * * * *}_{n \text{ elements of } B} \right\}$$

The left hand side of the identity counts the  $r$ -element subsets of  $U$ . Any such subset  $S$  has a certain number  $k$  of stars (*i.e.*,  $|S \cap B| = k$ ), and the remaining  $r - k$  elements are dots (*i.e.*,  $|S \cap A| = r - k$ ):

$$S \subseteq \left\{ \underbrace{\cdot \odot \odot \cdot \cdot \cdot \odot \cdot \cdot \cdot}_{r-k \text{ elements of } S} \underbrace{* * * \otimes * \otimes *}_{k \text{ elements of } S} \right\}$$

There are  $C(m, r-k)$  ways to choose the  $(r-k)$  out of  $m$  dots (the intersection  $S \cap A$ ) and, independently,  $C(n, k)$  ways to choose the  $k$  out of  $n$  stars (the intersection  $S \cap B$ ). By the [Product Rule](#), the total number of ways to choose an  $r$ -element subset *whose intersection with  $B$  has size  $k$*  is

$$C(m, r-k)C(n, k).$$

There remains to use the [Sum Rule](#) and sum up over all “reasonable” values of  $k$ : we must make sure that

$$0 \leq k \leq n \quad \text{and} \quad 0 \leq r-k \leq m,$$

*i.e.*, effectively  $k$  runs in the range

$$\max(0, r-m) \leq k \leq \min(r, n);$$

however, our convention will take care of that as all extra terms will just vanish as so will one of the two factors.  $\square$

**Remark 6.3.** I never tried to prove this statement algebraically. This may be quite a challenge, but you can give it a try!

*NB: your textbook insists that  $r \leq m$  and  $r \leq n$ . This is not necessary!*

*This is a very useful trick!*

**Corollary 6.4.** *For any integer  $n \geq 0$ , one has*

$$\binom{2n}{n} = \sum_{k=0}^n \binom{n}{k}^2.$$

*Proof.* This is Vandermonde's identity ([Theorem 6.1](#)) with  $r = m = n$ :

$$\binom{n+n}{n} = \sum_{k=0}^n \binom{n}{n-k} \binom{n}{k} = \sum_{k=0}^n \binom{n}{k}^2$$

(plus the symmetry of the binomial coefficients, [Corollary 3.7](#)).  $\square$

**Theorem 6.5.** For all integers  $0 \leq r \leq n$ , one has

$$\binom{n+1}{r+1} = \sum_{k=r}^n \binom{k}{r}.$$

*Combinatorial proof.* The left hand side counts the number of binary strings of length  $(n+1)$  with exactly  $(r+1)$  1's. Let us count these strings separately, according to the position  $k+1$  of the last 1.

Yet another useful trick!

$$\overbrace{? \ ? \ ? \ \dots \ ? \ ?}^{r \text{ 1's}} \underset{\substack{\uparrow \\ k \text{ positions}}}{k+1} 1 \overbrace{0 \ 0 \ \dots \ 0}^{\text{all 0's}}$$

Clearly,  $k$  takes values from  $r$  (as  $r$  more 1's should fit before position  $k+1$ ) to  $n$  and, for each fixed  $k$ , we have  $C(k, r)$  ways to select  $r$  out of  $k$  positions for the remaining  $r$  1's. Now, use the [Sum Rule](#).  $\square$

*Algebraic proof.* We iterate Pascal's identity ([Theorem 5.1](#)), each time expanding the last term (underlined) until it becomes zero (**red**); the **blue** terms stay:

$$\begin{aligned} \underline{\binom{n+1}{r+1}} &= \binom{n}{r} + \underline{\binom{n}{r+1}} = \binom{n}{r} + \binom{n-1}{r} + \underline{\binom{n-1}{r+1}} \\ &= \binom{n}{r} + \binom{n-1}{r} + \binom{n-2}{r} + \dots + \binom{r}{r} + \binom{r}{r+1} \quad \square \end{aligned}$$

The last proof is illustrated in Pascal's triangle:

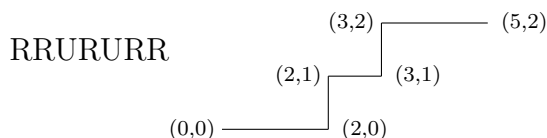
$$\begin{array}{cccccccc} & & & & 1 & & & \\ & & & 1 & & 1 & & \\ & & 1 & & 2 & & 1 & & 0 \\ & & & 1 & & 3 & & \underline{3} & & \underline{1} \\ & & 1 & & 4 & & \underline{6} & & \underline{4} & & 1 \\ & & & 1 & & 5 & & \underline{10} & & \underline{10} & & 5 & & 1 \\ & & 1 & & 6 & & \underline{15} & & \underline{20} & & 15 & & 6 & & 1 \\ & & & 1 & & 7 & & \underline{21} & & \underline{35} & & 35 & & 21 & & 7 & & 1 \\ & & 1 & & 8 & & 28 & & \underline{56} & & 70 & & 56 & & 28 & & 8 & & 1 \end{array}$$

## 7. Further applications

**Example 7.1.** A *lattice path* is a path in the  $xy$ -plane made up of a series of steps one unit to the **R**ight or one unit **U**p. (Going back to the left or down is not allowed.) What is the number of lattice paths connecting the origin  $(0,0)$  to the point  $(m,n)$ ,  $m, n \in \mathbb{N}$ ?

*Solution:* We need to make the total of  $(m+n)$  steps,  $m$  steps **R**ight and  $n$  steps **U**p. Thus, a path is **encoded** by a sequence of  $m$  R's and  $n$  U's. But we can as well replace  $R \mapsto 0$ ,  $U \mapsto 1$  and speak about bit strings of length  $(m+n)$  with exactly  $n$  1's. The number of these strings is  $C(m+n, n) = C(m+n, m)$ .

Here is an example of a lattice path and corresponding string.



Convenient  
encoding of the  
objects counted is  
crucial to most  
counting problems

## 8. Catalan's numbers

*Catalan's numbers* are  $C_n := \frac{1}{n+1} \binom{2n}{n}$ . They are all integers!

**Example 8.1.** Let us modify [Example 7.1](#) and count the number of lattice paths from  $(0, 0)$  to  $(n, n)$  *that stay below the diagonal  $y = x$ , i.e., at all times we have  $y \leq x$ .*

*Solution:* Arguing as in [Example 7.1](#), we conclude that our paths are encoded by strings of  $n$  R's and  $n$  U's such that, reading from left to right, at each moment *the number of U's does not exceed the number of R's* (as otherwise we would cross the diagonal). For example ( $n = 3$ ):

good: RRURUU,      bad: RURUUR

In the second string, at the **fifth step** we have 3 U's and 2 R's, with  $3 > 2$ . Thus, for small  $n$ , we have:

$n = 0$ :     $\emptyset$     1 path,  
 $n = 1$ :    RU    1 path,  
 $n = 2$ :    RRUU, RURU    2 paths,  
 $n = 3$ :    RURURU, RRUURU,  
             RURRUU, RRURUU, RRRUUU    5 path.

Before arriving at a closed formula, let us consider several closely related problems.

**Example 8.2.** What is the number of syntactically correct ways to parenthesize the product of  $(n + 1)$  factors? Here are examples:

$n = 0$ :     $a$     1 way,  
 $n = 1$ :     $(ab)$     1 way,  
 $n = 2$ :     $((ab)c), (a(bc))$     2 ways,  
 $n = 3$ :     $((a \cdot b) \cdot c) \cdot d, (((a(bc))d),$   
              $((ab)(cd)), (a((bc)d)), (a(b(cd)))$     5 ways.

*Solution:* You can observe a similarity with [Example 8.1](#). It does take a while to understand what “syntactically correct” means (*e.g.*, writing a parser for algebraic expressions or switching to the so-called *Polish postfix notation*), but, at the end of the day, a correct sequence of parentheses can be encoded by a sequence of **operations** “ $\cdot$ ” and **closing parentheses** “ $)$ ”, so that, at each time, the number of  $)$ 's does not exceed the number of  $\cdot$ 's. For example, the five ways for  $n = 3$  are encoded *via*

$\cdot\cdot\cdot\cdot\cdot), \quad \cdot\cdot\cdot\cdot\cdot), \quad \cdot\cdot\cdot\cdot\cdot), \quad \cdot\cdot\cdot\cdot\cdot), \quad \cdot\cdot\cdot\cdot\cdot).$

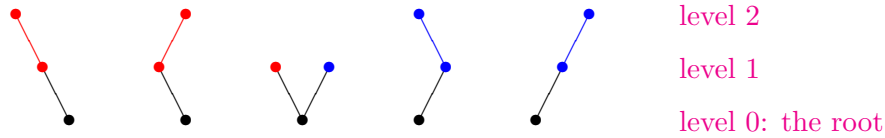
Now, it is clear that this problem is absolutely equivalent to [Example 8.1](#): just replace  $\cdot \mapsto R$  and  $) \mapsto U$ .

**Example 8.3.** What is the number of **oriented rooted binary** trees on  $n$  vertices? Here:

- **rooted** means that there is a distinguished vertex, called the *root*; the tree “grows” from the root upwards;
- **binary** means that, from each vertex, there are at most two outgoing (upward) branches (and there is one incoming one);

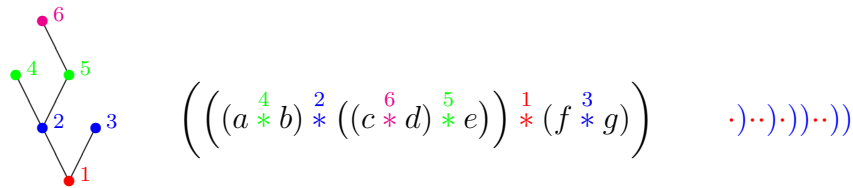
- **oriented** means that we distinguish between the left and right outgoing branches.

For example, here are the five trees on  $n = 3$  vertices:



*Solution:* As you may guess, we are going to establish a bijection between the set of trees on  $n$  vertices and the set in [Example 8.2](#), with  $(n + 1)$  factors and, hence,  $n$  operations. These  $n$  operations are the vertices of our tree; the left/right is the same as in the formula, and the “level” in the tree is the reversed order of execution: the operation executed last is the root, those (to the left and to the right) executed next to last are vertices of level 1, and so on:

We use two different encodings of the same set of objects. This trick is extremely important!

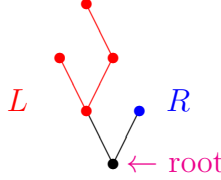


*Solutions.* Now, we are ready to solve all three problems. Let us count trees, and let us denote their number by  $t_n$ . We have

$$(8.4) \quad t_0 = 1, \quad t_1 = 1.$$

(Although questionable, we do accept the empty tree with no vertices. There obviously is a unique tree with one vertex.)

Given a tree  $T$  with  $(n+1)$  vertices, we can cut it at the root into the left “half”  $L$  and right “half”  $R$ :



Let  $L$  and  $R$  have  $p$  and  $q$  vertices, respectively, so that  $p \geq 0$ ,  $q \geq 0$ , and  $p + q = n$ . (One vertex—the root—has been removed!) Conversely, any pair  $L$ ,  $R$  can be “glued”, at their roots, into a single tree with  $p + q + 1$  vertices. Thus, by the **Product Rule**, the number of trees with  $(n+1)$  vertices and  $p$  vertices to the left from the root equals  $t_p t_{n-p}$ . Since  $p$  can vary from 0 to  $n$ , by the **Sum Rule**,

$$t_{n+1} = \sum_{p=0}^n t_p t_{n-p}.$$

Intuitively, it is clear that this *recurrence relation*, together with the initial data (8.4), determines the sequence:

$$\begin{aligned} t_1 &= t_0 t_0 = 1, \\ t_2 &= t_0 t_1 + t_1 t_0 = 2, \\ t_3 &= t_0 t_2 + t_1 t_1 + t_2 t_0 = 5, \quad \text{etc.} \end{aligned}$$

It is not easy to “solve” this relation; fortunately we know the answer:

**Theorem 8.5.** *Catalan’s numbers  $C_n$  satisfy the recurrence relation*

$$C_{n+1} = \sum_{p=0}^n C_p C_{n-p}.$$

We may prove this theorem later, when we discuss the so-called *generating functions*, which provide a convenient framework.

For now, taking **Theorem 8.5** for granted and observing that also

$$C_0 = C_1 = 1,$$

cf. (8.4), we see that  $t_n = C_n$  is the solution to all three problems!  $\square$

The first ten Catalan numbers are

$$1, 1, 2, 5, 14, 42, 132, 429, 1430, 4862, 16796.$$

They grow quite fast: asymptotically, as  $n \rightarrow \infty$ , we have  $C_n \approx 4^n$ .

## 9. Permutations with repetitions

We discuss a known subject under a different disguise.

**Example 9.1.** How many strings of length  $r$  can be formed from the 26 capital letters of the English alphabet?

*Solution:* This is a naked **Product Rule**: denoting by  $A$  the alphabet, strings in questions are elements of  $A^r$ , and their number is  $|A|^r = 26^r$ .

Another name for this problem is *permutations with repetitions*: we are speaking about  *$r$ -permutations* (or  $r$ -element arrangements) of the elements of a given  $n$ -element set  $A$  in which *repetitions are allowed*.

Another way to think about it is the following: we have a “bag”  $A$  with  $n$  distinct objects. We draw an object from the bag, record it, and put it back (unlike the case of ordinary permutations, where the objects drawn were removed), and we repeat this operation  $r$  times; then, at the end, we check our records, in which the *order is reflected* as well.

**Example 9.2.** Yet another way is to imagine a huge bag with objects of  $n$  distinct *kinds*, *unlimited supply* of each kind (cf. *combinations with repetitions* in §10 below):

$A, A, A, \dots, B, B, B, \dots, C, C, C, \dots, Z, Z, Z, \dots$

Then, we just draw  $r$  objects from the bag, *keeping track of the order*.

**Theorem 9.3** (the **Product Rule** = permutations with repetitions). *The number of  $r$ -permutations with repetitions of  $n$  distinct objects is*

$$n^r.$$

**Example 9.4.** How many strings of length **up to**  $r$  can be formed from an alphabet of length  $n$ ? (*E.g.*, identifiers in a very simple language.)

*Solution:* We throw in the **Sum Rule**:

$$\begin{aligned}
 \text{the number} &= n^0 \quad (\text{length } 0: \text{ the empty string}) \\
 &+ n^1 \quad (\text{length } 1) \\
 &+ n^2 \quad (\text{length } 2) \\
 &\quad \dots \dots \dots \\
 &+ n^i \quad (\text{length } i) \\
 &\quad \dots \dots \dots \\
 &+ n^r \quad (\text{length } r) \\
 \hline
 &= \frac{n^{r+1} - 1}{n - 1} \quad (\text{geometric progression}).
 \end{aligned}$$

## 10. Combinations with repetitions

Here is our motivating example.

**Example 10.1.** How many ways, **from the point of view of the restaurant**, are there to place an order for a party of 7 persons from the menu of 3 items: **B**urgers, **S**andwiches, and **C**hickens?

*Solution:* Of course, we assume that the restaurant has an **unlimited supply** of each kind of items (cf. *Permutations with repetitions* in §9). However, this time, **from the point of view of the restaurant**, the **order does not matter**: they only need to know the quantity of each item ordered! Thus, we are speaking about *combinations* rather than permutations, where still *repetitions are allowed*.

Compare with [Example 9.2](#): we have a huge bag with objects of 3 distinct *kinds*, **unlimited supply** of each kind:

BBB... S S S ... C C C ...;

we draw 7 objects from the bag, upon which we **forget of the order**.

As usual, the key is in encoding our selections in an appropriate way. The restaurant makes a selection and puts it on the shelf:

(10.2) BB S S S S C

The items are labeled as **B**urgers, **S**andwiches, and **C**hickens; however, to be on the safe side, let us also put separators | between different kinds:

BB|S S S S|C

But now, assuming that we **adopted a convention** that **B**urgers always go first, **S**andwiches go second, and **C**hickens go last, we can **erase the labels**, just remembering the quantities:

\* \* | \* \* \* \* | \*

Here, by our convention, the two (**unlabeled!**) items before the first bar **have** to be **B**urgers, the four in between, **S**andwiches, and the last one, a **C**hicken. Here are a few other examples of “recoding”:

\* \* \* \* | \* | \* \*   \* \* \* \* || \* \* \*   \* \* \* \* | \* \* \* |   || \* \* \* \* \* \* \*  
BBBB S CC   BBBB CCC   BBBB SSS   CCCCCC

Thus, the problem boils down to arranging 7 **unlabelled** objects \* and  $2 = 3 - 1$  separators |. In other words, we have a total of  $9 = 3 + 7 - 1$  positions, from which we need to select 7 for the \*’s (or complementary  $2 = 3 - 1$  for the |’s). And the answer is

$$C(3 + 7 - 1, 7) = C(3 + 7 - 1, 3 - 1) = 36.$$

Thus, we are speaking about *r-combinations with repetitions*, i.e., selections of *r* out of *n* **distinct** (kinds of) objects in which **repetitions allowed**.

Explain we the  
Division Rule does  
not work here! See  
Example 11.7

Since the **order**  
**does not matter**,  
we can choose our  
**favorite order!**  
This is a very neat  
trick!

**Theorem 10.3** (combinations with repetitions). *The number of  $r$ -combinations with repetitions of  $n$  distinct (kinds of) objects is*

$$C(n + r - 1, r) = C(n + r - 1, n - 1).$$

$r = \#(\text{of } * \text{'s});$   
 $n - 1 = \#(\text{of } | \text{'s})$

This result has many other disguises.

**Example 10.4.** What is the number of solutions to the equation

$$b + s + c = 7,$$

where  $b, s, c$  are nonnegative integers, i.e.,  $b, s, c \in \mathbb{N}$ ?

*Solution:* Back to [Example 10.1](#), let  $b, s, c$  be the numbers of **B**urgers, **S**andwiches, and **C**hickens, respectively. These are nonnegative integers that sum up to 7 (the total size of the order), i.e., they are precisely the natural solutions to our equation. On the other hand, these numbers uniquely describe the order (selection); in the learned language, we have a **bijection** between the two sets (the set of orders and that of solutions). For example, in (10.2) we have  $b = 2, s = 4, c = 1$ :

$$\text{BB SSSS C} = \text{BB} | \text{SSSS} | \text{C} = ** | **** | *$$

Hence, the number of solutions is

$$C(3 + 7 - 1, 7) = C(3 + 7 - 1, 3 - 1) = 36.$$

Here, 3 is the number of unknowns ( $b, s$ , and  $c$ ) in the equation!

**Theorem 10.5.** *The number of solutions to the equation*

$$x_1 + x_2 + \dots + x_n = r, \quad \text{where } x_i \in \mathbb{Z}, \quad x_i \geq 0,$$

$n = \#(\text{unknowns});$   
 $r = \text{RHS}$

*equals*

$$C(n + r - 1, r) = C(n + r - 1, n - 1).$$

**Example 10.6.** What is the number of solutions to the equation

$$x_1 + x_2 + x_3 = 20,$$

where  $x_1, x_2, x_3$  are integers and

$$x_1 > 0, \quad x_2 \geq 4, \quad x_3 \geq -2?$$

*Solution:* We reduce the problem to [Theorem 10.5](#). First, we make all inequalities non-strict, changing  $x_1 > 0$  to  $x_1 \geq 1$  (as  $x_1$  is an integer!). Then, we make a change of variables:

$$x_1 = y_1 + 1, \quad x_2 = y_2 + 4, \quad x_3 = y_3 - 2.$$

Make inequalities  
 $x_i \geq \text{smth}$

The RHS's of the  
 constraints

Substituting, we get  $(y_1 + 1) + (y_2 + 4) + (y_3 - 2) = 20$ , or

$$y_1 + y_2 + y_3 = 17 = 20 - 1 - 4 + 2, \quad y_i \in \mathbb{Z}, \quad y_i \geq 0.$$

Observe the signs!

Since the correspondence between the sets of  $x$ 's and  $y$ 's is one-to-one, by [Theorem 10.5](#) the number of solutions is

$$C(3 + 17 - 1, 3 - 1) = C(19, 2) = 171.$$

**Example 10.7.** Consider the following code fragment (the green part is related to Exercise 10.8):

```

k := 0
for i1 := 1 to n
  for i2 := 1 to i1 - 1
    ...
    for im := 1 to im-1 - 1
      k := k + 1  store (i1, i2, ..., im)

```

What is the value of  $k$  after execution?

*Solution:* We need to compute the number of times that the body of the innermost cycle is executed. **Mathematically**, we are speaking about the number of sequences  $(i_1, i_2, \dots, i_m)$ , where all  $i_s$  are integers subject to

$$1 \leq^{x_m} i_m \leq^{x_{m-1}} i_{m-1} \leq \dots \leq i_{s+1} \leq^{x_s} i_s \leq \dots \leq i_2 \leq^{x_1} i_1 \leq^{x_0} n.$$

Introduce new variables, viz. the “gaps” in the consecutive inequalities

$$\begin{aligned}
x_m &:= i_m - 1, \\
x_{m-1} &:= i_{m-1} - i_m, \\
&\dots\dots\dots \\
x_s &:= i_s - i_{s+1}, \\
&\dots\dots\dots \\
x_0 &:= n - i_1,
\end{aligned}$$

---


$$x_0 + x_1 + \dots + x_m = n - 1, \quad x_s \in \mathbb{Z}, \quad x_s \geq 0,$$

subject to an equation. Conversely, any solution to this equation gives us a sequence, viz.

$$i_s = n - x_0 - \dots - x_{s-1} \quad (\text{or } i_s = 1 + x_m + \dots + x_s).$$

By Theorem 10.5, the value of  $k$  = the number of sequences = the number of solutions is

$$C(m + n - 1, m) = C(m + n - 1, n - 1).$$

*Alternatively*, sequences as above are nothing but  $m$ -combinations from the  $n$ -element set  $\{1, \dots, n\}$  **with repetitions allowed**: a sequence is merely a combination written in its natural order. (Repetitions are allowed because the inequalities are  $\leq$  rather than  $<$ .) Then, directly by Theorem 10.3, their number is  $C(m + n - 1, m)$ .

