University of Lund

Lund University

unofficial Lecture Notes for the course

Discrete Mathematics

Course hold by Frank Wikström who kindly agreed for these notes to be published.

Author:
Leon Bernáth

March 30, 2024

Contents

Disclaimer: These are my personal notes for the lecture, so I do not guarantee correctness. If you come across errors, feel free to file an issue.

1 Overview

- First a few lectures (app. two weeks) on **combinatorics**: The art of counting
  - Basic combinatorics
  - Generating functions
  - Recursion
- **Graph theory**
- **Rings and (finite) fields**
- **Coding theory**: take a message and add things such that it is less likely to be corrupted.

2 Basic Combinatorics

The idea is that we want to count things.

2.1 Two basic principles

The first principle is that if we can do it either in one of 10 things this way, or 15 that way, than together there is the sum of those, so $10 + 15 = 25$ possibilities. So if ways are mutually exclusive, we can add the number of them up.

The second principle is the rule of product. Suppose we are at a restaurant and there are 5 possible starters, 6 possible mains and 