*E.g.*, in the Burger/Sandwich/Chicken Example 10.1, letting  $B = 3$ ,  $S = 2$ ,  $C = 1$ , the selection BBSSSSC of (10.2) corresponds to the sequence  $(3, 3, 2, 2, 2, 2, 1)$ :

$$\text{top} = n = 3 \geq 3 \geq 3 \geq 2 \geq 2 \geq 2 \geq 1 \geq \text{bottom},$$

which is the *ordered* version of any of  $(3, 2, 2, 1, 3, 2, 2)$  or  $(1, 2, 3, 2, 3, 2, 2)$  etc.: we just put all 3’s first, all 2’s second, and all 1’s last!

**Exercise 10.8.** What is the number of sequences  $(i_1, i_2, \dots, i_m)$ , where all  $i_s$  are integers subject to

$$1 \leq i_m < i_{m-1} < \dots < i_s < \dots < i_1 \leq n.$$

Try to find two solutions in the spirit of Example 10.7. Comparing the two results explains most of this section!

We have  $m + 1$  unknowns, but the RHS is  $r = n - 1$

*Solution:* According to the *second* approach, the sequences in question are nothing but **ordinary** (**without** repetitions)  $m$ -combinations from the  $n$ -element set  $\{1, \dots, n\}$ : we merely **record each combination in its natural order**. Hence, the number is  $C(n, m)$ .

By the *first approach*, introducing the “gap” variables  $x_0, \dots, x_m$  as in [Example 10.7](#), we have

$$x_0 + \dots + x_m = n - 1, \quad x_i \in \mathbb{Z},$$

but this time

$$x_0 \geq 0, \quad x_1 > 0, \dots, x_{m-1} > 0, \quad x_m \geq 0.$$

Well, we know what to do, cf. [Example 10.6](#): let

$$x_0 = y_0, \quad x_s = y_s + 1 \quad \text{for } s = 1, \dots, m-1, \quad x_m = y_m.$$

Thus, we shift  $(m-1)$  variables by  $-1$ , arriving at

$$y_0 + \dots + y_m = n - m, \quad y_i \in \mathbb{Z}, \quad y_i \geq 0.$$

The number of solutions is given by [Theorem 10.5](#) as

$$C((m+1) + (n-m) - 1, (m+1) - 1) = C(n, m).$$

Ordering things that are originally unordered is a useful trick!

And this is how combinations are generated: see the “green” code in [Example 10.7](#)

This example explains how ordinary combinations account for those with repetitions: we just shift the variables by  $-1$ !

**Example 10.9** (digression). What is the number of ways to break a  $2n$ -element set into **unordered** collections of **unordered** pairs?

*Solution:* We use the ordering trick. Assuming the set  $A := \{1, \dots, 2n\}$ , order each pair  $(a_i, b_i)$  so that  $a_i < b_i$ , and then order the pairs by the increasing of their  $a_i$  part (smallest element):

$$a_1 < a_2 < \dots < a_n.$$

Then, select the pairs one by one according to this order. At each step  $i$ , **we have no choice for  $a_i$ :**

$$a_i = \min(A - \{a_1, b_1, a_2, b_2, \dots, a_{i-1}, b_{i-1}\})$$

has to be the smallest element left so far. Then,  $b_i$  is **any** element of the remaining set,

$$b_i \in (A - \{a_1, b_1, a_2, b_2, \dots, a_{i-1}, b_{i-1}, a_i\}),$$

and we have  $(2n - 2i + 1)$  choices. By the **Product Rule**,

$$\text{the number of ways} = (2n - 1) \cdot (2n - 3) \cdot \dots \cdot 3 \cdot 1 = (2n - 1)!!.$$

Here,  $m!!$  is the product of all integers from 1 to  $m$  **of the same parity**:

$$(2k)!! = 2 \cdot 4 \cdot \dots \cdot (2k - 2) \cdot 2k = 2^k k!,$$

$$(2k - 1)!! = 1 \cdot 3 \cdot \dots \cdot (2k - 3) \cdot (2k - 1) \frac{(2k)!!}{(2k)!!} = \frac{(2k)!}{2^k k!}.$$

**Exercise 10.10.** What is the number of ways to break a  $3n$ -element set into unordered collections of unordered triples? What about a  $kn$ -element set and unordered collections of unordered  $k$ -tuples?

**Example 10.11.** As a last example, what is the number of solutions to the *inequality*

$$x_1 + x_2 + \dots + x_n \leq r, \quad \text{where } x_i \in \mathbb{Z}, \quad x_i \geq 0?$$

We introduce a dummy unknown  $x_{n+1} := r - x_1 - \dots - x_n$  to make it an *equation*

$$x_1 + x_2 + \dots + x_n + x_{n+1} = r, \quad \text{where } x_i \in \mathbb{Z}, \quad x_i \geq 0.$$

The fact that also  $x_{n+1} \geq 0$  is precisely the meaning of the original inequality! Thus, the number of solutions is given by **Theorem 10.5** as

$$C(n + r, r) = C(n + r, n).$$

Homework!

Yet another common and useful trick!

## A brief summary

The results of several previous sections (combinations *vs.* permutations with or without repetitions) can be summarized as follows:

TABLE 1. Combinations and permutations of  $r$  out of  $n$  objects

In the example,  $r = 2$  and  $n = 3$ , with the sample set  $\{a, b, c\}$ .

| Order?       | w/out repetitions                                    | w/ repetitions                                   |
|--------------|------------------------------------------------------|--------------------------------------------------|
| permutations | $\frac{n!}{(n-r)!}$<br>ab ba ac ca bc ca<br>aa bb cc | $n^r$<br>ab ba ac ca bc ca<br>aa bb cc           |
| combinations | $\frac{n!}{r!(n-r)!}$<br>ab ac bc                    | $\frac{(n+r-1)!}{r!(n-1)!}$<br>aa ab ac bb bc cc |
|              | $C(n, r)$<br>the most important formula!             | $C(n+r-1, r)$<br>just remember the trick!        |

The binomial coefficients  $C(n, r)$  are used virtually everywhere! The formula at the bottom right corner can also be interpreted in a variety of different ways:

- *combinations with repetition*, see Theorem 10.3, with  $r$  the size of the selection and  $n$  the size of the universe;
- counting *solutions to the equation* in Theorem 10.5: then  $r$  is the right hand side and  $n$  is the number of the unknowns;
- counting *non-increasing sequences* as in Example 10.7: then,  $r$  is the length of the sequence and  $n$  is the upper bound;
- placing  $r$  *indistinguishable objects* to  $n$  *distinguishable boxes*, see §12.2 below.

## 11. Permutations with indistinguishable objects

**Example 11.1.** How many ways are there to permute the letters of the word

MISSISSIPPI?

Here is one example:

MISSISSIPPI.

I have permuted the first two S's. (Believe me I did!) But, alas, no one can see the difference, so probably we should not count this as a separate permutation!

*Solution:* The problem is that some of the letters are repeated. As usual, counting becomes much easier if everything is clearly distinguishable. So, let us label the letters:

$M_1 I_1 S_1 S_2 I_2 S_3 S_4 I_3 P_1 P_2 I_4.$

(There was no need to label the sole “M”, but, after all, why not?) Now, my second permutation *does* differ from the first one!

$M_1 I_1 S_2 S_1 I_2 S_3 S_4 I_3 P_1 P_2 I_4.$

Thus, we have  $1 + 4 + 4 + 2 = 11$  **distinct** objects, and the number of ways to permute them is  $11! = 39,916,800$ . Now, it's time to erase the labels. For example, with the rest fixed, we have  $4! = 24$  permutations that differ only by the position of the four I's:

$\dots I_1 \dots I_2 \dots I_3 \dots I_4 \dots$

When the indices are erased, they are no longer distinguishable; therefore, by the [Division Rule](#), we should divide by 24. Likewise, we should divide by  $4! = 24$  for the four S's, and by  $2! = 2$  for the two P's. (We can also divide by  $1! = 1$  for the one M.) Hence, at the end, the number of permutations is

$$\frac{11!}{1! \cdot 2! \cdot 4! \cdot 4!} = 34,650.$$

This is our  
favorite word! :)

*Alternative solution:* The formula resembles *combinations* rather than *permutations*, and it can be explained in terms of such. Altogether we have  $1 + 4 + 4 + 2$  positions. First, there are  $C(11, 1) = 11$  ways to choose 1 position for M. Then, there are  $C(10, 4)$  ways to choose four out of the *remaining 10* positions for the four I's. Then, there are  $C(6, 4)$  ways to choose four out of the remaining 6 positions for the S's, and the remaining two positions unavoidably (in  $C(2, 2) = 1$  way) belong to the P's. Hence, by the *Product Rule*, the total number of choices is

Most formulas can be explained in many different ways: typically, there are many ways to count the same set!

$$\begin{aligned} C(11, 1) \cdot C(10, 4) \cdot C(6, 4) \cdot C(2, 2) \\ = \frac{11!}{1! \cdot 10!} \cdot \frac{10!}{4! \cdot 6!} \cdot \frac{6!}{4! \cdot 2!} \cdot \frac{2!}{2! \cdot 0!} = \frac{11!}{1! \cdot 4! \cdot 4! \cdot 2!}. \end{aligned}$$

This approach generalizes to a theorem.

**Theorem 11.2.** *The number of permutations of  $n = n_1 + n_2 + \dots + n_k$  objects, of which  $n_1$  are of kind 1,  $n_2$  are of kind 2,  $\dots$ ,  $n_k$  are of kind  $k$ , equals*

$$C(n; n_1, n_2, \dots, n_k) = \binom{n}{n_1, n_2, \dots, n_k} := \frac{n!}{n_1! \cdot n_2! \cdot \dots \cdot n_k!}.$$

**Remark 11.3.** In the statement of *Theorem 11.2* and the notation used therein, it is **always assumed** that the  $n_i$ 's sum up to  $n$ . If necessary, we add a number of 1's (some objects are present in one copy only), cf.

$$\binom{11}{1, 4, 4, 2} = \frac{11!}{1! \cdot 4! \cdot 4! \cdot 2!}$$

in *Example 11.1*, where 1 accounts for the single M.

**Remark 11.4.** Note that here, unlike *Theorem 2.6*, we can count **full** permutations only! The reason is that we only solve those problems that we can! :) There just is no nice formula for the number of ( $r < n$ )-permutations out of  $n$  objects of which **not all are distinct**! Should you ever need to count them, you'll have to write them all down!

**Remark 11.5.** The notation resembles that of binomial coefficients (*aka combinations*), and, indeed,

$$C(m + n; m, n) = \binom{m + n}{m, n} = \binom{m + n}{m} = C(m + n, m)$$

in the old notation. (Like in some advanced programming languages, you can declare several functions with the same name, and the compiler will choose the right one according to the number and types of the actual parameters.) This is indeed the same number! Permutations of  $m + n$  objects of just **two** different kinds, say,  $m$  0's and  $n$  1's are nothing but combinations, cf. *Example 13.6* (bit strings of length  $m + n$  with exactly  $n$  1's). In a sense, the difference between permutations and combinations is purely psychological: it depends on the point of view!

**Remark 11.6.** The numbers

$$C(n; n_1, n_2, \dots, n_k) = \binom{n}{n_1, n_2, \dots, n_k}$$

in Theorem 11.2 are often called *multinomial coefficients*, as they do appear as coefficients in the so-called *multinomial formula*

$$(x_1 + \dots + x_k)^n = \sum_{n_1 + \dots + n_k = n} \binom{n}{n_1, n_2, \dots, n_k} x_1^{n_1} \dots x_k^{n_k}.$$

Accidentally, what is the number of terms in this formula? The proof is literally the same as that of the binomial formula (see Theorem 4.1). The formula is hardly useful in practice, but in theory it is good to know that the expansion looks like this.

**Example 11.7.** Now, we can explain why the Division Rule does not work in the Burger/Sandwich/Chicken Example 10.1: we cannot count the **permutations** with repetitions first (as in Theorem 9.3) and then divide by the overcount. The reason is that the overcount, which is given by Theorem 11.2, **depends** on the selection! Here are examples:

$$\text{BBS S S S C} : \quad C(7; 2, 4, 1) = 105 \quad \text{permutations,}$$

$$\text{BBBBCCC} : \quad C(7; 4, 0, 3) = 35 \quad \text{permutations,}$$

$$\text{CCCCCCC} : \quad C(7; 0, 0, 7) = 1 \quad \text{permutations.}$$

Note, accidentally, that you can add any number of 0's to the argument list on the right! Intuitively, this corresponds to increasing the number of “kinds” without adding any new objects to the pool (or adding zero objects of a new kind): clearly, this does not change the count!

It is given by  
Theorem 10.5 as  
 $C(n + k - 1, n)$

## 12. Combinatorist's favorite game

Our favorite game is distributing objects to boxes! :) The solution to this problem (and the number of extra constraints that we can throw in) depends dramatically on whether the objects and boxes in question are *distinguishable* (*labeled*) or not! Depending on the version, the problem may have a number of other interpretations!

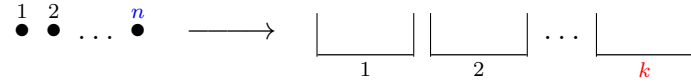
As a general rule, problems where the gadgets are *distinguishable* are much easier to solve!

Thus, we have  $n$  objects which we want to distribute into  $k$  boxes:



As usual, we are interested in the number of ways of doing that!

**12.1. Distinguishable objects to distinguishable boxes.** The easy case is that where all object and boxes are distinguishable (labelled, numbered, *etc.*):



Distributing such objects is the same as considering a function

$$\{1, \dots, n\} \rightarrow \{1, \dots, k\}, \quad i \mapsto \text{the box containing } \overset{i}{\bullet}$$

For example, this distribution of 5 objects into 3 boxes

$$(12.1) \quad \boxed{\overset{4}{\bullet}}_1 \boxed{\overset{3}{\bullet} \overset{5}{\bullet}}_2 \boxed{\overset{1}{\bullet} \overset{2}{\bullet}}_3$$

corresponds to the function

$$1 \mapsto 3, \quad 2 \mapsto 3, \quad 3 \mapsto 2, \quad 4 \mapsto 1, \quad 5 \mapsto 2.$$

We know the number of such functions: it is  $k^n$ . Refreshing the argument, each object may go to any of the  $k$  boxes, *i.e.*, in  $k$  different ways, and we need to repeat this procedure, independently,  $n$  times, once for each object. The answer is given by iterating the **Product Rule**:

$$\underbrace{k \cdot k \cdot \dots \cdot k}_{n \text{ factors}} = k^n.$$

For example, if you want to put 20 distinct books into 3 distinct shelves, you can do that in  $3^{20} = 3,486,784,401$  ways!

This problem is so easy that we can even add additional requirements. Let's say that

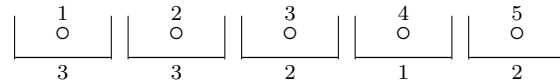
box 1 is to get  $n_1$  objects, ( $n_1$  copies of box 1)

box 2 is to get  $n_2$  objects, ( $n_2$  copies of box 2)

...

box  $k$  is to get  $n_k$  objects; ( $n_k$  copies of box  $k$ )

certainly, we assume that  $n_1 + n_2 + \dots + n_k = n$ . This question leads us to *permutations with indistinguishable objects*, see §11, but the things to be permuted are **boxes**, not objects! A way to think about this is that, instead of placing objects to boxes, we keep them intact (as placeholders) and “cover” them by “copies” of the boxes. For example, (12.1) will look like this:



The number of copies of each box is given by the constraints (green above), and the answer is given by **Theorem 11.2**:

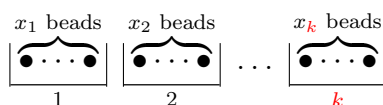
$$C(n; n_1, n_2, \dots, n_k) = \binom{n}{n_1, n_2, \dots, n_k} = \frac{n!}{n_1! \cdot n_2! \cdot \dots \cdot n_k!}.$$

**Example 12.2.** How many ways are there to distribute poker hands (5 cards each, out of the standard deck of 52 cards) to each of the four players?

*Solution:* We have 52 distinguishable objects (cards) and 4 individual boxes (players). However, things do not quite match: each box gets five objects, and there are  $32 = 52 - 5 - 5 - 5 - 5$  cards left undistributed. Well, we do the usual trick: introduce a dummy (box 5) who holds the remaining 32 cards. Thus, the answer is

$$\frac{52!}{5! \cdot 5! \cdot 5! \cdot 5! \cdot 32!} = 1,478,262,843,475,644,020,034,240$$

**12.2. Indistinguishable objects to distinguishable boxes.** This one is also pretty straightforward. We have  $k$  labelled cans to which  $n$  beads are to be placed. Since all beads are alike, the situation is completely described by the number  $x_i$  of beads that can  $i$  gets:



Since all  $n$  beads are to be distributed, we have

$$x_1 + x_2 + \dots + x_k = n,$$

and, of course, all  $x_i$ 's are natural number. Thus, by Theorem 10.5,

$$\text{the number of ways} = C(n + k - 1, n) = C(n + k - 1, k - 1).$$

(Be careful about the notation; it is impossible to keep track of the usage of letters like  $n$ ,  $k$ ,  $r$ , etc. throughout the whole lecture course. Here,  $k$  is the number of the unknowns and  $n$  is the right hand side!)

**12.3. Distinguishable objects to indistinguishable boxes.** This is a messy one! Here is an example: 4 employees are to be placed into 3 absolutely indistinguishable offices. For now, the best we can do is to list all possibilities. We do that according to the four *partitions* of 4 into up to 3 parts (see §12.5), which are

$$4 = 4 = 3 + 1 = 2 + 2 = 2 + 1 + 1;$$

each partition needs to be analyzed separately and has **its own “rule”** for counting the number of ways!

3 relabellings

|         |  |  |
|---------|--|--|
| 1,2,3,4 |  |  |
|---------|--|--|

$C(4, 4) = 1$

6 relabellings

|       |   |  |       |   |  |
|-------|---|--|-------|---|--|
| 1,2,3 | 4 |  | 1,2,4 | 3 |  |
| 1,3,4 | 2 |  | 2,3,4 | 1 |  |

$C(4, 3) = 4$

|     |     |  |     |     |  |     |     |  |
|-----|-----|--|-----|-----|--|-----|-----|--|
| 1,2 | 3,4 |  | 1,3 | 2,4 |  | 1,4 | 2,3 |  |
|-----|-----|--|-----|-----|--|-----|-----|--|

$3!! = 3$ , Ex. 10.9

|     |   |   |     |   |   |
|-----|---|---|-----|---|---|
| 1,2 | 3 | 4 | 1,3 | 2 | 4 |
| 1,4 | 2 | 3 | 2,3 | 1 | 4 |
| 2,4 | 1 | 3 | 3,4 | 1 | 2 |

$C(4, 2) = 6$

We see that altogether there are 14 ways, broken into several “groups”, some of which have an “official” count!

We cannot apply the **Division Rule** (label the offices first, drop the labels later) as the number of **relabellings** depends on the distribution! In fact, it depends on the number of offices left empty! Once the people are there, the **non-empty** offices have a “natural” order, *e.g.*, lexicographically:

$$(1, 2) < (3) < (4), \quad (1) < (2, 4) < (3), \quad (1, 4) < (2, 3).$$

But **we cannot tell between the empty ones!** *Cf.*

|                                                                                          |         |         |       |                                                                                          |       |         |   |                                                                                          |   |       |         |
|------------------------------------------------------------------------------------------|---------|---------|-------|------------------------------------------------------------------------------------------|-------|---------|---|------------------------------------------------------------------------------------------|---|-------|---------|
| <table border="1"><tr><td>1,2,3,4</td><td></td><td></td></tr></table><br>A      B      C | 1,2,3,4 |         |       | <table border="1"><tr><td></td><td>1,2,3,4</td><td></td></tr></table><br>A      B      C |       | 1,2,3,4 |   | <table border="1"><tr><td></td><td></td><td>1,2,3,4</td></tr></table><br>A      B      C |   |       | 1,2,3,4 |
| 1,2,3,4                                                                                  |         |         |       |                                                                                          |       |         |   |                                                                                          |   |       |         |
|                                                                                          | 1,2,3,4 |         |       |                                                                                          |       |         |   |                                                                                          |   |       |         |
|                                                                                          |         | 1,2,3,4 |       |                                                                                          |       |         |   |                                                                                          |   |       |         |
| vs.                                                                                      |         |         |       |                                                                                          |       |         |   |                                                                                          |   |       |         |
| <table border="1"><tr><td>1,2,4</td><td>3</td><td></td></tr></table><br>A      B      C  | 1,2,4   | 3       |       | <table border="1"><tr><td>1,2,4</td><td></td><td>3</td></tr></table><br>A      B      C  | 1,2,4 |         | 3 | <table border="1"><tr><td>3</td><td>1,2,4</td><td></td></tr></table><br>A      B      C  | 3 | 1,2,4 |         |
| 1,2,4                                                                                    | 3       |         |       |                                                                                          |       |         |   |                                                                                          |   |       |         |
| 1,2,4                                                                                    |         | 3       |       |                                                                                          |       |         |   |                                                                                          |   |       |         |
| 3                                                                                        | 1,2,4   |         |       |                                                                                          |       |         |   |                                                                                          |   |       |         |
| <table border="1"><tr><td>3</td><td></td><td>1,2,4</td></tr></table><br>A      B      C  | 3       |         | 1,2,4 | <table border="1"><tr><td></td><td>1,2,4</td><td>3</td></tr></table><br>A      B      C  |       | 1,2,4   | 3 | <table border="1"><tr><td></td><td>3</td><td>1,2,4</td></tr></table><br>A      B      C  |   | 3     | 1,2,4   |
| 3                                                                                        |         | 1,2,4   |       |                                                                                          |       |         |   |                                                                                          |   |       |         |
|                                                                                          | 1,2,4   | 3       |       |                                                                                          |       |         |   |                                                                                          |   |       |         |
|                                                                                          | 3       | 1,2,4   |       |                                                                                          |       |         |   |                                                                                          |   |       |         |

In general, for a partition like  $16 = 3 + 3 + 2 + 2 + 2 + 1 + 1 + 1 + 1$ , the count is going to be

$$\binom{16}{6} \cdot \frac{1}{2} \binom{6}{3} \cdot \binom{10}{6} \cdot (6-1)!! = 252,252,000,$$

*cf.* Example 10.9 and Exercise 10.10. Thus, if we have 16 employees and  $\geq 16$  offices, we can write something like this *for each of the 231 partitions of 16* and then sum up the results!

12.4. **Digression: the Stirling numbers.** In fact, there is a “formula” for the previous problem, but it is even uglier than the direct count.

The number of ways to distribute  $n$  distinguishable objects into  $k$  indistinguishable boxes so that exactly  $r$  boxes are left nonempty is given by the so-called *Stirling number of the second kind*

$$S(n, r) = \frac{1}{r!} \sum_{i=0}^{r-1} (-1)^i \binom{r}{i} (r-i)^n.$$

$1/r!$  here is given  
by the Division  
Rule: it works if  $r$   
is fixed!

Obviously, this does not really depend on  $k$ . In fact,  $r! \cdot S(n, r)$  is the number of **surjections**

$$\{n\text{-element set}\} \twoheadrightarrow \{r\text{-element set}\};$$

then, we divide it by  $P(r) = r!$  to drop the labels from the target. We **can use** the **Division Rule** here, but a new difficulty is to make sure that the function is a surjection! We will learn this formula when we do the principle of inclusion and exclusion.

Now, there remains to use the **Sum Rule**, summing up over all possible numbers  $1 \leq r \leq k$  of non-empty boxes:

$$\text{the count} = \sum_{r=1}^k S(n, r) = \sum_{r=1}^k \sum_{i=0}^{r-1} \frac{(-1)^i}{r!} \binom{r}{i} (r-i)^n.$$

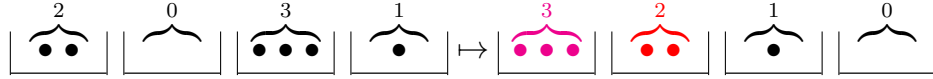
You can try to check if you really get 14 for  $n = 4$  and  $k = 3$ . :)

**12.5. Indistinguishable objects to indistinguishable boxes.** This one is completely intractable. It is related to the so-called *partitions of integers*; one can write *generating functions* and study them, but there is nothing like a “closed formula.”

We have to actually list all distributions by hands. This **can** be done if you organize your computation in a smart way (a sort of recursion).

**Example 12.3.** What is the number of ways to distribute 6 (indistinguishable) copies of the same book into 4 (indistinguishable) boxes?

*Solution:* Since our packings are **unordered**, we can order them ourselves, usually by decreasing:



Then, we list the packings *according to the maximal number that goes to one box*. For each such number, the rest is distributed to the remaining boxes in a similar way (**second maximal**, etc.):

- |                             |                                                     |
|-----------------------------|-----------------------------------------------------|
| $6 = 6$                     | • <b>max</b> = 6, nothing is left                   |
| $6 = 5 + 1$                 | • <b>max</b> = 5, one way for the one left          |
| $6 = 4 + 2$                 | • <b>max</b> = 4, two partitions of the 2 left      |
| $6 = 4 + 1 + 1$             |                                                     |
| $6 = 3 + 3$                 | • <b>max</b> = 3; three partitions of the 3 left    |
| $6 = 3 + 2 + 1$             |                                                     |
| $6 = 3 + 1 + 1 + 1$         |                                                     |
| $6 = 2 + 2 + 2$             | • <b>max</b> = 2; the rest is a partition of 4 with |
| $6 = 2 + 2 + 1 + 1$         | each term $\leq 2$ and at most three terms          |
| $6 = 2 + 1 + 1 + 1 + 1$     | • these do not work: too many parts                 |
| $6 = 1 + 1 + 1 + 1 + 1 + 1$ |                                                     |

Thus, there are **nine** ways to pack the books.

**Remark 12.4.** The *partitions* of 6 are (**unordered**) ways to represent this number as a sum

$$6 = n_1 + n_2 + \dots$$

of positive integers. Unlike [Theorem 10.5](#), the number of summands is not fixed. On the other hand, in **unordered partitions**, we can assume the terms ordered:

$$n_1 \geq n_2 \geq n_3 \geq \dots$$

In our particular packing problem, we have an extra constraint: the number of *parts* must be at most four. As mentioned above, one can try to write a generating function, but no “closed formula” is known.

### 13. Recurrence relations

**Example 13.1** (Fibonacci, *Liber Abaci*, 1202). A young couple of rabbits is placed on an uninhibited island. We assume that:

- (1) rabbits never die (ha-ha);
- (2) a couple does not mate until it is two months old (16+);
- (3) after two months, a couple produces a new couple every month.

How many couples are there on the island after  $n$  months?

*Solution:* Let us denote the number in question  $f_n$  (known as the  $n$ -th *Fibonacci number*), and let us try to model the situation:

$$\begin{array}{lcl}
 f_1 = 1: & \begin{array}{c} 1 \\ \bullet \\ 0 \end{array} & \\
 f_2 = 1: & \begin{array}{c} 1 \\ \bullet \end{array} & \\
 f_3 = 2: & \begin{array}{cc} 1 & 2 \\ \bullet & \bullet \\ & 1 \end{array} & \\
 f_4 = 3: & \begin{array}{ccc} 1 & 2 & 3 \\ \bullet & \bullet & \bullet \\ & 1 & \end{array} & \\
 f_5 = 5: & \begin{array}{ccccc} 1 & 2 & 3 & 4 & 5 \\ \bullet & \bullet & \bullet & \bullet & \bullet \\ & 1 & 2 & \end{array} & \\
 f_6 = 8: & \begin{array}{cccccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ \bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet \\ & 1 & 2 & 3 & \end{array} & \\
 f_7 = 13: & \begin{array}{ccccccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 \\ \bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet \\ & 1 & 2 & 3 & 4 & 5 & \end{array} & 
 \end{array}$$

Now, it is clear what is going on: the population  $f_n$  on month  $n$  is

$$\begin{aligned}
 f_n &= f_{n-1} \quad (\text{all "old" ones: rabbits never die}) \\
 &+ f_{n-2} \quad (\text{offsprings of those at least 2 months old}).
 \end{aligned}$$

And it appears that this is the best we can do: we cannot find  $f_n$  unless we know  $f_{n-1}$  and  $f_{n-2}$ . However, since we also know  $f_1 = f_2 = 1$ , given time and patience, we can compute all other ones one-by-one, *recursively* (a sort of our favorite *induction* ladder):

$$\begin{aligned}
 f_3 &= f_2 + f_1 = 1 + 1 = 2 \quad (f_1, f_2 \text{ are known in advance}), \\
 f_4 &= f_3 + f_2 = 2 + 1 = 3 \quad (f_3 \text{ has just been computed}), \\
 f_5 &= f_4 + f_3 = 3 + 2 = 5 \quad (f_4 \text{ has just been computed}), \\
 f_6 &= f_5 + f_4 = 5 + 3 = 8 \quad (f_5 \text{ has just been computed}), \\
 f_7 &= f_6 + f_5 = 8 + 5 = 13 \quad (f_6 \text{ has just been computed}), \text{ etc.}
 \end{aligned}$$

Thus, for the moment, the best we can do is stating that

$$(13.2) \quad f_1 = f_2 = 1, \quad \text{and} \quad f_n = f_{n-1} + f_{n-2} \quad \text{for } n \geq 3.$$

Here, the first part  $f_1 = f_2 = 1$  is called the *initial data* (the basic step of induction), and the expression  $f_n = f_{n-1} + f_{n-2}$  of  $f_n$  in terms of several **previous** terms of the sequence is called a *recurrence relation* (the inductive step). **Both parts are important:** a recurrence relation without initial data makes no sense! (like missing basic step)

*NB:* Induction can be thought of as a recursive computation of the truth value with very special "recurrence relation"  
 $f_{n-1} \Rightarrow f_n$   
 linear homogeneous of degree 2

This computation appears quite boring. Can we come up with a “closed formula”? Yes, we can! (next time?), and the formula is:

$$(13.3) \quad f_n = \frac{1}{\sqrt{5}} \left[ \left( \frac{1+\sqrt{5}}{2} \right)^n - \left( \frac{1-\sqrt{5}}{2} \right)^n \right].$$

This expression definitely deserves a few remarks.

*First*, there obviously is no way to come up with something like (13.3) by actually *counting* things one-by-one; *it is not even immediately obvious that  $f_n$  given by (13.3) is an integer!* Thus, **we need a sort of theory!**

*Second*, the computation by (13.3) is hardly easier than that by (13.2). Thus, **“closed formulas” don’t solve all problems.**

*Third*, some properties of  $\{f_n\}$  can be derived from (13.3). For example, observe that  $|(1 - \sqrt{5})/2| \approx 0.618 < 1$  and, hence, for each  $n \geq 0$ , the second term in (13.3) is smaller than  $1/\sqrt{5} \approx 0.447 < 1/2$  (in absolute value). It follows that, essentially,  $f_n$  grow exponentially:

$$f_n = \text{the integer closest to } \left[ \frac{1}{\sqrt{5}} \left( \frac{1+\sqrt{5}}{2} \right)^n \right].$$

However, some other properties (*e.g.*, arithmetical, which  $f_n$  have a lot!) are much easier derived directly from (13.2). Below is an example.

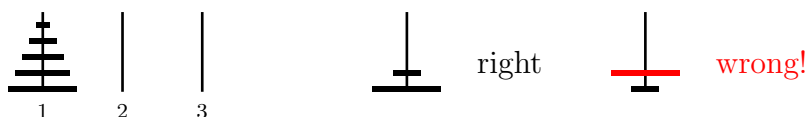
**Exercise 13.4.** Prove that any two consecutive Fibonacci numbers  $f_n, f_{n+1}$  are coprime, *i.e.*,  $\text{g.c.d.}(f_n, f_{n+1}) = 1$ . What about  $\text{g.c.d.}(f_n, f_{n+2})$ ? Or  $\text{g.c.d.}(f_n, f_{n+3})$ ? Use (13.2). I can hardly think how this can be done by (13.3)!

As a homework, try to prove this using the binomial formula. The devil is in the signs!

NB: very good for midterms!

There even is a mathematical journal dedicated solely to Fibonacci numbers!

**Example 13.5** (The Tower of Hanoi). Here is a puzzle that used to be popular. We have a board with three poles, and  $n$  disks, of pairwise distinct sizes, on one of the poles:



The objective of the game is moving all disks from pole 1 to pole 3 observing the following rules:

- (1) only one disk can be moved (transferred from one pole to another) at a time;
- (2) a larger disk cannot be placed on top of a smaller one.

How many moves does it take to solve the puzzle with  $n$  disks?

*Solution:* Denoting the number by  $H_n$ , I claim that  $H_n = 2H_{n-1} + 1$ . Indeed, here is what we do:



It is crucial that, playing the puzzle with  $(n-1)$  disks, we can forget about **the last one**: it is the **largest**, so it creates no obstruction! (Anything can be placed on top of it.) **A true mathematician would also ask for a proof that fewer moves would not do, but we will skip this part.**

Thus, again, we obtain a **recurrence relation** with obvious **initial data** (one move is enough for one disk):

$$H_1 = 1, \quad \text{and} \quad H_n = 2H_{n-1} + 1 \quad \text{for } n \geq 2.$$

This one can easily be “solved” by hands:.

$$\begin{aligned} H_n &= 2H_{n-1} + 1 \\ &= 2(2H_{n-2} + 1) + 1 = 4H_{n-2} + 2 + 1 \\ &= 4(2H_{n-3} + 1) + 2 + 1 = 8H_{n-3} + 4 + 2 + 1 \\ &\quad \dots\dots\dots \\ &= 2^{n-1} \cdot H_1 + 2^{n-2} + \dots + 2 + 1 = 2^n - 1. \end{aligned}$$

Once this has been guessed, **it must be proved!** Here, it can easily be done by induction:

**Basic step:**  $H_1 = 1 = 2^1 - 1$  is given by the **initial data!** ✓

**Inductive step:** assuming  $H_k = 2^k - 1$ , we have, by the **recurrence relation**,

$$H_{k+1} \stackrel{\text{RR}}{=} 2H_k + 1 \stackrel{\text{IH}}{=} 2(2^k - 1) + 1 = 2^{k+1} - 1. \quad \checkmark$$

Certainly, the same applies to (13.2): once you’ve managed to guess (13.3), it is relatively easy to prove it by (strong) induction.

Someone is playing this game with 64 disks, and the world will end upon completion. How much time do we have left?

linear nonhomogeneous of degree 1

Thus,  $n = 64$  would require  $H_{64} = 2^{64} - 1 = 18,446,744,073,709,551,615$  moves—the famous *chess number*

Yet another illustration of the relation between the two!

**Example 13.6** (more down to earth: counting bit strings). What is the number  $a_n$  of bit strings of length  $n$  that **do not contain two consecutive 0's**? That is, a substring "00" is forbidden?

01101110 good,      011**00**111 bad.

*Solution:* Normally, bit strings can easily be constructed and counted recursively: to obtain a bit string of length  $n$ , we can take a bit string  $S$  of length  $(n - 1)$  and append 1 or 0, thus doubling the number:

$$\underbrace{??? \dots ??}_{n-1} 1, \\ \underbrace{??? \dots ??}_{n-1} 0.$$

In our problem, we can freely append 1, but we should be careful when appending 0: if  $S$  ends in 0, the result will be illegal, ending in 00:

$$\underbrace{??? \dots ?0}_{n-1} 0.$$

Therefore, if we are planning to append 0, we must make sure that  $S$  **ends in 1**, i.e., is itself obtained by appending 1 to a bit string  $S'$  of length  $(n - 2)$ :

$$\underbrace{??? \dots ??}_{n-1} 1 \quad (a_{n-1} \text{ strings}), \\ \underbrace{??? \dots ?}_{n-2} 10 \quad (a_{n-2} \text{ strings}).$$

(Of course, we should also assume that  $S$  and  $S'$  themselves are legal strings, so that their count is given by  $a_{n-1}$  and  $a_{n-2}$ , respectively.)

At the end, we arrive at the same *recurrence relation* (13.2) as for *Fibonacci numbers*:

$$a_n = a_{n-1} + a_{n-2}.$$

The *initial conditions* are different:

$$a_0 = 1 \quad (" " \text{ only}), \quad a_1 = 2 \quad ("0" \text{ and } "1" \text{ are both valid}).$$

Still, the solution looks very similar to (13.3).

**Exercise 13.7.** Explain that  $a_n = f_{n+2}$  and, hence,  $a_n$  is given by (13.3) with  $(n + 2)$  substituted instead of  $n$ .

linear  
homogeneous of  
degree 2

Homework!

**Example 13.8** (yet another string count). A decimal string is considered a *valid codeword* if it contains an *even number of 0's*: *e.g.*, 100 is valid but 90 is not (although 090 is still valid!) What is the number  $c_n$  of valid codewords of length  $n$ ?

*Solution:* As in the previous example, we can construct decimal strings recursively, by appending a digit (0 to 9) to a string of length  $(n - 1)$ . Again, we should be careful:

$$\underbrace{??? \dots ?}_{\text{valid}} d \quad (c_{n-1} \text{ strings for each } d = 1, \dots, 9) \times 9,$$

$$\underbrace{??? \dots ?}_{\text{invalid}} 0 \quad (\text{the } 10^{n-1} - c_{n-1} \text{ invalid strings}).$$

(As usual, *invalid* is everything that is not *valid*, so the number of *invalid* strings of length  $(n - 1)$  is  $10^{n-1} - c_{n-1}$  by the *Subtraction Rule*.) Thus, we get a *recurrence relation*

$$c_n = 9c_{n-1} + (10^{n-1} - c_{n-1}) = 8c_{n-1} + 10^{n-1}$$

with *initial data*

$$c_0 = 1 \quad (\text{the only string "" of length 0 is valid}).$$

We will see that the solution is

$$c_n = \frac{1}{2}(8^n + 10^n).$$

**Example 13.9** (Catalan's numbers). An example of a *nonlinear* recurrence relation is

$$C_n = \sum_{p=0}^{n-1} C_p C_{n-p-1}, \quad C_0 = 1,$$

*cf.* §8. This will **not** be covered by our theory: one can only **guess** that it is solved by Catalan's numbers and try to **prove** this guess by other means (which is not immediately obvious, either).

linear  
nonhomogeneous  
of degree 1

## 14. Linear homogeneous recurrence relations

A *linear homogeneous* recurrence relation of degree  $d$  with constant coefficients is a recurrence relation of the form

$$(14.1) \quad a_n = c_1 a_{n-1} + c_2 a_{n-2} + \dots + c_d a_{n-d}.$$

Here,

- $a_n$  is the sequence to be determined; usually, we assume  $n \geq 0$ ;
- the *degree*  $d$  is the number of previous terms,  $a_{n-1}$  down to  $a_{n-d}$ , used to compute  $a_n$ :

$$a_n = a_{n-1} - a_{n-2} - a_{n-3} \quad \text{is a relation of degree } 3;$$

- *linear* means, roughly, that the terms  $a_n$  are never multiplied by one another:

$$a_n = a_{n-1} + a_{n-2} + 1: \quad \text{right,}$$

$$a_n = a_{n-1} \cdot a_{n-2} \quad \text{or} \quad a_n = a_{n-1}^2: \quad \text{wrong!}$$

in other words, all “terms” of the relation are of degree at most one in the  $a_i$ ’s;

- *homogeneous* means that there is no “free term” of degree 0, *i.e.*, all terms are of degree **exactly one**:

$$a_n = a_{n-1} - a_{n-2}: \quad \text{right,}$$

$$a_n = a_{n-1} + 1 \quad \text{or} \quad a_n = a_{n-1} + n: \quad \text{wrong!}$$

- *with constant coefficients* means that the **coefficients**  $c_i$  in (14.1) are constant, *i.e.*, do not depend on  $n$ :

$$a_n = 3a_{n-1} - 3a_{n-2}: \quad \text{right,}$$

$$a_n = na_{n-1}: \quad \text{wrong! } (c_1 = n)$$

Common sense suggests that, in order to solve a relation (14.1) of degree  $d$ , we need  $d$  pieces of *initial data*

$$a_0 = \text{value}_0, \quad a_1 = \text{value}_1, \quad \dots, \quad a_{d-1} = \text{value}_{d-1};$$

then, from (14.1),

$$a_d = c_1 a_{d-1} + c_2 a_{d-2} + \dots + c_d a_0,$$

$$a_{d+1} = c_1 a_d + c_2 a_{d-1} + \dots + c_d a_1,$$

$$a_{d+2} = c_1 a_{d+1} + c_2 a_d + \dots + c_d a_2, \text{ etc.}$$

For example,

$$a_0 = 1, \quad a_n = na_{n-1} \quad \text{has the solution } a_n = n!,$$

$$a_0 = 0, \quad a_n = a_{n-1} + 1 \quad \text{has the solution } a_n = n,$$

$$a_0 = 0, \quad a_n = a_{n-1} + n \quad \text{has the solution } a_n = n(n+1)/2.$$

In other words,

$$(14.2) \quad \text{the solution to (14.1) depends on } d \text{ arbitrary parameters.}$$

Explain!

In linear algebra, we would say that the dimension of the solution space of (14.1) is  $d$

**14.1. The linearity concept.** This is one of the most important ideas in mathematics. In a nutshell, we know almost everything about linear problems, whereas we know almost nothing about non-linear ones. For this reason, usually we try to *linearize* the problem at hand; if the solution works, we are happy; if it does not, we throw in “higher order terms” and try to cope with them.

In a sense, half of Calculus is just about that: we replace a complicated non-linear function  $f(x)$  with its *best linear approximation*

This is a digression

$$f(x) \approx f(x_0) + f'(x_0)(x - x_0)$$

and see what we can get out of this. (Note that  $x_0 = \text{const}$  and, hence, also  $f(x_0) = \text{const}$  and  $f'(x_0) = \text{const}$ , so the expression is indeed linear in the variable  $x$ .) Sometimes we have to add the second, third, *etc.* order terms of the *Taylor approximation*

$$f(x) \approx f(x_0) + f'(x_0)(x - x_0) + \frac{1}{2}f''(x_0)(x - x_0)^2 + \dots$$

For example, we do this in the *second derivative test*.

In the realm of *recurrence relations*, the linearity manifests itself in the form of the following theorem.

**Theorem 14.3.** If  $a_n$  and  $b_n$  are solutions to a **linear homogeneous** recurrence relation (14.1), then so is  $x_n := pa_n + qb_n$  for any  $p, q \in \mathbb{R}$ .

*Proof.* We do not need constant coefficients here!

This is how linearity works!

$$\begin{aligned} x_n &= pa_n + qb_n \\ &= (c_1a_{n-1} + c_2a_{n-2} + \dots + c_da_{n-d})p \\ &\quad + (c_1b_{n-1} + c_2b_{n-2} + \dots + c_db_{n-d})q \\ &= c_1x_{n-1} + c_2x_{n-2} + \dots + c_dx_{n-d}. \quad \square \end{aligned}$$

In view of (14.2), it appears that it should suffice to find  $d$  sufficiently different solutions  $x_n, y_n, \dots, z_n$ ; then, we may hope to find **any** solution in the form of a *linear combination*

This is called the general solution

$$a_n = Xx_n + Yy_n + \dots + Zz_n, \quad X, Y, \dots, Z \in \mathbb{R},$$

**which is also a solution!** How different? We want to be able to serve any collection of  $d$  pieces of *initial data*, *i.e.*, solve the linear system

linearly independent in linear algebra  
Unknowns are  $X, Y, Z$ . The rest are given numbers!

$$(14.4) \quad \begin{cases} Xx_0 + Yy_0 + \dots + Zz_0 = a_0, \\ Xx_1 + Yy_1 + \dots + Zz_1 = a_1, \\ \dots \\ Xx_{d-1} + Yy_{d-1} + \dots + Zz_{d-1} = a_{d-1} \end{cases}$$

of  $d$  equations with  $d$  unknowns  $X, Y, \dots, Z$ . (Once  $x_n, y_n, \dots, z_n$  are known, here  $a_0, \dots, a_{d-1}$  will be **known numbers**!) Do not be scared: in practice, it is much easier than it seems!

**Remark 14.5.** This all is very similar to *linear homogeneous differential equations of degree  $d$  with constant coefficients*; even the terminology is the same! Recurrence relations are merely a discrete counterpart thereof!

If you took differential equation, this stuff should be easy!

14.2. **Recurrence relations of degree 1.** We deal with a recurrence relation

$$a_n = ca_{n-1} \quad (\text{let us assume that } c := c_1 \neq 0)$$

and a single piece of initial data

$$a_0 = \text{value}.$$

Let us try something simple, well known, *e.g.*, a *geometric progression*  $x_n = r^n$ ,  $r \neq 0$ . Substituting, we get

$$r^n = cr^{n-1}, \quad \text{or} \quad r = c.$$

Thus,  $x_n = c^n$  **is a solution!** On the other hand, (14.4) boils down to a single equation

$$X = a_0,$$

which certainly can be solved (in fact, already is solved) for any right hand side  $a_0$ . (Note that  $x_0 = c^0 = 1$ .) Thus, the complete solution to our problem (*recurrence relation* and *initial data*) is

$$a_n = a_0 c^n.$$

14.3. **Recurrence relations of degree 2.** Now, we try to consider a recurrence relation

$$a_n = c_1 a_{n-1} + c_2 a_{n-2} \quad (\text{it is wise to assume that } c_2 \neq 0. \text{ Why?})$$

with **two pieces** of initial data

$$a_0 = \text{value}_0, \quad a_1 = \text{value}_1.$$

We need to find **two** (independent) solutions  $x_n$ ,  $y_n$ , and (14.4) would boil down to

Two unknowns  
 $X, Y$ ! The rest is  
known by now!

$$\begin{cases} Xx_0 \cdot x_1 + Yy_0 \cdot x_1 = a_0 \cdot x_1, \\ Xx_1 \cdot x_0 + Yy_1 \cdot x_0 = a_1 \cdot x_0. \end{cases}$$

From high school (??), this system has a solution **for any pair**  $a_0, a_1$  of the right hand sides if and only if

$$(14.6) \quad \begin{vmatrix} x_0 & x_1 \\ y_0 & y_1 \end{vmatrix} = x_0 y_1 - x_1 y_0 \neq 0.$$

Let us push our luck and see if we can still find  $x_n$  (and  $y_n$ ) in the form of a *geometric progression*  $x_n = r^n$ ,  $r \neq 0$ . We have

$$r^n = c_1 r^{n-1} + c_2 r^{n-2},$$

or

$$r^2 = c_1 r + c_2.$$

This **quadratic equation** is called the *characteristic equation* of the recurrence relation in question. Now, it appears that we need to consider three cases, **according to how many roots** (two, one, or none) the characteristic equation has. (The last case is an illusion, but let us stick to the Book.)

To solve, we'll  
need to **divide** by  
this!

This is the  
discrete  
counterpart of the  
exponential  
function  $y = e^{\lambda x}$   
solving linear  
differential  
equations

14.4. **Case 1: two distinct real roots.** Assume that the **characteristic equation** has **two distinct real roots**  $r \neq s$ . Then, we get **two solutions**  $x_n = r^n$  and  $y_n = s^n$ , and (14.6) becomes

$$r^0 \cdot s^1 - r^1 \cdot s^0 = s - r \neq 0,$$

which certainly is true (as  $r \neq s$ ). Thus, **we have found two independent solutions**, and the problem is solved!

**Remark 14.7.** Note that we could as well have started with **any other pair of initial data**

$$a_m = \text{value}_m, \quad a_{m+1} = \text{value}_{m+1}.$$

Indeed, (14.6) becomes

$$r^m s^{m+1} - r^{m+1} s^m = r^m s^m (s - r) \neq 0,$$

which is true since also  $r, s \neq 0$ . (Why?)

**Example 14.8.** Solve the recurrence relation

$$a_0 = 1, \quad a_1 = 3, \quad a_n = 3a_{n-1} - 2a_{n-2} \quad \text{for } n \geq 2.$$

*Solution:* The characteristic equation  $r^2 = 3r - 2$  has two distinct real roots  $r = 1$  and  $s = 2$ . Therefore, we should be able to find a solution in the form (here  $x_n = 1^n$  and  $y_n = 2^n$ )

$$a_n = X \cdot 1^n + Y \cdot 2^n = X + Y \cdot 2^n.$$

Substituting  $n = 0$  or  $1$ , we get the system

$$\begin{cases} X + Y = 1 = a_0, \\ X + 2Y = 3 = a_1, \end{cases}$$

which is easily solved:  $X = -1$ ,  $Y = 2$ . Hence,

$$a_n = -1 + 2 \cdot 2^n = 2^{n+1} - 1 \quad (\text{a slight simplification}).$$

**Example 14.9** (the Fibonacci sequence). Let us work out the *Fibonacci numbers*, i.e., solve the recurrence relation

$$a_1 = a_2 = 1, \quad a_n = a_{n-1} + a_{n-2} \quad \text{for } n \geq 3.$$

We can do it directly as stated, but, as a *slight* simplification, we can change the initial data to

$$a_0 = 0, \quad a_1 = 1;$$

then,  $a_2 = a_1 + a_0 = 1 + 0 = 1$  comes out right. The characteristic equation  $r^2 = r + 1$  has two distinct real roots; following Dan Brown, let us denote them

$$\varphi := \frac{1 + \sqrt{5}}{2}, \quad \psi := \frac{1 - \sqrt{5}}{2}.$$

(In fact,  $\psi = -1/\varphi$  by Vieta's theorem.) Hence, the *general solution* is of the form  $a_n = X\varphi^n + Y\psi^n$ , and  $X, Y$  are found from the system

$$\begin{cases} X + Y = 0 = a_0, \\ X\varphi + Y\psi = 1 = a_1. \end{cases}$$

From the first equation,  $Y = -X$ , whereupon the second one becomes  $X(\varphi - \psi) = 1$ , or  $X\sqrt{5} = 1$ , or  $X = 1/\sqrt{5}$ , which gives us (13.3).

With the original initial data, we would have to solve

$$\begin{cases} X\varphi + Y\psi = 1 = a_1, \\ X\varphi^2 + Y\psi^2 = 1 = a_2, \end{cases}$$

which is a bit more challenging, but still manageable.

We can also solve the bit string counting [Example 13.6](#), which differs from Fibonacci only by the initial data

$$a_0 = 1, \quad a_1 = 2.$$

The system for  $X, Y$  becomes

$$\begin{cases} X + Y = 1 = a_0, \\ X\varphi + Y\psi = 2 = a_1, \end{cases}$$

which gives us

$$\begin{aligned} X &= \frac{2 - \psi}{\varphi - \psi} = \frac{1}{\sqrt{5}} \frac{\sqrt{5} + 3}{2} = \frac{\varphi^2}{\sqrt{5}}, \\ Y &= \frac{\varphi - 2}{\varphi - \psi} = \frac{1}{\sqrt{5}} \frac{\sqrt{5} - 3}{2} = \frac{-\psi^2}{\sqrt{5}}, \end{aligned}$$

i.e., the *Fibonacci numbers* with the index shifted by two. With this set of initial data, the computation with the radicals is a bit boring and the final “simplification” requires a good guess of what you are trying to achieve...

14.5. **Case 2: one real root.** Assume that the characteristic equation has one root  $r$  only. Recall that this means that

$$x^2 - c_1x - c_2 = (x - r)^2 = x^2 - 2rx + r^2,$$

i.e., the original recurrence relation has the form

$$(14.10) \quad a_n = 2ra_{n-1} - r^2a_{n-2}.$$

We have one solution  $x_n = r^n$ , but we need two! Another lucky guess is that

$$x_n = r^n \quad \text{and} \quad y_n = nr^n$$

**is a pair of independent solutions!** Why solutions? We know this for  $x_n$ , and here is a check for  $y_n$ :

$$\begin{aligned} 2ry_{n-1} - r^2y_{n-2} &= 2r(n-1)r^{n-1} - r^2(n-2)r^{n-2} \\ &= [2(n-1) - (n-2)]r^n \\ &= nr^n \\ &= y_n. \end{aligned}$$

Now, this is **the rule!**  
Just like  $y = xe^{\lambda x}$  in differential equations!

Note that we did use the special form (14.10) of our recurrence relation! In general,  $y_n = nr^n$  is a solution **if and only if**  $r$  is a *multiple root* of the characteristic equation!

Why are they independent? Just consider (14.6):

$$x_0y_1 - x_1y_0 = 1 \cdot r - r \cdot 0 = r \neq 0,$$

which is true since  $r \neq 0$  (as  $c_2 = -r^2 \neq 0$ ).

**Example 14.11** (arithmetic progressions). Find the *general solution* to the recurrence relation

$$a_n = 2a_{n-1} - a_{n-2}.$$

*Solution:* The characteristic equation

$$r^2 = 2r - 1$$

has a single multiple root  $r = 1$ . Hence, the general solution is

$$a_n = X \cdot 1^n + Yn \cdot 1^n = X + nY.$$

In other words, solutions to our recurrence relation are precisely all arithmetic progressions! This is not a surprise, as arithmetic progressions are characterized by the property

$$a_{n-1} + a_{n+1} = 2a_n,$$

which is essentially our relation (with an index shift).

14.6. **Case 3: no real roots.** If the **characteristic equation** has no real root, we seem to be in trouble, and the Book leaves this case out. Thus, let us discuss it very briefly.

Of course, **any** algebraic equation has roots (the so-called *Fundamental Theorem of Algebra*), but they may happen to be *complex*, i.e., involve the *imaginary unit*  $i = \sqrt{-1}$ . Thus, our equation does have two roots

$$\alpha \pm \beta i,$$

which are complex conjugate (in particular, **distinct**), and all that was said above applies: a *general solution* can be written in the form

$$a_n = X(\alpha + \beta i)^n + Y(\alpha - \beta i)^n, \quad X, Y \in \mathbb{C}.$$

Now, one can work hard, using the *trigonometric form* of complex numbers and *de Moivre's formula*, and get rid of  $i$ , representing the result by an ugly formula, involving geometric progressions **and trigonometric functions**, but using real numbers only. We will follow the Book and leave it out; those familiar with complex numbers can do this as an extra homework.

**Example 14.12.** Consider the recurrence relation

$$a_n = -a_{n-2}.$$

Its characteristic equation  $r^2 = -1$  has no real root. On the other hand, the relation itself does have solutions! One example is the sequence

$$1, 1, -1, -1, 1, 1, -1, -1, \dots$$

The *general solution* to this recurrence relation can be written in the form

$$a_n = X \sin \frac{n\pi}{2} + Y \cos \frac{n\pi}{2}, \quad X, Y \in \mathbb{R}.$$

Note that, if  $X, Y \in \mathbb{Z}$ , so are all  $a_n$ , in spite of the look of the formula!

**Remark 14.13.** *Differential equations* of this kind, e.g.,  $y'' + y = 0$ , describe all kinds of oscillations and hence are indispensable in physics; that is why they have to be considered in the differential equation courses. On the other hand, similar recurrence relations do not often appear in counting problems, and we can live without them!

as they do in  
differential  
equations

Relax: we will not  
do this in the  
future!

14.7. **The general case of degree  $d$ .** Back to the general case, to a degree  $d$  recurrence relation

$$(14.14) \quad a_n = c_1 a_{n-1} + c_2 a_{n-2} + \dots + c_{d-1} a_{n-d+1} + c_d a_{n-d}$$

we can associate its *characteristic equation*

$$(14.15) \quad r^d = c_1 r^{d-1} + c_2 r^{d-2} + \dots + c_{d-1} r + c_d.$$

(We replace all  $a$ 's with powers of  $r$ , starting from  $r^0 = 1$  in the rightmost term and moving **right to left**, increasing the exponent by 1 at each step.) Arguing as above, a *geometric progression*  $x_n = r^n$  is a solution to (14.14) if and only if  $r$  is a root of (14.15). Recall that a polynomial equation of degree  $d$  has **exactly  $d$  roots**, counted with *multiplicities*, i.e., the polynomial can be factored in the form (in our case)

You must have seen this in Calculus

$$\begin{aligned} r^d - c_1 r^{d-1} - c_2 r^{d-2} - \dots - c_{d-1} r - c_d \\ = (r - r_1)^{m_1} (r - r_2)^{m_2} \dots (r - r_s)^{m_s} \end{aligned}$$

with  $m_1 + m_2 + \dots + m_s = d$ . Some of the roots  $r_i$  may be complex, but we will assume that they are all real.

**THE RULE.** In this notation, the recurrence relation (14.14) has  $d$  independent solutions, **constructed as follows**: each  $m_i$  fold root  $r_i$  gives rise to  $m_i$  solutions

$$x_n = n^p r_i^n, \quad p = 0, 1, \dots, m_i - 1.$$

This is very similar to the partial fractions in Calculus, is it not?

**Example 14.16.** Assume that a degree 9 recurrence relation has

$$r^9 - c_1 r^{d-1} - c_2 r^{d-2} - \dots = (r - 1)^4 (r + 2)^3 (r - 3)(r + 3).$$

(Here, the last two roots  $r = \pm 3$  have multiplicities  $m_3 = m_4 = 1$ ; such roots are called *simple*.) Then, the 9 independent solutions are

$$\begin{aligned} 1^n = 1, \quad n1^n = n, \quad n^2 1^n = n^2, \quad n^3 1^n = n^3, & \quad (\text{the 4-fold root } r = 1), \\ (-2)^n, \quad n(-2)^n, \quad n^2(-2)^n & \quad (\text{the 3-fold root } r = -2), \\ 3^n, & \quad (\text{the simple root } r = 3), \\ (-3)^n, & \quad (\text{the simple root } r = -3). \end{aligned}$$

Hence, the *general solution* is

$$A + Bn + Cn^2 + Dn^3 + E(-2)^n + F(-2)^n + Gn^2(-2)^n + H3^n + I(-3)^n,$$

and you need 9 pieces of initial data to find the 9 constants  $A, \dots, I$ .

Of course, in reality we will try to stick to recurrence relations of degree two or, at most, three!

**Remark 14.17.** The statement above is a **theorem**, meaning that the system you set up to find the constants **must have a unique solution**. If it has none or more than one, you have made a mistake and you should check your computation. if you have no time, at least you should indicate that something went wrong and you see this!

**Example 14.18.** Solve the recurrence relation

$$a_0 = 2, \quad a_1 = 5, \quad a_2 = 15, \quad a_n = 6a_{n-1} - 11a_{n-2} + 6a_{n-3} \quad \text{for } n \geq 3.$$

*Solution:* The characteristic equation

$$r^3 = 6r^2 - 11r + 6$$

has three roots 1, 2, and 3.

*Hint.* Although there is a “formula” for solving a cubic equation, in practice it is useless. Therefore, our only hope is to **guess** at least one root! Typically, our equations have integer coefficients, and we hope that at least one root is also an integer! (Otherwise, how can we guess it?) The candidates to be tried, one-by-one, are the divisors of the free term, *i.e.*, in our case,  $\pm 1, \pm 2, \pm 3, \pm 6$ . Once one of the roots, say,  $r = 1$ , has been guessed, you can reduce the degree by polynomial division:

$$r^3 - 6r^2 + 11r - 6 = (r - 1)(r^2 - 5r + 6).$$

Note that it **must** be divisible! Otherwise, 1 is not a root and something is wrong! Now, the remaining roots are those of  $r^2 - 5r + 6$ , and they can be found by the high school formula.

Back to the example, the general solution is

$$a_n = A \cdot 1^n + B \cdot 2^n + C \cdot 3^n, \quad A, B, C \in \mathbb{R}.$$

Substituting  $n = 0, 1, 2$ , we get a system

$$\begin{cases} A + B + C = 2, & (\#1) \\ A + 2B + 3C = 5, & (\#2) \\ A + 4B + 9C = 15. & (\#3) \end{cases}$$

Subtract (#1) from (#2) and (#3) to get

$$\begin{cases} B + 2C = 3, \\ 3B + 8C = 13, \end{cases} \quad \text{hence} \quad 2C = 4, \quad C = 2, \quad \text{and} \quad B = -1;$$

then, from (#1),  $A = 1$ . Finally, the solution is

$$a_n = 1 - 2^n + 2 \cdot 3^n.$$

**Example 14.19.** Solve the recurrence relation

$$a_0 = 1, \quad a_1 = -2, \quad a_2 = -1, \quad a_n = -3a_{n-1} - 3a_{n-2} - a_{n-3} \quad \text{for } n \geq 3.$$

*Solution:* The characteristic equation

$$r^3 + 3r^2 + 3r + 1 = (r + 1)^3 = 0$$

has a single triple root  $r = -1$  (recognizing the high school formula).

The general solution is

$$a_n = A(-1)^n + Bn(-1)^n + Cn^2(-1)^n$$

and, substituting  $n = 0, 1, 2$ ,

$$\begin{cases} A = 1, & (\#1) \\ -A - B - C = -2, & (\#2) \\ A + 2B + 4C = -1. & (\#3) \end{cases}$$

Then,  $A = 1$  is given by (#1), and  $2(\#2) + (\#3)$  becomes  $2C = -4$ , or  $C = -2$ . Then  $B = 3$  from (#2), and the solution is

$$a_n = (1 + 3n - 2n^2)(-1)^n.$$

**Example 14.20.** Find the general solution to

$$a_n = 3a_{n-2} + 2a_{n-3}.$$

*Solution:* The characteristic equation is

$$r^3 = 3r + 2.$$

(Pay attention to the terms!) Observing that  $r = -1$  is a root, we divide

$$r^3 - 3r - 2 = (r + 1)(r^2 - r - 2) = (r + 1)^2(r - 2)$$

and solve  $r^2 - r - 2 = 0$  to find two more roots  $r = 2$  and  $r = -1$ .

It follows that, in the original equation,  $r = -1$  is a double root (of multiplicity  $m = 2$ ) and  $r = 2$  is a simple root (of multiplicity  $m = 1$ ).

Hence, the general solution is

$$a_n = (A + Bn)(-1)^n + C \cdot 2^n, \quad A, B, C \in \mathbb{R}.$$

**Remark 14.21.** Later, we will develop another way of handling this problem, based on the generating functions. It would also apply to the nonhomogeneous relations!

the discrete counterpart of the so-called Laplace transform in differential equations

14.8. **Summation formulas.** If a sequence  $a_n$  satisfies a recurrence relation

$$(14.22) \quad a_n = c_1 a_{n-1} + c_2 a_{n-2} + \dots + c_{d-1} a_{n-d+1} + c_d a_{n-d}$$

of degree  $d$ , then the sequence of its *partial sums*

$$s_n := \sum_{k=0}^n a_k$$

satisfies a similar relation of degree  $d+1$ , which we can “solve” instead of trying to guess the formula and prove it by induction. Indeed, just observe that

$$a_n = s_n - s_{n-1}$$

and substitute to (14.22) to get

$$s_n = (c_1 + 1)s_{n-1} + (c_2 - c_1)s_{n-2} + \dots + (c_d - c_{d-1})s_{n-d} - c_d s_{n-d-1}.$$

It looks a bit awkward, but it is not worth remembering: the only thing that matters is that *the characteristic equation of this new relation is obtained from that for the old one by the multiplication by  $r-1$* . (This is all that we need to know to solve the new relation!)

**Example 14.23** (geometric progression). Any *geometric progression*  $a_n = c^n$  satisfies the recurrence relation  $a_n = ca_{n-1}$  (this is how we solve them!) with the characteristic equation  $r - c = 0$ . Hence, the sequence of sums  $s_n$  satisfies the relation

$$s_n = (c+1)s_{n-1} - cs_{n-2}$$

with the characteristic equation

$$(r-1)(r-c) = r^2 - (c+1)r + c = 0.$$

Now, **assuming that**  $c \neq 1$  (the case  $c = 1$  needs special attention and the answer is totally different!), we arrive at

$$s_n = A + Bc^n,$$

where  $A, B$  are found from the initial data

$$s_0 = a_0 = 1, \quad s_1 = a_0 + a_1 = c + 1,$$

i.e., from the system

$$\begin{cases} A + B = 1, \\ A + cB = c + 1, \end{cases} \quad \text{hence} \quad B = \frac{c}{c-1}, \quad A = -\frac{1}{c-1}.$$

Thus, we obtain the classical formula

$$s_n = \frac{c^{n+1} - 1}{c - 1}.$$

**Example 14.24** (summation of integers). The sequence

$$a_n = n,$$

like any *arithmetic progression* (cf. Example 14.11), satisfies the degree two recurrence relation

$$a_n = 2a_{n-1} - a_{n-2}$$

with the characteristic equation  $r^2 - 2r + 1 = (r - 1)^2 = 0$ . Hence, the sequence

$$s_n := \sum_{k=0}^n a_k = \sum_{k=0}^n k,$$

which we studied *via* induction, must satisfy the degree three relation

$$s_n = 3s_{n-1} - 3s_{n-2} + s_{n-3}$$

$$r^3 = 3r^2 - 3r + 1r^0$$

with the characteristic equation  $(r - 1)^3 = 0$ . Its general solution is

$$s_n = A + Bn + Cn^2,$$

and we only need three pieces of initial data

$$s_0 = 0, \quad s_1 = 0 + 1 = 1, \quad s_2 = 0 + 1 + 2 = 3$$

to find  $A = 0$  and  $B = C = \frac{1}{2}$  from the system

$$\begin{cases} A & = 0, \\ A + B + C & = 1, \\ A + 2B + 4C & = 3. \end{cases}$$

Thus,

$$s_n = \frac{1}{2}n + \frac{1}{2}n^2 = \frac{n(n+1)}{2}.$$

Here are the two written side by side, so that you can see the correspondence

**Example 14.25** (summation of integer powers). Now, we can do the same for any degree  $p$ , computing

$$s_n = \sum_{k=0}^n n^p.$$

The sequence  $a_n := n^p$  satisfies the degree  $(p+1)$  recurrence relation with the characteristic equation  $(r-1)^{p+1} = 0$ .

Indeed, if the characteristic equation is  $(r-1)^{p+1} = 0$ , i.e., has a single root  $r = 1$  of the maximal multiplicity  $m = p+1$ , the general solution is

$$(14.26) \quad a_n = (C_0 + C_1 n + \dots + C_p n^p) \cdot 1^n = C_0 + C_1 n + \dots + C_p n^p,$$

i.e., any polynomial in  $n$  of degree up to  $p$ !

Hence,  $s_n$  satisfies the degree  $(p+2)$  recurrence relation with the characteristic equation  $(r-1)^{p+2} = 0$ . (By now, we understand that we can save on the boring job of writing down the explicit relation!) Hence, by our theory, just as in (14.26),  $s_n$  is a polynomial of degree  $p+1$ :

$$(14.27) \quad s_n = C_0 + C_1 n + \dots + C_{p+1} n^{p+1}.$$

To find the coefficients, we merely need to compute the first  $(p+2)$  values

$$s_0 = 0, \quad s_1 = 1, \quad \dots, \quad s_{p+1} = 1^p + 2^p + \dots + (p+1)^p$$

and solve the respective system.

**Remark 14.28.** The coefficients in (14.27) give rise to a remarkable sequence of (rational) numbers called *Bernoulli numbers*; mysteriously, they keep reappearing everywhere, including physics and geometry! In a sense, up to some binomial coefficients and common factor  $1/(p+1)$ , these coefficients do not depend on  $p$ ! Here are the first few polynomials:

$$\begin{aligned} \sum_{k=0}^n n &= \frac{1}{2}n^2 + \frac{1}{2}, \\ \sum_{k=0}^n n^2 &= \frac{1}{3}n^3 + \frac{1}{2}n^2 + \frac{1}{6}n, \\ \sum_{k=0}^n n^3 &= \frac{1}{4}n^4 + \frac{1}{2}n^3 + \frac{1}{4}n^2, \\ \sum_{k=0}^n n^4 &= \frac{1}{5}n^5 + \frac{1}{2}n^4 + \frac{1}{3}n^3 - \frac{1}{30}n, \\ \sum_{k=0}^n n^5 &= \frac{1}{6}n^6 + \frac{1}{2}n^5 + \frac{5}{12}n^4 - \frac{1}{12}n^2. \end{aligned}$$

Can you explain why?

## 15. Linear NON-homogeneous recurrence relations

A *linear NON-homogeneous* recurrence relation of degree  $d$  with constant coefficients is a recurrence relation of the form

$$(15.1) \quad a_n = c_1 a_{n-1} + c_2 a_{n-2} + \dots + c_d a_{n-d} + F(n),$$

where  $F(n)$  is a given function of  $n$  (aka sequence). To this, we *associate* the corresponding *homogeneous* relation

$$(15.2) \quad a_n = c_1 a_{n-1} + c_2 a_{n-2} + \dots + c_d a_{n-d}$$

(by simply dropping  $F(n)$ ). This time, the linearity manifests as follows.

**GOAL:** *general solution*  $a_n$  (with constants  $A, B, \dots$ ) to (15.1).

**KNOWN:** *general solution*  $a_n^{(h)}$  to (15.2).

So that later we can find these constants from the initial data

**Theorem 15.3.** *The general solution to a nonhomogeneous relation (15.1) has the form*

$$a_n = a_n^{(h)} + a_n^{(p)},$$

where  $a_n^{(h)}$  is the **general** solution to the *associated homogeneous relation* (15.2) and  $a_n^{(p)}$  is **any fixed particular solution** to the *original relation* (15.1).

h for homogeneous  
p for particular

In other words, since we know how to solve (15.2), if we know **one solution** to (15.1), we know **them all**!

*Proof.* First, check that this is a solution:

$$\begin{aligned} a_n &= a_n^{(h)} + a_n^{(p)} \\ &= c_1 a_{n-1}^{(h)} + c_2 a_{n-2}^{(h)} + \dots + c_d a_{n-d}^{(h)} && \text{by (15.2)} \\ &+ c_1 a_{n-1}^{(p)} + c_2 a_{n-2}^{(p)} + \dots + c_d a_{n-d}^{(p)} + F(n) && \text{by (15.1)} \\ &= c_1 a_{n-1} + c_2 a_{n-2} + \dots + c_d a_{n-d} + F(n), \end{aligned}$$

which is precisely (15.1) for  $a_n$ . There remains to observe that  $a_n^{(h)}$  is the *general solution*: as such, it contains  $d$  arbitrary constants, and they suffice to serve **any** collection of  $d$  pieces of initial conditions.  $\square$

**THE RULE.** Therefore, here is how we proceed to solve (15.1):

- (1) Use the rule in §14.7 on page 47 to find the **general** solution  $a_n^{(h)}$  to the *associated homogeneous relation* (15.2). (Arbitrary constants are involved: **leave them as such** for the time being!)
- (2) Use the rule §15.1 on the next page to find a **particular** solution  $a_n^{(p)}$  to the *original relation* (15.1). (Constants are also involved: **resolve them**!)
- (3) Write  $a_n = a_n^{(h)} + a_n^{(p)}$ , with the constants left over from item 1. **Resolve these constants** by using the initial data (as in the homogeneous case).

keep it the **general** solution!

find a **particular** solution!

Now, find a **particular** solution to (15.1)

15.1. **THE RULE** (for some special functions  $F(n)$ ). For now, we can handle only free parts of a very special kind, *viz.* polynomial times exponential:

$$(15.4) \quad F(n) = (u_0 + u_1 n + \dots + u_t n^t) \cdot s^n,$$

where  $u_0, \dots, u_t$  and  $s$  are fixed. (Note that  $s$  may be equal to 1, which makes it a bare polynomial. Conversely, a polynomial **must** be treated as (15.4), *i.e.*, you **must** implicitly assume an  $s = 1$ : this **may be very important later**, see **Remark 15.6!**)

The theorem states that a particular solution  $a_n^{(p)}$  to the relation (15.1) with  $F(n)$  as in (15.4) can be found in the form

$$(15.5) \quad a_n^{(p)} = (A + Bn + \dots + Zn^t) \cdot s^n \cdot n^m,$$

where  $A, B, \dots, Z$  are some constants that **are to be found by substituting (15.5) to the original relation (15.1)** and equating the terms with the same power of  $n$ . (In other words, it is a polynomial of the same degree  $t$  multiplied by the same exponential  $s^n$ ; you must use **all** terms from  $An^0$  to  $Zn^t$  even if some of them are missing in (15.4)!) very much like partial fractions in Calculus!

In particular, the theorem states that you **must** be able to find a **unique** set of  $A, B, \dots, Z$ ; if you cannot find them or found too many, **something must be wrong!**

However, **do not relax yet**: there are underwater currents! If  $s$  in (15.4) happens to be a root of the **characteristic equation** of (15.2) of some multiplicity  $m$ , this expression (15.5) **is to be multiplied by  $n^m$** . Intuitively, in this case the first  $m$  terms

$$(A + Bn + \dots + Dn^{m-1}) \cdot s^n$$

are useless as they satisfy the **associated homogeneous relation** (15.2), not contributing to the “non-homogeneity”  $F(n)$ ; hence, we get rid of these useless terms by shifting everything  $m$  units up!

**Remark 15.6.** It is this extra clause, the possible extra  $n^m$ , where you should not forget about the *possible implicit*  $s = 1$  in (15.4), as  $1$  may as well be a root of the characteristic equation!

**Example 15.7** (The Tower of Hanoi, cf. [Example 13.5](#)). Solve the recurrence relation

$$H_1 = 1, \quad H_n = 2H_{n-1} + 1.$$

*Solution:* The associated homogeneous relation is

$$a_n = 2a_{n-1}$$

(drop the  $+1$ ), its characteristic equation  $r = 2$  has a single root  $r = 2$ , and the **general solution** is

$$a_n^{(h)} = A \cdot 2^n,$$

**all** these satisfy

$$a_n = 2a_{n-1}$$

where  $A$  is a constant which is to be left intact for now! A **particular solution**  $a_n^{(p)}$  is to be found in the form

$$a_n^{(p)} = B = (Bn^0) \cdot 1^n$$

only **one** of these satisfies

$$a_n = 2a_{n-1} + 1$$

(a polynomial of degree  $0$  times  $1^n$ ), and the constant  $B$  is to be found **now!** Substituting (to the **original nonhomogeneous relation**), we get

$$B = 2B + 1,$$

or  $B = -1$ . (There is a unique solution!) Hence, the **general solution** to the **original nonhomogeneous relation** is

$$H_n = A \cdot 2^n - 1.$$

Now (**and not before**), we use the initial data to find  $A$ :

$$H_1 = 1 = A \cdot 2^1 - 1, \quad \text{or} \quad A = 1.$$

only **one** satisfies the initial data as well!

Finally,

$$H_n = 1 \cdot 2^n - 1 = 2^n - 1,$$

which we already know!

**Example 15.8** (valid decimal codes, cf. [Example 13.8](#)). Solve the recurrence relation

$$c_0 = 1, \quad c_n = 8c_{n-1} + 10^{n-1}.$$

*Solution:* This is literally the same as the previous one (so I have just copy-pasted it). The associated homogeneous relation is

$$c_n = 8c_{n-1}$$

(drop the  $+10^{n-1} = \frac{1}{10}10^n$ ), its characteristic equation  $r = 8$  has a single root  $r = 8$ , and the **general solution** is

$$c_n^{(h)} = A \cdot 8^n,$$

where  $A$  is a constant which is to be left intact for now! A **particular solution**  $c_n^{(p)}$  is to be found in the form

$$c_n^{(p)} = B \cdot 10^n = (Bn^0) \cdot 10^n$$

(a polynomial of degree 0 times  $10^n$ ), and the constant  $B$  is to be found **now!** Substituting (to the **original nonhomogeneous relation**), we get

$$B \cdot 10^n = 8B \cdot 10^{n-1} + 10^{n-1}, \quad \text{or} \quad B \cdot 10 = 8B + 1,$$

or  $B = \frac{1}{2}$ . (There is a unique solution!) Hence, the **general solution** to the **original nonhomogeneous relation** is

$$c_n = A \cdot 8^n + \frac{1}{2} \cdot 10^n.$$

**Now**, we use the initial data to find  $A$ :

$$c_0 = 1 = A \cdot 8^0 + \frac{1}{2} \cdot 10^0, \quad \text{or} \quad A = \frac{1}{2}.$$

Finally,

$$c_n = \frac{1}{2} \cdot 8^n + \frac{1}{2} \cdot 10^n = \frac{1}{2}(8^n + 10^n),$$

as promised!

**Remark 15.9.** You should **never, ever, ever** try to use the initial data to find the coefficients  $A, \dots$  at the first stage, in the **general solution** to the **associated homogeneous relation**: this relation has nothing to do with the initial conditions, and its solutions have no reason to satisfy them! If you tried that in this (or previous) example, you would get a completely different sequence! (Try it, just for fun...)

**all** these satisfy  
 $c_n = 2c_{n-1}$

only **one** of these  
 satisfies  
 $c_n = 2c_{n-1} + 1$

only **one** satisfies  
 the initial data as  
 well!

**Example 15.10.** What does a particular solution  $a_n^{(p)}$  for the recurrence relation

$$a_n = 6a_{n-1} - 9a_{n-2} + F(n)$$

look like if

- (1)  $F(n) = 3^n$ ?
- (2)  $F(n) = n3^n$ ?
- (3)  $F(n) = n^2 2^n$ ?
- (4)  $F(n) = (n^2 + 1)3^n$ ?

*Solution:* First of all, observe that the characteristic equation

$$r^2 = 6r - 9$$

has a single double root  $r = 3$  (i.e., its multiplicity is  $m = 2$ .)

Now, in Case (3), since  $2 \neq 3$ , there is no problem:

$$a_n^{(p)} = (A + Bn + Cn^2)2^n.$$

(Note, though, that we have to use all terms from  $n^0$  to  $n^2$ , even though only  $n^2$  is present in  $F(n)$ !)

In Case (1), it would have been  $A \cdot 3^n$ ; however, since  $s = 3$  is a 2-fold root of the characteristic equation, this is to be multiplied by  $n^2$ :

$$a_n^{(p)} = A \cdot 3^n \cdot n^2.$$

Likewise, in Cases (2) and (4), we do the same, multiplying the solution suggested by the rule by an extra  $n^2$ :

$$a_n^{(p)} = (A + Bn) \cdot 3^n \cdot n^2 \quad \text{and} \quad a_n^{(p)} = (A + Bn + Cn^2) \cdot 3^n \cdot n^2,$$

respectively. Note again that all powers of  $n$ , from  $n^0 = 1$  to the maximum present in  $F(n)$ , should be used.

In fact, let us try to solve some of these and find the coefficients. In Case (1), we have

$$A \cdot 3^n \cdot n^2 = 6A \cdot 3^{n-1} \cdot (n-1)^2 - 9A \cdot 3^{n-2} \cdot (n-2)^2 + 3^n,$$

or, cancelling  $3^n$  and multiplying out,

$$An^2 = 2A(n^2 - 2n + 1) - A(n^2 - 4n + 4) + 1, \quad \text{or} \quad 0 = -2A + 1;$$

thus,  $A = \frac{1}{2}$ . Observe that all terms with  $n^2$  and  $n^1$  are gone no matter what  $A$  is! Essentially, that is why we had to multiply by  $n^2$ . If I tried  $a_n^{(p)} = A \cdot 3^n$  (or even  $A \cdot 3^n \cdot n$ ), I would be doomed:

$$A \cdot 3^n = 2 \cdot 3 \cdot A \cdot 3^{n-1} - 3^2 \cdot A \cdot 3^{n-2} + 3^n, \quad \text{or} \quad 0 = 1$$

has no solution!

What is written here is wrong!

In Case (3),

$$(A + Bn + Cn^2)4 \cdot 2^{n-2} = 6[(A + B(n-1) + C(n-1)^2]2 \cdot 2^{n-2} \\ - 9[(A + B(n-2) + C(n-2)^2]2^{n-2} + n^2 4 \cdot 2^{n-2}$$

boils down to (cancelling  $2^{n-2}$ )

$$4A + \underline{4Bn} + \underline{\underline{4Cn^2}} = 12A + 12B(\underline{n} - 1) + 12C(\underline{\underline{n^2}} - \underline{2n} + 1) \\ - 9A - 9B(\underline{n} - 2) - 9C(\underline{\underline{n^2}} - \underline{4n} + 4) + \underline{\underline{4n^2}}$$

or, collecting similar terms ( $n^0$ ,  $\underline{n^1}$ , and  $\underline{\underline{n^2}}$ ),

$$\begin{cases} \underline{A} - 6\underline{B} + 24\underline{C} = 0, \\ \underline{B} - 12\underline{C} = 0, \\ \underline{C} = 4. \end{cases}$$

Hence, working backwards,

$$\underline{C} = 4, \quad \underline{B} = 48, \quad \underline{A} = 192$$

(assuming that I did everything right). Note, again, that **this would not work** if we left out  $A$  or  $Bn$  (*i.e.*, with  $A = B = 0$ ): we would still find  $C = 4$ , but **the other terms would not match!**

**Example 15.11** (summation again). Find the sum

$$a_n = \sum_{k=0}^n k.$$

*Solution:* This time, we say that our sequence is subject to the nonhomogeneous recurrence relation

$$a_0 = 0, \quad a_n = a_{n-1} + n,$$

just by the definition. The characteristic equation  $r = 1$  has a single root  $r = 1$ , and the general solution to the associated homogeneous relation is

$$a_n^{(h)} = A \cdot 1^n = A, \quad A \in \mathbb{R}.$$

The free term is  $F(n) = n \cdot 1^n$ , and the implicit  $s = 1$  matters, as it is a root of the characteristic equation! Hence, we are looking for a particular solution in the form

$$a_n^{(p)} = (B + Cn) \cdot n = Bn + Cn^2.$$

Substituting,

$$Bn + Cn^2 = B(n-1) + C(n^2 - 2n + 1) + n,$$

or

$$0 = (C - B) + (1 - 2C)n, \quad \text{hence } B = C = \frac{1}{2},$$

and, from the initial data,

$$0 = a_0^{(h)} + a_0^{(p)} = A.$$

Thus, as usual,

$$a_n = \frac{1}{2}n + \frac{1}{2}n^2 = \frac{n(n+1)}{2}.$$

(Remember that our theorem states that  $a_n^{(p)}$  is one of the solutions; here, *accidentally*, it turns out that it is the one!)

**Remark 15.12.** Next week we will see another way of solving such recurrence relations. It is based in the *generating functions*, which, in this context, can be regarded as an analog of the so-called *Laplace transform* for differential equations.

## 16. Generating functions

Our goal is still to describe, in some reasonable terms, a sequence

$$a_n: \quad a_0, a_1, a_2, \dots$$

of real numbers. Throughout this section, we **always start the count from  $n = 0$** .

**Definition 16.1.** The *generating function* of a sequence  $a_0, a_1, \dots, a_n, \dots$  is the power series

$$G(x) = a_0 + a_1x + \dots + a_nx^n + \dots = \sum_{n=0}^{\infty} a_nx^n.$$

Here,  $x$  is a *dummy variable* (you can call it  $y$  or whatever); it merely serves as a placeholder, indicating the index  $n$ . Say, if I write

$$G(x) = 2 \cdot x^0 - 3x^1 + 0 \cdot x^2 + 5x^3,$$

I know that  $a_0 = 2$ ,  $a_1 = -3$ ,  $a_2 = 0$ ,  $a_3 = 5$ , and all other  $a_n = 0$ ,  $n \geq 4$ . Thus, for now, we can say that the generating function is a way to combine several (infinitely many) equations  $a_n = ?$  into a single one! (Of course, it is much better than just that, as we will see shortly.)

**Attention: CALCULUS.** Strictly speaking,  $G(x)$  is defined as a so-called *formal* power series, *i.e.*, the question of convergence is not raised. However, usually we want  $G$  to be given by a “nice formula”, and for this to make sense, we need the power series to have a *positive* radius of convergence (*i.e.*, it must converge at least somewhere except  $x = 0$ , so that we can “check” our “formula”). In any case, we will deal with but a few sequences whose generating functions are known from Calculus (or, rather, they are the coefficient sequences of the few power series known from Calculus).

**Example 16.2.** Here are a few examples of how the generating function collects the information about the sequence and represents it in a very compact form. Recall that **our sequences always start at  $n = 0$ !**

$$a_n = 3: \quad 3, 3, 3, 3, \dots, \quad G(x) = \sum_{n=0}^{\infty} 3x^n = \frac{3}{1-x}$$

(the famous *geometric series*: all others are derived from this!)

$$a_n: \quad 0, 0, 3, 3, 3, 3, \dots, \quad G(x) = \sum_{n=2}^{\infty} 3x^n = x^2 \sum_{m=0}^{\infty} 3x^m = \frac{3x^2}{1-x}.$$

Note that, because of a slight “irregularity” at the beginning, I cannot define  $a_n$  by a “formula”; nevertheless,  $G(x)$  still looks nice!

A very common  
trick: let  
 $m = n - 2$

$$a_n = 2^n: \quad 1, 2, 4, 8, \dots, \quad G(x) = \sum_{n=0}^{\infty} 2^n x^n = \sum_{n=0}^{\infty} (2x)^n = \frac{1}{1-2x}$$

(the *geometric series* again).

$$a_n = n + 1: \quad 1, 2, 3, 4, \dots, \quad G(x) = \sum_{n=0}^{\infty} (n+1)x^n = \frac{1}{(1-x)^2}$$

(a special case of the *binomial series*; to be explained later).

$$a_n: \quad 1, 1, 1, 1, 1, 1, 0, 0, \dots \quad a_n = 0 \text{ for } n \geq 6,$$

$$G(x) = 1 + x + x^2 + x^3 + x^4 + x^5 = \frac{x^6 - 1}{x - 1}.$$

Here, the sum is actually finite, as all terms with  $n \geq 6$  vanish.

$$a_n = C(N, n) \quad \text{for a fixed } N \in \mathbb{N}, \quad G(x) = \sum_{n=0}^N C(N, n)x^n = (1+x)^N$$

(the *binomial theorem*). Here, by our convention that  $C(N, n) = 0$  for  $n > N$ , we can as well run the summation over all  $0 \leq n < \infty$ .

**16.1. What you need to know about power series.** The best known power series is the *geometric series*:

$$\frac{1}{1-x} = \sum_{n=0}^{\infty} x^n \quad \text{for } |x| < 1.$$

(I indicate the interval of convergence even though we do not care!) As a slight generalization,

$$\frac{1}{1-rx} = \sum_{n=0}^{\infty} r^n x^n \quad \text{for } |x| < 1/|r|;$$

this is the generating function for the *geometric progression*  $a_n = r^n$ .

**Theorem 16.3.** *If*

$$f(x) = \sum_{n=0}^{\infty} a_n x^n, \quad g(x) = \sum_{n=0}^{\infty} b_n x^n,$$

*then*

$$f(x) + g(x) = \sum_{n=0}^{\infty} (a_n + b_n) x^n, \quad f(x)g(x) = \sum_{n=0}^{\infty} \left( \sum_{k=0}^n a_k b_{n-k} \right) x^n.$$

*Thus, power series can be added and multiplied like polynomials!*

Here is how the multiplication works: as usual, multiply each by each and collect similar terms:

$$\begin{aligned} (a_0 + a_1x + a_2x^2 + \dots)(b_0 + b_1x + b_2x^2 + \dots) \\ = (a_0b_0) + (a_0b_1 + a_1b_0)x + (a_0b_2 + a_1b_1 + a_2b_0)x^2 + \dots \end{aligned}$$

**Remark 16.4.** The multiplication formula is **our everything!** It is the basis for the application of generating functions to the counting problems! Roughly, we count the number  $c_n$  of ways to accomplish something depending on  $n$  (say, certain “ $c$ -strings”). Assume that this task can be broken into two phases, one “of length  $p$ ” with  $a_p$  outcomes and one “of length  $q$ ” with  $b_q$  outcomes, so that  $p + q = n$ . (A  $c$ -string of length  $n$  is a concatenation of an  $a$ -string of length  $p$  and a  $b$ -string of length  $q$ .) Then, the **Sum Rule** and **Product Rule** combine to

$$c_n = \sum_{p+q=n} a_p b_q,$$

*i.e., the generating function for  $c_n$  is the product of those for  $a_n$  and  $b_n$ .* Thus, instead of thinking hard, we can merely manipulate the generating functions algebraically! We will see more of that later!

**Example 16.5** (*cf.* also **Example 16.7**). Here is another application of the multiplication:

$$\begin{aligned} \frac{1}{(1-x)^2} &= \frac{1}{1-x} \cdot \frac{1}{1-x} \\ &= \left( \sum_{n=0}^{\infty} 1x^n \right) \left( \sum_{n=0}^{\infty} 1x^n \right) = \sum_{n=0}^{\infty} \underbrace{\left( \sum_{k=0}^n 1 \cdot 1 \right)}_{n+1 \text{ terms}} x^n = \sum_{n=0}^{\infty} (n+1)x^n. \end{aligned}$$

Of course, this holds within a common interval of convergence!

Here is another useful operation producing “new” power series from known ones.

**Theorem 16.6** (CALCULUS!). *Power series can be differentiated: if*

$$f(x) = \sum_{n=0}^{\infty} a_n x^n,$$

within the interval  
of convergence  
shift  $m = n - 1$

then

$$f'(x) = \sum_{n=0}^{\infty} (a_n x^n)' = \sum_{m=0}^{\infty} (m+1) a_{m+1} x^m.$$

**Example 16.7.** Here is another way to accomplish Example 16.5:

$$\frac{1}{(1-x)^2} = \left( \frac{1}{1-x} \right)' = \left( \sum_{n=0}^{\infty} x^n \right)' = \sum_{m=0}^{\infty} (m+1) x^m.$$

We could continue like this, with minor modifications, to obtain the power series for

$$\frac{1}{(1-x)^3}, \frac{1}{(1-x)^4}, \dots, \frac{1}{(1-x)^N}, \dots,$$

but we will have a general theorem in a minute!

**Exercise 16.8.** If  $G(x)$  is the generating function for a sequence  $a_n$ , then the following are generating functions for

$$\begin{array}{ll} x^2 G(x) & \text{for } 0, 0, a_0, a_1, a_2, \dots \text{ (index shift),} \\ G'(x) & \text{for } a_1, 2a_2, 3a_3, \dots \text{ } (b_n = (n+1)a_{n+1}), \\ [G(x)]^2 & \text{for } b_n = \sum_{k=0}^n a_k a_{n-k}, \\ \frac{G(x)}{1-x} & \text{for } b_n = \sum_{k=0}^n a_k \text{ (partial sums again!)} \end{array}$$

Explain!

**Example 16.9** (Catalan's numbers). Let  $G(x)$  be the generating function of a sequence  $a_n$  satisfying the recurrence relation (in black)

$$\frac{G(x) - a_0}{x} = \sum_{n=0}^{\infty} a_{n+1} \cdot x^n = \sum_{n=0}^{\infty} \left( \sum_{k=0}^n a_k a_{n-k} \right) \cdot x^n = [G(x)]^2.$$

Multiply by  $x^n$  and sum up, as shown, to get a *functional equation* for  $G(x)$ . If  $a_0 = 1$  (*Catalan's numbers*, see §8), we get

$$G = 1 + xG^2, \quad \text{or} \quad G(x) = \frac{1 - \sqrt{1 - 4x}}{2x}.$$

(We have to choose the “ $-$ ” in the formula so that  $G(x)$  has limit as  $x \rightarrow 0$ .) This is the generating function for Catalan's numbers!

I may need to explain a bit more the left hand side:

$$\begin{aligned} \sum_{n=0}^{\infty} a_{n+1} x^n &= a_1 + a_2 x + a_3 x^2 + \dots \\ &= \frac{1}{x} (a_1 x + a_2 x^2 + a_3 x^3 + \dots) = \frac{1}{x} [G(x) - a_0]. \end{aligned}$$

In other words, if we want to shift the sequence to the *right*, we multiply  $G(x)$  by a power of  $x$ . If we want to shift it to the *left*, we need to **divide** by a power of  $x$ . But, in order to make it divisible, we have to get rid of the few first terms first! Yet another way to put it, if I want to shift a sequence

$$a_0, a_1, a_2, a_3, \dots,$$

say, two units to the *left*, the *red* terms are going to disappear; so, I must kill them beforehand to make it  $0, 0, a_2, a_3, \dots$

We will explore this approach to recurrence relations on the regular basis later!

16.2. **The binomial series.** Recall that

$$C(n, k) = \frac{n!}{k!(n-k)!} = \frac{n(n-1)\dots(n-k+1)}{k!}.$$

and observe that the **second** formula (unlike the first one) makes sense **for any**  $n$ , not necessarily an integer! (It is just a polynomial in  $n$ .) Thus, **by convention**, we extend the binomial coefficients to **arbitrary** real values of  $n$  (whereas  $k$  is still a nonnegative integer):

$$C(u, k) = \binom{u}{k} := \frac{\overbrace{u(u-1)\dots(u-k+1)}^{k \text{ consecutive factors}}}{k!}, \quad u \in \mathbb{R}, \quad k \in \mathbb{N}.$$

Just in case,  $C(u, 0) = 1$  for any  $u \in \mathbb{R}$  (product of 0 factors is 1).

**Example 16.10.** Here is what happens when  $u = -n$  is a **negative** integer:

$$\begin{aligned} \binom{-n}{r} &= \frac{\overbrace{(-n)(-n-1)\dots(-n-r+1)}^{r \text{ negative factors}}}{r!} \\ &= (-1)^r \frac{(n+r-1)(n+r-2)\dots n}{r!} \cdot \frac{(n-1)!}{(n-1)!} \\ &= (-1)^r \frac{(n+r-1)!}{r!(n-1)!} \\ &= (-1)^r \binom{n+r-1}{r} = (-1)^r C(n+r-1, r). \end{aligned}$$

**Example 16.11.** Now, try a fraction  $u = 1/2$ :

$$\begin{aligned} \binom{1/2}{r+1} &= \frac{\overbrace{\frac{1}{2}(-\frac{1}{2})(-\frac{3}{2})\dots(\frac{1}{2}-r)}^{r \text{ negative factors}}}{(r+1)!} \\ &= \frac{(-1)^r}{2^{r+1}} \cdot \frac{1 \cdot 1 \cdot 3 \cdot \dots \cdot (2r-1)}{(r+1)!} \cdot \frac{\overbrace{2 \cdot 4 \cdot \dots \cdot 2r}^{r \text{ even factors}}}{2^r \cdot (1 \cdot 2 \cdot \dots \cdot r)} \\ &= \frac{(-1)^r}{2^{2r+1}} \cdot \frac{(2r)!}{(r+1)!r!} \\ &= \frac{(-1)^r}{2^{2r+1}} \cdot \frac{1}{r+1} \cdot \frac{(2r)!}{r! \cdot r!} \\ &= \frac{(-1)^r}{2^{2r+1}} \cdot \frac{1}{r+1} \binom{2r}{r} = \frac{(-1)^r}{2^{2r+1}} C_r. \end{aligned}$$

If  $r = -1$ , this expression equals  $C(1/2, 0) = 1$ , whereas  $C_{-1}$  hardly makes sense. **This is quite common: one should be very careful in the “border cases.”**

Beware of the sign! It differs from previous formulas with power series!

**Theorem 16.12** (the *binomial series*). For any  $u \in \mathbb{R}$ , one has

$$(1 + x)^u = \sum_{n=0}^{\infty} \binom{u}{n} x^n \quad \text{for all } |x| < 1.$$

**Remark 16.13.** If  $u$  is a **nonnegative integer**, we have  $\binom{u}{n} = 0$  for  $n > u$  and the summation is finite,  $0 \leq n \leq u$ . Thus, we get the usual *binomial formula*, see [Theorem 4.1](#).

**Example 16.14.** Let  $u = -N$  be a negative integer. Then

$$\begin{aligned} \frac{1}{(1+x)^N} &= (1+x)^{-N} = \sum_{n=0}^{\infty} \binom{-N}{n} x^n \\ &= \sum_{n=0}^{\infty} (-1)^n C(N+n-1, n) x^n. \quad (\text{see Example 16.10}) \end{aligned}$$

Changing  $x$  to  $-x$ ,

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

**Example 16.15** (Catalan's numbers yet again). Let  $u = \frac{1}{2}$ . Then

$$\begin{aligned} \sqrt{1+x} &= (1+x)^{1/2} = \sum_{n=0}^{\infty} \binom{1/2}{n} x^n \\ &= 1 + \sum_{n=1}^{\infty} \frac{(-1)^{n-1}}{2^{2n-1}} C_{n-1} x^n. \quad (\text{see Example 16.11}) \end{aligned}$$

Changing  $x$  to  $-4x = -2^2x$ ,

$$\sqrt{1-4x} = 1 + \sum_{n=1}^{\infty} \frac{(-1)^{n-1} (-1)^n 2^{2n}}{2^{2n-1}} C_{n-1} x^n = 1 - 2 \sum_{n=1}^{\infty} C_{n-1} x^n.$$

Playing further (subtracting and dividing),

$$\frac{1 - \sqrt{1-4x}}{2x} = \sum_{m=0}^{\infty} C_m x^m.$$

Thus, at the end we have proved that Catalan's numbers are Catalan's numbers, *i.e.*, that the sequence  $a_n$  satisfying the recurrence relation in [Example 16.9](#) and initial condition  $a_0 = 1$  is

$$a_n = C_n = \frac{1}{n+1} \binom{2n}{n}.$$

As you see, sometimes you need to go quite a way to solve a counting problem! But, of course, our problems will be much easier!

**16.3. Useful power series.** Here are the few power series/polynomials that you are supposed to know. Most are nothing but special cases of [Theorem 16.12](#).

$$(16.16) \quad (1 + rx)^N = \sum_{n=0}^N \binom{N}{n} r^n x^n, \quad N \in \mathbb{N},$$

$$(16.17) \quad \frac{1 - x^{N+1}}{1 - x} = \sum_{n=0}^N x^n, \quad N \in \mathbb{N},$$

$$(16.18) \quad \frac{1}{1 - rx} = \sum_{n=0}^{\infty} r^n x^n,$$

$$(16.19) \quad \frac{1}{(1 - rx)^2} = \sum_{n=0}^{\infty} (n+1) r^n x^n,$$

$$(16.20) \quad \frac{1}{(1 - rx)^N} = \sum_{n=0}^{\infty} \binom{N+n-1}{n} r^n x^n, \quad N \in \mathbb{N},$$

$$(16.21) \quad (1 + rx)^u = \sum_{n=0}^{\infty} \binom{u}{n} r^n x^n, \quad u \in \mathbb{R}.$$

You can also make further substitutions (in the table, in most cases I have substituted  $x \mapsto rx$ ). For example, substituting  $x \mapsto -x^2$  in the geometric series (16.18), we get

$$\frac{1}{1 + x^2} = \sum_{n=0}^{\infty} (-1)^n x^{2n} = 1 + 0x - x^2 + 0x^3 + x^4 + 0x^5 - x^6 + \dots$$

This is the generating function for the rather sophisticated 4-periodic sequence

$$a_n: 1, 0, -1, 0, 1, 0, -1, 0, 1, \dots$$

which is not easy to describe by a “closed formula”: the best I can think of is

$$a_n = \cos \frac{\pi n}{4}, \quad n \geq 0.$$

Remember that we assume **all** powers of  $x$  present! Some may have coefficient **0**, which are part of the sequence!

## 17. Generating functions and counting

As mentioned before, in the applications of generating functions our everything is the *product formula*

$$(17.1) \quad \left( \sum_{n=0}^{\infty} a_n x^n \right) \left( \sum_{n=0}^{\infty} b_n x^n \right) = \sum_{n=0}^{\infty} \left( \sum_{k=0}^n a_k b_{n-k} \right) x^n$$

for polynomials/power series (see [Theorem 16.3](#)), which combines the [Sum Rule](#) and [Product Rule](#) in a single algebraic manipulation!

**Example 17.2.** Let us start with a very stupid example: what is the number  $a_n$  of solutions to the equation

$$e_1 = n, \quad e_1 \in \mathbb{Z}, \quad 2 \leq e_1 \leq 5?$$

Obviously, there is **one** solution if  $2 \leq n \leq 5$  and **none** otherwise, *i.e.*,  $a_n$  is the sequence

$$a_n: 0, 0, 1, 1, 1, 1, 0, 0, 0, \dots$$

with the generating function

$$A(x) = x^2 + x^3 + x^4 + x^5 = x^2(1 + x + x^2 + x^3).$$

(Here, the terms with coefficient 1 are those whose exponent is a value that can be taken by  $e_1$ .)

Likewise, if I want to count the number  $b_n$  of solutions to

$$e_2 = n, \quad e_2 \in \mathbb{Z}, \quad 3 \leq e_2 \leq 6,$$

I end up with the sequence

$$b_n: 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, \dots$$

with the generating function

$$B(x) = x^3 + x^4 + x^5 + x^6 = x^3(1 + x + x^2 + x^3).$$

Now, watch my hands! Let us combine the two and count solutions to

$$(17.3) \quad e_1 + e_2 = n, \quad e_1, e_2 \in \mathbb{Z}, \quad 2 \leq e_1 \leq 5, \quad 3 \leq e_2 \leq 6.$$

I can “break” the equation into two:

$$(17.4) \quad e_1 = p, \quad e_2 = q, \quad p + q = n.$$

Any solution to (17.3) occurs as a solution to (17.4) for **some**  $0 \leq p \leq n$  and  $q = n - p$ . By the [Product Rule](#), for a **fixed**  $p$ , the number of solutions is

$$a_p b_q \quad (\text{this happens to be 0 or 1, but it's not important})$$

Now, letting  $p$  run from 0 to  $n$ , by the [Sum Rule](#), the number is given by the sequence

$$u_n = \sum_{p=0}^n a_p b_{n-p}$$

with the generating function

$$U(x) = A(x)B(x) = x^5(1 + x + x^2 + x^3)^2,$$

*cf.* (17.1)!

**Example 17.5** (continued). Now, let us make it less trivial and throw in a third variable:

$$\begin{aligned} e_1 + e_2 + e_3 &= n, & e_1, e_2, e_3 &\in \mathbb{Z}, \\ 2 \leq e_1 \leq 5, & 3 \leq e_2 \leq 6, & 4 \leq e_3 \leq 7. \end{aligned}$$

Let us use some sort of induction (or recursion) and, as above, “break” the equation into two:

$$e_1 + e_2 = p, \quad e_3 = q, \quad p + q = n.$$

The number of solutions to the first equation, by the previous example, is given by the sequence  $u_n$  about which, for the moment, we know only its generating function

$$U(x) = x^5(1 + x + x^2 + x^3)^2.$$

The number of solutions to the second one is given by

$$c_q: 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, \dots$$

with the generating function (as above)

$$C(x) = x^4 + x^5 + x^6 + x^7 = x^4(1 + x + x^2 + x^3).$$

Hence, arguing as above, solutions to our original equation are counted by the sequence

$$v_n = \sum_{p=0}^n u_p c_{n-p}$$

with the generating function

$$(17.6) \quad V(x) = U(x)C(x) = A(x)B(x)C(x) = x^9(1 + x + x^2 + x^3)^3.$$

And **this is the answer!** If, say, I want to find  $v_{17}$ , I would just say that it is the coefficient of  $x^{17}$  in (17.6)!

**Remark 17.7.** A few comments are due.

- (1) I do not claim that it easy to use (17.6) to find the precise numeric value of  $u_n$  for any given  $n$ . In fact, computing this coefficient is essentially the same as counting, one-by-one, the solutions to the equation! However, for some questions, the answer in terms of generating functions is more than enough, or even preferred!
- (2) You may guess (and further examples will confirm) that the main difficulty is in the **upper bounds** on the variables: they make the generating functions **polynomials** rather than power series. Strange as it seems, manipulating power series (at least those that we know) is **much easier**, as they are “more regular.”
- (3) One (although not the most important) advantage of the answer in terms of generating functions (especially if we cannot do better) becomes apparent when you want to use the power of a computer algebra system like **Maple**. It is not easy to explain it to **Maple** that you want to count solutions to an equation! You will have to write a couple of nested cycles and actually count them, *e.g.*,

```
count := 0;
for e1 from 2 to 5 do
  for e2 from 3 to 6 do
    for e3 from 4 to 7 do
      if e1 + e2 + e3 = 17 then count := count + 1; fi;
    od;
  od;
od;
```

This will be fast, but *after you have done the programming!* However, if you have the answer in the form of (17.6), this is done by a single standard command:

```
coeff(x^9*(1 + x + x^2 + x^3)^3, x, 17);
```

3

(And this is no longer our problem that **Maple** would have to do essentially the same counting internally! :)

**Example 17.8** (power series are easier!). Just to illustrate this claim, let us solve a known standard problem: count the solutions to the equation

$$e_1 + e_2 + \dots + e_r = n, \quad e_i \in \mathbb{Z}, \quad e_i \geq 0.$$

(I have to change the notation as I want this as a “function” of  $n$ , *i.e.*, a sequence  $a_n$ , with the number  $r$  of variables fixed.)

*Solution:* This time, each variable can take all values  $0, 1, 2, 3, \dots$ , and the “corresponding” generating function is

$$(17.9) \quad f(x) = 1 + x + x^2 + x^3 + \dots = \sum_{n=0}^{\infty} x^n = \frac{1}{1-x}.$$

Arguing as before, the generating function  $A(x)$  for our sequence  $a_n$  is obtained by multiplying  $r$  copies (one for each variable) of  $f(x)$ :

$$A(x) = [f(x)]^r = \frac{1}{(1-x)^r} = \sum_{n=0}^{\infty} \binom{r+n-1}{n} x^n,$$

see (16.20). Therefore,

$$a_n = \binom{r+n-1}{n} = C(r+n-1, n) = C(r+n-1, r-1),$$

as we know very well!

**Remark 17.10.** And, again, the power of the method is that, *once you got the idea*, you obtain the answer **automatically**, without a single extra thought!

**Example 17.11** (combinations with repetitions). As we know, the last example is related to combinations with repetitions. Can we do it directly in that language? yes, we can!

Let  $G_r(x)$  be the generating function for the sequence  $a_n$  counting the combinations of  $n$  out of  $r$  objects, *with repetitions allowed*. I will show by induction (in  $r$ ) that

$$G_r(x) = [G_1(x)]^r = \frac{1}{(1-x)^r} = \sum_{n=0}^{\infty} \binom{r+n-1}{n} x^n.$$

*Basic step*: for each  $n \geq 0$ , there is **one** way to select  $n$  copies **of the same object**; therefore, the sequence is

$$a_n = 1: 1, 1, 1, 1, 1, \dots \quad \text{and} \quad G_1(x) = \sum_{n=0}^{\infty} x^n = \frac{1}{1-x}. \quad \checkmark$$

*Inductive step*: to select  $n$  out of  $(r+1)$  object, we can select  $0 \leq p \leq n$  out of the first  $r$  objects, and then we have to make the remaining  $q := n-p$  the remaining  $(r+1)$ -st object. As above, this count corresponds to the multiplication of the respective generating functions:

$$G_{r+1}(x) = G_r(x)G_1(x) \stackrel{\text{IH}}{=} [G_1(x)]^r G_1(x) = [G_1(x)]^{r+1} = \frac{1}{(1-x)^{r+1}}. \quad \checkmark$$

**Example 17.12** (ordinary combinations). We can stretch the idea and count ordinary (without repetitions) combinations of  $n$  out of  $N$  elements. This is the same as counting solutions to

$$e_1 + e_2 + \dots + e_N = n, \quad e_i \in \{0, 1\}.$$

Here, each variable  $e_i$  takes value 0 (the  $i$ -th element is not chosen) or 1 (the  $i$ -th element is chosen). The total number of 1's should equal  $n$ , as  $n$  elements are chosen altogether; hence, the equation.

Hence, the generating function “corresponding” to each variable is

$$G_i(x) = x^0 + x^1 = 1 + x,$$

and their product (there are  $N$  copies of this) is

$$G(x) = \overbrace{G_1(x) \cdot \dots \cdot G_N(x)}^{N \text{ factors}} = (1+x)^N = \sum_{n=0}^N \binom{N}{n} x^n.$$

**Example 17.13** (for this, we will have **no other method**). Find the number  $a_n$  of solutions to the equation

$$e_1 + 2e_2 + 5e_3 = n, \quad e_i \in \mathbb{N}.$$

*Solution:* We can make a change of variables

$$y_1 = e_1, \quad y_2 = 2e_2, \quad y_3 = 5e_3$$

to make it look more familiar,

$$y_1 + y_2 + y_3 = n,$$

as before. However, this time  $y_i$  are not just natural numbers, but they also take values in certain restricted sets! Namely,

$$\begin{aligned} y_1 &\in \{0, 1, 2, 3, \dots\}, & G_1(x) &= 1 + x^1 + x^2 + x^3 + \dots = \frac{1}{1-x}, \\ y_2 &\in \{0, 2, 4, 6, \dots\}, & G_2(x) &= 1 + x^2 + x^4 + x^6 + \dots = \frac{1}{1-x^2}, \\ y_3 &\in \{0, 5, 10, 15, \dots\}, & G_3(x) &= 1 + x^5 + x^{10} + x^{15} + \dots = \frac{1}{1-x^5}. \end{aligned}$$

The “corresponding” generating functions are written according to the values taken by each variable. Now, our general paradigm suggests that these functions are to be multiplied, *i.e.*, the generating function for  $a_n$  is

$$(17.14) \quad G(x) = G_1(x)G_2(x)G_3(x) = \frac{1}{(1-x)(1-x^2)(1-x^5)}.$$

**Remark 17.15.** There is a way, using partial fractions (as in Calculus) and working with complex numbers, to reduce (17.14) to the sum of a bunch of binomial series and come up with a “closed formula.” (Simpler examples will be worked out later.) However, we will leave it as is.

**Example 17.16 (non-trivial!!!).** How many ways are there to pay an amount of  $n$ \$ with 1\$, 2\$, and 5\$ coins if

- (1) the order of coins does not matter?
- (2) the order does matter?

*Solution:* *Case (1).* This is just [Example 17.13](#): all that matters are the numbers  $e_1, e_2, e_3$  of the coins of each denomination, and these numbers must sum up to  $n$ .

*Case (2).* This one is **completely different!** First, let us count the number of ways to pay  $n$ \$ with **exactly**  $r$  ordered coins. We count the solutions to the equation

$$e_1 + e_2 + \dots + e_r = n, \quad e_i \in \{1, 2, 5\};$$

this time,  $e_i$  is the *denomination* of the  $i$ -th coin. As in [Example 17.12](#), the generating function for the corresponding sequence is

$$G_r(x) = \overbrace{(x^1 + x^2 + x^5)}^{\text{values of } e_i}{}^r$$

Now, by the [Sum Rule](#), we need to **sum up** over  $r = 0, 1, 2, \dots$ :

$$G(x) = 1 + (x + x^2 + x^5) + (x + x^2 + x^5)^2 + \dots = \frac{1}{1 - (x + x^2 + x^5)}.$$

Do not overlook the first term: the number of ways to pay  $n$ \$ with **0** coins is given by the sequence  $1, 0, 0, 0, \dots$  with the generating function

$$1 = (x + x^2 + x^5)^0.$$

**Remark 17.17.** Judging by the look of the last expression, the sequence in question must be subject to a *linear homogeneous recurrence relation of degree five*. Can you find this relation?

*Solution:* Take the last coin out. If it is a 1\$, the rest pays a sum of  $(n - 1)$ \$. Likewise, if the last coin is 2\$ or 5\$, the rest pays  $(n - 2)$ \$ or  $(n - 5)$ \$, respectively. By the [Sum Rule](#),

$$a_n = a_{n-1} + a_{n-2} + a_{n-5}.$$

By trial and error,

$$a_0 = a_1 = 1, \quad a_2 = 2, \quad a_3 = 3, \quad a_4 = 5.$$

For the last two values, we have

$$3 = 1 + 2 = 2 + 1 = 1 + 1 + 1,$$

$$4 = 2 + 2 = 2 + 1 + 1 = 1 + 2 + 1 = 1 + 1 + 2 = 1 + 1 + 1 + 1.$$

Solving this recurrence relation *via* generating functions (see the next section), we would arrive at the same expression.

**Knowing the answer** to Part (1), one can probably write down (and even “explain”) a recurrence relation for that sequence as well (same as in [Example 17.13](#)). It should be of degree eight, with the characteristic equation

$$(r - 1)(r^2 - 1)(r^5 - 1) = 0$$

(or else something non-homogeneous of lower degree). Try this at home!

This can be written as sum of five **very ugly** geometric progressions, using complex numbers!

## 18. Generating functions and recurrence relations

I will do but one example. This approach applies to any linear recurrence relation with constant coefficients (homogeneous or not), *provided that you know the generating function for the free term  $F(n)$ .*

**Example 18.1.** Solve the recurrence relation

$$a_0 = 1, \quad a_n = 8a_{n-1} + 10^{n-1}.$$

Here, by “solve” we understand “find the generating function for  $a_n$ .” We denote this **unknown** (for now) function by

$$(18.2) \quad G(x) = a_0 + a_1x^1 + a_2x^2 + a_3x^3 + \dots$$

*Solution:* We multiply the recurrence relation by  $x^n$  and sum up over all  $1 \leq n < \infty$ . (We start from  $n = 1$  because we have  $a_{n-1}$  involved, which would not make sense for  $n = 0$ . A degree 2 relation would be summed up over  $n \geq 2$ , etc.)

$$\sum_{n=1}^{\infty} a_n x^n = \sum_{n=1}^{\infty} 8a_{n-1} x^n + \sum_{n=1}^{\infty} 10^{n-1} x^n$$

Let me spell this out:

$$\begin{aligned} a_1 x^1 &= 8a_0 x^1 + 10^0 x^1, \\ a_2 x^2 &= 8a_1 x^2 + 10^1 x^2, \\ a_3 x^3 &= 8a_2 x^3 + 10^2 x^3, \\ a_4 x^4 &= 8a_3 x^4 + 10^3 x^4, \\ a_5 x^5 &= 8a_4 x^5 + 10^4 x^5, \\ &\dots \end{aligned}$$

---


$$G(x) - 1 = 8xG(x) + \frac{x}{1 - 10x}.$$

Be careful: everything is more or less clear, but there are certain “border artifacts”:

- the first column is  $G(x)$  **with one term  $a_0 = 1$  missing**;
- the second column is  $8G(x)$  **multiplied by an extra  $x$** ;
- the third column, in spite of its looks, is the geometric series

$$\frac{1}{10}(1 + 10x + 10^2x^2 + \dots) = \frac{1}{10} \cdot \frac{1}{1 - 10x},$$

*i.e.*, the generating function for  $F(n) = 10^{n-1}$ , **with the first term  $1/10$  missing**.

And now, the unknown function  $G$  is found from the equation

$$G - 1 = 8xG + \frac{x}{1 - 10x}.$$

Collecting  $G$  on one side and the rest, on the other,

$$(1 - 8x)G = 1 + \frac{x}{1 - 10x}, \quad \text{or} \quad G(x) = \frac{1 - 9x}{(1 - 8x)(1 - 10x)}.$$

Once again, here, **the unknown is  $G$** , and, if you've done everything right, this equation must be **linear in  $G$** :

$$(\text{something})G = (\text{something}), \quad \text{hence} \quad G = \frac{(\text{something})}{(\text{something})}.$$

Note also that **the initial data have already been automatically incorporated in this solution**: we used them when saying that the missing term  $a_0$  equals 1.

What do we do next? We proceed as in Calculus, decomposing  $G$  into partial fractions. (And for the same reason: we cannot integrate products  $\int uv \, dx$ , but we can easily integrate sums  $\int (u+v) \, dx$ ; likewise, it is difficult to multiply power series, but it is easy to add them!)

Thus, in this case, we should be able to find  $A, B$  such that

$$G(x) = \frac{1-9x}{(1-8x)(1-10x)} = \frac{A}{1-8x} + \frac{B}{1-10x}.$$

Clearing the denominators:

$$1-9x = A(1-10x) + B(1-8x)$$

and equating similar terms:

$$1 = A + B, \quad -9 = -10A - 8B,$$

we find  $A = B = \frac{1}{2}$ . Hence,

$$G(x) = \frac{1}{2} \frac{1}{1-8x} + \frac{1}{2} \frac{1}{1-10x} = \sum_{n=0}^{\infty} \underbrace{\left( \frac{1}{2} 8^n + \frac{1}{2} 10^n \right)}_{\text{this is } a_n} x^n.$$

**Example 18.3** (Fibonacci again). Just to illustrate what happens in the summation, let us do Fibonacci:

$$a_0 = 0, \quad a_1 = 1, \quad a_n = a_{n-1} + a_{n-2}.$$

Here we go, summing up over  $n \geq 2$ :

$$\sum_{n=2}^{\infty} a_n x^n = \sum_{n=2}^{\infty} a_{n-1} x^n + \sum_{n=2}^{\infty} a_{n-2} x^n$$

Let me spell this out:

$$\begin{aligned} a_2 x^2 &= a_1 x^2 + a_0 x^2, \\ a_3 x^3 &= a_2 x^3 + a_1 x^3, \\ a_4 x^4 &= a_3 x^4 + a_2 x^4, \\ a_5 x^5 &= a_4 x^5 + a_3 x^5, \\ a_6 x^6 &= a_5 x^6 + a_4 x^6, \\ &\dots \end{aligned}$$

---


$$G(x) - a_0 - a_1 x = x(G(x) - a_0) + x^2 G(x).$$

Pay close attention to the **missing terms** and to the fact that these terms are **given by the initial data**! Using  $a_0 = 0$  and  $a_1 = 1$ ,

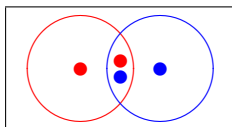
$$G - x = xG + x^2 G, \quad (1 - x - x^2)G = x, \quad G = \frac{x}{1 - x - x^2}$$

(**linear** equation in  $G$ ).

Refer to your  
Calculus textbook,  
Partial fractions,  
for the details

The denominator  
is, essentially, the  
characteristic  
equation (read  
“backwards”).  
This is not an  
accident!

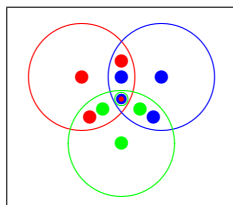
## 19. The principle of inclusion/exclusion



The case of two sets:

We know this as the **Subtraction Rule**.

$$|A \cup B| = |A| + |B| - \underbrace{|A \cap B|}_{\times 2}.$$



The case of three sets:

$$\begin{aligned} |A \cup B \cup C| &= |A| + |B| + |C| - \underbrace{|A \cap B|}_{\times 2} - \underbrace{|A \cap C|}_{\times 2} - \underbrace{|B \cap C|}_{\times 2} + \underbrace{|A \cap B \cap C|}_{\times 3} \end{aligned}$$

**Example 19.1.** How many integers  $1 \leq n \leq 1000$  are divisible by 5, 7, or 11?

*Solution:* The sets involved are

$$\begin{aligned} A &= \{\text{integers divisible by } 5\}, \\ B &= \{\text{integers divisible by } 7\}, \\ C &= \{\text{integers divisible by } 11\}, \\ A \cap B &= \{\text{integers divisible by } 5 \cdot 7 = 35\}, \\ A \cap C &= \{\text{integers divisible by } 5 \cdot 11 = 55\}, \\ B \cap C &= \{\text{integers divisible by } 7 \cdot 11 = 77\}, \\ A \cap B \cap C &= \{\text{integers divisible by } 5 \cdot 7 \cdot 11 = 385\}. \end{aligned}$$

Since the number of integers  $1 \leq n \leq 1000$  divisible by  $m$  is  $\lfloor 1000/m \rfloor$ , we obtain

$$\begin{aligned} \# \text{ in question} &= \left\lfloor \frac{1000}{5} \right\rfloor + \left\lfloor \frac{1000}{7} \right\rfloor + \left\lfloor \frac{1000}{11} \right\rfloor \\ &\quad - \left\lfloor \frac{1000}{35} \right\rfloor - \left\lfloor \frac{1000}{55} \right\rfloor - \left\lfloor \frac{1000}{77} \right\rfloor \\ &\quad + \left\lfloor \frac{1000}{385} \right\rfloor \\ &= 200 + 142 + 90 - 28 - 18 - 12 + 2 \\ &= \boxed{376}. \end{aligned}$$

**Theorem 19.2.** For  $n$  sets  $A_1, \dots, A_n$ , we have

We include the  
sets, exclude  
double  
intersections,  
include triple  
intersections,  
exclude quadruple,  
etc.

$$\begin{aligned}
 \left| \bigcup_{i=1}^n A_i \right| &= \underbrace{|A_1 \cup \dots \cup A_n|}_{\text{we want } 1 = C(r, 0)} \\
 &= \underbrace{\sum_{1 \leq i \leq n} |A_i|}_{r=C(r,1)} - \underbrace{\sum_{1 \leq i < j \leq n} |A_i \cap A_j|}_{C(r,2)} + \underbrace{\sum_{1 \leq i < j < k \leq n} |A_i \cap A_j \cap A_k|}_{C(r,3)} + \dots \\
 &\quad + (-1)^{r+1} \underbrace{\sum_{1 \leq i_1 < \dots < i_r \leq n} |A_{i_1} \cap \dots \cap A_{i_r}|}_{1=C(r,r)} + \dots \\
 &\quad + (-1)^{n-1} \underbrace{|A_1 \cap \dots \cap A_n|}_{0 \text{ (if } r < n)}.
 \end{aligned}$$

*Proof.* Assume that an element  $a$  is contained in **exactly**  $r \leq n$  sets, say,  $A_1, \dots, A_r$ , and let us see how many times it is counted in the left hand side. (The counts are shown in the formula.) We get

$$C(r, 1) - C(r, 2) + C(r, 3) - \dots + (-1)^{r-1} C(r, r),$$

and we want this to be equal to 1 **if**  $r \geq 1$  (each point **contained in at least one of the sets** must be counted once) or 0 **if**  $r = 0$  (points **not contained in any of the sets** should not be counted). But that is one of our formulas (see [Corollary 4.7](#)):

$$\underbrace{C(r, 0)}_{\text{this is 1}} - \overbrace{\left( C(r, 1) - C(r, 2) + \dots + (-1)^{r-1} C(r, r) \right)}^{\text{I have changed the signs here}} = \begin{cases} 0, & \text{if } r \geq 1, \\ 1, & \text{if } r = 0. \end{cases}$$

this is the count in the RHS

That is, the right hand side sums up to 1, if  $r \geq 1$ , or 0, if  $r = 0$ .  $\square$

**Example 19.3.** Already for four sets, this is quite ugly:

$$\begin{aligned}
 |A \cup B \cup C \cup D| &= \\
 &+ |A| + |B| + |C| + |D| \\
 &- |A \cap B| - |A \cap C| - |A \cap D| - |B \cap C| - |B \cap D| - |C \cap D| \\
 &+ |A \cap B \cap C| + |A \cap B \cap D| + |A \cap C \cap D| + |B \cap C \cap D| \\
 &- |A \cap B \cap C \cap D|.
 \end{aligned}$$

Thus, usually we hope that either things are quite “regular” (e.g., all  $k$ -fold intersections have the same cardinality, depending only on  $k$ ) or, else, that most intersections are empty for “obvious” reasons.

## 20. An alternative form

Typically, we use a slightly different form of [Theorem 19.2](#). Assume that we have a certain *universe*  $U$  and a number of *conditions*  $P_1, \dots, P_n$  which we do **not** want satisfied! That is, we want to find the number

$$N(\bar{P}_1 \dots \bar{P}_n)$$

of elements  $x \in U$  that do **not** satisfy **any** of the conditions. Instead, as usual, we count **bad** elements, *i.e.*, those satisfying **at least one** of the conditions. We introduce the sets

$$A_i := \{x \in U \mid P_i(x) \text{ holds}\},$$

$$A_i \cap A_j \cap \dots \cap A_k := \{x \in U \mid P_i(x), P_j(x), \dots, P_k(x) \text{ all hold}\}$$

and denote their cardinalities by

$$N(P_i P_j \dots P_k) := \#\{x \in U \text{ satisfying (at least) } P_i, P_j, \dots, P_k\}.$$

Then, combining [Theorem 19.2](#) and the [Subtraction Rule](#),

$$(20.1) \quad N(\bar{P}_1 \dots \bar{P}_n) = N - \sum_{1 \leq i \leq n} N(P_i) + \sum_{1 \leq i < j \leq n} N(P_i P_j) \\ - \sum_{1 \leq i < j < k \leq n} N(P_i P_j P_k) + \dots + (-1)^n N(P_1 \dots P_n).$$

**Example 20.2.** For three conditions  $P_1, P_2, P_3$  the formula would read

$$(20.3) \quad N(\bar{P}_1 \bar{P}_2 \bar{P}_3) = N - N(P_1) - N(P_2) - N(P_3) \\ + N(P_1 P_2) + N(P_1 P_3) + N(P_2 P_3) - N(P_1 P_2 P_3).$$

**Example 20.4.** Find the number of integer solutions to

$$x_1 + x_2 + x_3 = 11, \quad 0 \leq x_1 \leq 3, \quad 0 \leq x_2 \leq 4, \quad 0 \leq x_3 \leq 6.$$

*Solution:* Our “bad” conditions are

$$P_1: x_1 \geq 4, \quad P_2: x_2 \geq 5, \quad P_3: x_3 \geq 7.$$

Indeed, “ $P_1$  fails” means that  $x_1 < 4$ , or  $x_1 \leq 3$ , *etc.* Thus, we want **all three conditions** to **fail**! Then, by (20.3),

$$\begin{aligned} +N &= \#\{\text{all solutions}\} = C(3 + 11 - 1, 11) = 78, \\ -N(P_1) &= \#\{\text{solutions w/ } x_1 \geq 4\} = C(3 + 7 - 1, 7) = 36, \\ -N(P_2) &= \#\{\text{solutions w/ } x_2 \geq 5\} = C(3 + 6 - 1, 6) = 28, \\ -N(P_3) &= \#\{\text{solutions w/ } x_3 \geq 7\} = C(3 + 4 - 1, 4) = 15, \\ +N(P_1 P_2) &= \#\{\text{solutions w/ } x_1 \geq 4, x_2 \geq 5\} = C(3 + 2 - 1, 2) = 6, \\ +N(P_1 P_3) &= \#\{\text{solutions w/ } x_1 \geq 4, x_3 \geq 7\} = C(3 + 0 - 1, 0) = 1, \\ +N(P_2 P_3) &= \#\{\text{solutions w/ } x_2 \geq 5, x_3 \geq 7\} = 0, \\ -N(P_1 P_2 P_3) &= \#\{\text{solutions w/ } x_1 \geq 4, x_2 \geq 5, x_3 \geq 7\} = 0, \end{aligned}$$

In other words, we want that **all conditions fail**!

Remember, we need **non-strict** inequalities

The standard “*shift down to 0*” techniques

---

This is what we want:  $N(\bar{P}_1 \bar{P}_2 \bar{P}_3) = 78 - 36 - 28 - 15 + 6 + 1 + 0 - 0 = \boxed{6}.$

## 21. Applications of inclusion/exclusion

**21.1. The sieve of Eratosthenes.** If we want to count the number of primes up to  $n$ , it suffices to know all primes up to  $\sqrt{n}$ . Though, if there are too many of them, the computation is likely to get out of hand.

**Example 21.1.** How many primes  $p \leq 100$  are there?

*Solution:* A number  $p \leq 100$  is a prime if and only if it has no prime divisor  $d \leq \sqrt{100} = 10$ . In other words,  $p$  should not be divisible by any of 2, 3, 5, or 7. Therefore, these are our “bad” conditions:

$$P_1(x): 2 \mid x, \quad P_2(x): 3 \mid x, \quad P_3(x): 5 \mid x, \quad P_4(x): 7 \mid x.$$

Since the factors are prime (and thus pairwise coprime), combinations of these conditions mean the divisibility by the respective product, *e.g.*,

$$P_1(x) \& P_3(x): (2 \cdot 5) \mid x \text{ or, equivalently, } 10 \mid x.$$

Therefore, the number of integers  $p \leq 100$  **not** divisible by any of 2, 3, 5, or 7 is given by (20.1) as

$$\begin{aligned} \# &= 100 \\ &- \left\lfloor \frac{100}{2} \right\rfloor - \left\lfloor \frac{100}{3} \right\rfloor - \left\lfloor \frac{100}{5} \right\rfloor - \left\lfloor \frac{100}{7} \right\rfloor \\ &+ \left\lfloor \frac{100}{2 \cdot 3} \right\rfloor + \left\lfloor \frac{100}{2 \cdot 5} \right\rfloor + \left\lfloor \frac{100}{2 \cdot 7} \right\rfloor + \left\lfloor \frac{100}{3 \cdot 5} \right\rfloor + \left\lfloor \frac{100}{3 \cdot 7} \right\rfloor + \left\lfloor \frac{100}{5 \cdot 7} \right\rfloor \\ &- \left\lfloor \frac{100}{2 \cdot 3 \cdot 5} \right\rfloor - \left\lfloor \frac{100}{2 \cdot 3 \cdot 7} \right\rfloor - \left\lfloor \frac{100}{2 \cdot 5 \cdot 7} \right\rfloor - \left\lfloor \frac{100}{3 \cdot 5 \cdot 7} \right\rfloor \\ &+ \left\lfloor \frac{100}{2 \cdot 3 \cdot 5 \cdot 7} \right\rfloor \\ &= 100 - 50 - 33 - 20 - 14 + 16 + 10 + 7 + 6 + 4 + 2 \\ &\quad - 3 - 2 - 1 - 0 + 0 \\ &= 22. \end{aligned}$$

However, *this is not quite the answer to our original problem yet*: this count excludes the original four primes 2, 3, 5, and 7 and, on the other hand, it includes 1, which is not regarded as prime. Therefore, we must add 4 and subtract 1:

$$\#\{\text{primes } p \leq 100\} = 22 + 4 - 1 = \boxed{25}.$$

**21.2. The Stirling numbers.** Let  $A$  be an  $m$ -element set and  $B$ , an  $n$ -element set. Now, we can count the number of surjections  $f: A \twoheadrightarrow B$ . Of course, we can assume that  $B = \{1, 2, \dots, n\}$ . Introduce the “bad” conditions as

$$P_i(f): \text{ the image of } f \text{ misses the point } i \in B, \quad 1 \leq i \leq n.$$

Thus, we are speaking about the functions

$$\begin{aligned} \text{all: } f: A &\rightarrow \underbrace{B}_{n \text{ elements}}, & N &= (n-0)^m, \\ P_i: f: A &\rightarrow \underbrace{B - \{i\}}_{n-1 \text{ elements}}, & N(P_i) &= (n-1)^m, \\ P_i \& P_j: f: A &\rightarrow \underbrace{B - \{i, j\}}_{n-2 \text{ elements}}, & N(P_i P_j) &= (n-2)^m, \\ P_{i_1} \& \dots \& P_{i_r}: f: A &\rightarrow \underbrace{B - \{i_1, \dots, i_r\}}_{n-r \text{ elements}}, & N(P_{i_1} \dots P_{i_r}) &= (n-r)^m. \end{aligned}$$

This is an example of a “regular” situation, where the intersection count  $N(P_{i_1} \dots P_{i_r})$  depends on the number  $r$  of the subsets only, but does not depend on the subsets themselves. Since the number of unordered  $r$ -tuples  $\{i_1, \dots, i_r\} \subset B$  equals  $C(m, r)$ , we arrive at the following count of the number of surjections.

**Theorem 21.2.** *If  $|A| = m$  and  $|B| = n$ , then*

$$\begin{aligned} \#\{f: A \twoheadrightarrow B\} &= C(n, 0)n^m - C(n, 1)(n-1)^m + C(n, 2)(n-2)^m + \dots \\ &\quad + (-1)^{n-1}C(n, n-1) \cdot 1^m + (-1)^n C(n, n) \cdot 0^m \\ &= \sum_{r=0}^n (-1)^r \binom{n}{r} (n-r)^m. \end{aligned}$$

(You can run the summation to  $n$  or to  $(n-1)$ : this does not matter since the last term  $\pm 0^m$  vanishes anyway.)

Recall that what we obtained counts the number of ways to put  $m$  distinguishable objects (the elements of  $A$ ) into  $n$  distinguishable boxes (the elements of  $B$ ) **so that none is left empty**. However, if none of the boxes is empty, they are automatically intrinsically distinguishable (by the objects they contain); hence, there are  $n!$  ways to relabel them. Hence, the number above is divisible by  $n!$  (which is far from obvious from the formula), and *the number of ways to put  $m$  distinguishable objects into  $n$  undistinguishable boxes so that none is left empty* is given by the so-called *Stirling number of the second kind*

$$S(m, n) = \frac{1}{n!} \sum_{r=0}^n (-1)^r \binom{n}{r} (n-r)^m.$$

In this notation,

$$\#\{f: A \rightarrow B\} = n! \cdot S(m, n).$$

**Example 21.3.** It is not very easy to compute Stirling numbers using the formula. Here are a few examples using *combinatorial arguments* (*aka* common sense):

$$\begin{aligned} S(m, 0) &= 0 && \text{(cannot put objects to zero boxes),} \\ S(m, 1) &= 1 && \text{(everyone goes to the only box),} \\ S(m, 2) &= 2^{m-1} - 1 && \text{(pairs } \emptyset \neq S \subsetneq A, A - S), \\ &&& \dots\dots\dots \\ S(m, m-1) &= C(m, 2) && \text{(two objects share a box),} \\ S(m, m) &= 1 && \text{(each object to a separate box),} \\ S(m, n) &= 0 && \text{if } n > m \text{ (there must be empty boxes).} \end{aligned}$$

As you can see, these numbers are **far from symmetric**.

**21.3. Derangements.** A *derangement* is an arrangement (*aka* permutation) that **moves every single element**. For example:

$$(2, 4, 1, 3) \text{ good}, \quad (3, 2, 4, 1) \text{ bad}.$$

The derangements of the 3-element set  $\{1, 2, 3\}$  are

$$(2, 3, 1), \quad (3, 1, 2);$$

two out of the total of six permutations! There are nine (out of 24) derangements of the 4-element set  $\{1, 2, 3, 4\}$ :

$$(4, 1, 2, 3), \quad (3, 4, 1, 2), \quad (2, 3, 4, 1), \quad (4, 3, 1, 2), \quad (3, 1, 4, 2), \\ (3, 4, 2, 1), \quad (2, 4, 1, 3), \quad (4, 3, 2, 1), \quad (2, 1, 4, 3).$$

**Theorem 21.4.** *The number of derangements of an  $n$ -element set is*

$$D_n = n! \left[ 1 - \frac{1}{1!} + \frac{1}{2!} - \frac{1}{3!} + \dots + (-1)^n \frac{1}{n!} \right].$$

*Proof.* As usual, we consider all  $N = n!$  permutations and remove that bad ones. The “bad” conditions are

$$P_i: \text{ element } i \text{ is not moved}, \quad 1 \leq i \leq n.$$

As before, the counts  $N(P_{i_1} \dots P_{i_r})$  depend only on the number  $r$  of the conditions:

$$\begin{aligned} N(P_{i_1} \dots P_{i_r}) &= \#\{\text{arrangements fixing } i_1, \dots, i_r\} \\ &= \#\{\text{arrangements of } \underbrace{A - \{i_1, \dots, i_r\}}_{n-r \text{ elements}}\} \\ &= (n-r)!. \end{aligned}$$

Therefore, as before,

$$\begin{aligned} D_n &= \sum_{r=0}^n (-1)^r \binom{n}{r} (n-r)! \\ &= \sum_{r=0}^n (-1)^r \frac{n!}{r! (n-r)!} (n-r)! \\ &= n! \sum_{r=0}^n (-1)^r \frac{1}{r!}, \end{aligned}$$

as stated. □

**CALCULUS!** I hope you all recognize the sum in [Theorem 21.4](#): it is the  $n$ -th partial sum of the series

$$\sum_{r=0}^{\infty} (-1)^r \frac{1}{r!} = e^{-1} = \frac{1}{e} \approx 0.368.$$

It is an *alternating series with decreasing  $r$ -th term*; by the *alternating series test* (aka *Leibniz test*), the error of the approximation of the sum  $1/e$  by a partial sum does not exceed the *first term dropped*, i.e.,

$$\left| \frac{1}{e} - \sum_{r=0}^n (-1)^r \frac{1}{r!} \right| < \frac{1}{(n+1)!}.$$

Multiplying this by  $n!$ , we see that

$$\left| D_n - \frac{n!}{e} \right| < \frac{1}{n+1} \leq \frac{1}{2} \quad \text{whenever } n \geq 1.$$

In other words, for  $n \geq 1$ ,

$$D_n = \text{closest integer to } \frac{n!}{e}.$$

We also see that

$$\frac{D_n}{P(n)} \xrightarrow{n \rightarrow \infty} \frac{1}{e} \quad (\text{quite fast}).$$

The learned term for the left hand side is the *probability of derangement*.

## APPENDIX A. Sample questions

**Example A.1.** Give a combinatorial argument that

$$k \binom{n}{k} = n \binom{n-1}{k-1}.$$

*Solution:* Out of a group of  $n$  people, we select a committee consisting of  $k$  members, one of which as the chair.

*Way 1:* We select the  $k$  members of the committee, in  $C(n, k)$  ways, and, among them, select the chair, in  $k$  ways. This is the **left hand side**.

*Way 2:* out of the  $n$  people, we select the chair, in  $n$  ways, and then select the remaining  $(k-1)$  members of the committee out of the remaining  $(n-1)$  people, in  $C(n-1, k-1)$  ways. This is the **right hand side**.

**Example A.2.** In how many ways can the letters in MATHEMATICS can be arranged:

- (1) if there are no further constraints?
- (2) if there should be no consecutive A's?
- (3) if all four vowels should stay together?

*Solution:* *Case (1).* We are speaking about permutations with indistinguishable objects. Here are the counts:

$$2 \times \text{M}, 2 \times \text{A}, 2 \times \text{T}, 1 \times \text{each of H, E, I, C, S},$$

*i.e.,*

$$n_1 = n_2 = n_3 = 2, \quad n_4 = \dots = n_8 = 1, \quad n = n_1 + \dots + n_8 = 11.$$

Thus, the number of ways is

$$\binom{11}{2, 2, 2, 1, 1, 1, 1, 1} = \frac{11!}{2! \cdot 2! \cdot 2! \cdot 1! \cdot 1! \cdot 1! \cdot 1! \cdot 1!} = \boxed{4989600}.$$

*Case (2).* Count **bad** arrangements instead, *i.e.*, those where the two A's are next to each other. Thus, we replace  $2 \times \text{A}$  with a single letter **AA**, and the number is

$$\binom{10}{2, 2, 1, 1, 1, 1, 1, 1} = \frac{10!}{2! \cdot 2! \cdot 1! \cdot 1! \cdot 1! \cdot 1! \cdot 1! \cdot 1!} = \boxed{907200}.$$

Hence, the number of **good** ones is (by the **Subtraction Rule**)

$$\text{good} = \text{all} - \text{bad} = \frac{11}{2} \frac{10!}{2! \cdot 2!} - \frac{10!}{2! \cdot 2!} = \frac{9 \cdot 10!}{2 \cdot 2! \cdot 2!} = 4082400.$$

*Case (3).* First, we count the **arrangements with a single "letter" AA EI**; then, **rearrange the ingredients of this "letter"**:

$$\binom{8}{2, 2, 1, 1, 1, 1} \binom{4}{2, 1, 1} = \frac{8! \cdot 4!}{2! \cdot 2! \cdot 2!} = \boxed{120960}.$$

**Example A.3.** Find the number of integer solutions to

$$x_1 + x_2 + x_3 + x_4 = 32, \quad x_i \in \mathbb{Z},$$

where

- (1)  $x_1, x_2, x_3, x_4 \geq 0$ ;
- (2)  $x_1, x_2, x_3 > 0, x_4 > 25$ ;
- (3)  $x_1, x_2, x_3 > 0, 0 < x_4 \leq 25$ .

*Solution:* *Case (1).* This is a textbook problem; the number is

$$C(32 + 4 - 1, 4 - 1) = C(35, 3) = \frac{35 \cdot 34 \cdot 33}{1 \cdot 2 \cdot 3} = 35 \cdot 17 \cdot 11 = \boxed{6545}.$$

*Case (2).* To make all inequalities  $\geq 0$ , we make a change of variables

$$y_1 = x_1 - 1, \quad y_2 = x_2 - 1, \quad y_3 = x_3 - 1, \quad y_4 = x_4 - 26.$$

Then,

$$y_1 + y_2 + y_3 + y_4 = 32 - 29 = 3, \quad y_i \geq 0,$$

and the number of solutions is

$$C(3 + 4 - 1, 4 - 1) = C(6, 3) = \boxed{20}.$$

*Case (3).* We do it *via*

$$\text{good} = \text{all} - \text{bad} = 4495 - 20 = \boxed{4475}.$$

where “bad” are given by Case (2) and “all” are the solutions with all  $x_i > 0$ . As above, by a change of variables  $y_i = x_i - 1$  (for all  $i = 1, 2, 3, 4$ ) we count “all” as

$$C(28 + 4 - 1, 4 - 1) = C(31, 3) = 31 \cdot 5 \cdot 29 = 4495.$$

## MARGINAL NOTES

- 1/ 4: *NB*: Normally, there is no need to compute things like this anyway!
- 2/ 4: *NB*: Normally, do not compute this!
- 3/ 4: This trick will be used very often, on various occasions
- 4/ 5: *NB*: we do expect you to compute the combinations of reasonable size, especially if they are used further!
- 5/ 6: *NB*: a popular class of problems!
- 6/ 6: *NB*: this probably should not be computed in the exams
- 7/ 6: Another useful fact!
- 8/ 6: Instead of looking at what's selected, look at what's left. **Or:** repaint black to white and *vice versa*
- 9/ 7: In all such formulas, we let  $x^0 = 1$  no matter what: even  $0^0 = 1$ . Forget Calculus! Or, as in Calculus:  $\lim_{x \rightarrow 0} x^0 = 1$ .
- 10/ 10: Selecting a point is a useful trick! We did this before!
- 11/ 12: *NB*: your textbook insists that  $r \leq m$  and  $r \leq n$ . This is not necessary!
- 12/ 12: This is a very useful trick!
- 13/ 14: Yet another useful trick!
- 14/ 15: Convenient encoding of the objects counted is crucial to most counting problems
- 15/ 17: We use two different encodings of the same set of objects. This trick is extremely important!
- 16/ 20: Explain we the Division Rule does not work here! See Example 11.7
- 17/ 20: Since the order does not matter, we can choose our **favorite order**!
- 18/ 20: This is a very neat trick!
- 19/ 21:  $r = \#(\text{of } * \text{'s}); n - 1 = \#(\text{of } | \text{'s})$
- 20/ 21:  $n = \#(\text{unknowns}); r = \text{RHS}$
- 21/ 21: Make inequalities  $x_i \geq \text{smth}$
- 22/ 21: The RHS's of the constraints
- 23/ 21: Observe the signs!
- 24/ 22: We have  $m + 1$  unknowns, but the RHS is  $r = n - 1$
- 25/ 23: Ordering things that are originally unordered is a useful trick! And this is how combinations are generated: see the "green" code in Example 10.7
- 26/ 23: This example explains how ordinary combinations account for those with repetitions: we just shift the variables by  $-1$ !
- 27/ 24: Homework!
- 28/ 24: Yet another common and useful trick!
- 29/ 26: This is our favorite word! :)
- 30/ 27: Most formulas can be explained in many different ways: typically, there are many ways to count the same set!
- 31/ 28: It is given by Theorem 10.5 as  $C(n + k - 1, n)$
- 32/ 33:  $1/r!$  here is given by the Division Rule: it works if  $r$  is fixed!
- 33/ 35: *NB*: Induction can be thought of as a recursive computation of the truth value with very special "recurrence relation"  $f_{n-1} \Rightarrow f_n$
- 34/ 35: linear homogeneous of degree 2
- 35/ 36: As a homework, try to prove this using the binomial formula. The devil is in the signs!
- 36/ 36: *NB*: very good for midterms!
- 37/ 36: There even is a mathematical journal dedicated solely to Fibonacci numbers!

38/ 37: Someone is playing this game with 64 disks, and the world will end upon completion. How much time do we have left?

39/ 37: linear nonhomogeneous of degree 1

40/ 37: Thus,  $n = 64$  would require  $H_{64} = 2^{64} - 1 = 18,446,744,073,709,551,615$  moves—the famous *chess number*

41/ 37: Yet another illustration of the relation between the two!

42/ 38: linear homogeneous of degree 2

43/ 38: Homework!

44/ 39: linear nonhomogeneous of degree 1

45/ 40: Explain!

46/ 40: In linear algebra, we would say that the dimension of the solution space of (14.1) is  $d$

47/ 41: This is a digression

48/ 41: This is how linearity works!

49/ 41: This is called the *general solution*

50/ 41: *linearly independent* in linear algebra Unknowns are  $X, Y, Z$ . The rest are given numbers!

51/ 41: If you took *differential equation*, this stuff should be easy!

52/ 42: e.g., the solution to  $a_n = 2a_{n-1}$  is obviously  $a_0 \cdot 2^n$

53/ 42: from now on, **this is the rule!**

54/ 42: Two unknowns  $X, Y$ ! The rest is known by now!

55/ 42: To solve, we'll need to **divide** by this!

56/ 42: This is the discrete counterpart of the exponential function  $y = e^{\lambda x}$  solving linear differential equations

57/ 45: Now, **this is the rule!** Just like  $y = xe^{\lambda x}$  in differential equations!

58/ 46: as they do in differential equations

59/ 46: Relax: we will not do this in the future!

60/ 47: You must have seen this in Calculus

61/ 47: This is very similar to the partial fractions in Calculus, is it not?

62/ 49: the discrete counterpart of the so-called *Laplace transform* in differential equations

63/ 51: Here are the two written side by side, so that you can see the correspondence

64/ 52: Can you explain why?

65/ 53: So that later we can find these constants from the initial data

66/ 53: **h** for homogeneous **p** for particular

67/ 53: keep it the **general** solution!

68/ 53: find a **particular** solution!

69/ 53: Now, find a **particular** solution to (15.1)

70/ 54: very much like *partial fractions* in Calculus!

71/ 55: **all** these satisfy  $a_n = 2a_{n-1}$

72/ 55: only **one** of these satisfies  $a_n = 2a_{n-1} + 1$

73/ 55: only **one** satisfies the initial data as well!

74/ 56: **all** these satisfy  $c_n = 2c_{n-1}$

75/ 56: only **one** of these satisfies  $c_n = 2c_{n-1} + 1$

76/ 56: only **one** satisfies the initial data as well!

77/ 57: What is written here is **wrong!**

78/ 61: A very common trick: let  $m = n - 2$

79/ 62: Of course, this holds within a common interval of convergence!

80/ 63: within the interval of convergence **shift**  $m = n - 1$

81/ 64: We will explore this approach to recurrence relations on the regular basis later!

82/ 66: Beware of the sign! It differs from previous formulas with power series!

83/ 67: Remember that we assume **all** powers of  $x$  present! Some may have coefficient 0, **which are part of the sequence!**

84/ 74: This can be written as sum of five **very ugly** geometric progressions, using complex numbers!

85/ 76: Refer to your Calculus textbook, *Partial fractions*, for the details

86/ 76: The denominator is, essentially, the **characteristic equation** (read “backwards”). This is not an accident!

87/ 78: We *include* the sets, *exclude* double intersections, *include* triple intersections, *exclude* quadruple, *etc.*

88/ 79: In other words, we want that **all conditions fail!**

89/ 79: Remember, we need **non-strict** inequalities

90/ 79: The standard “*shift down to 0*” techniques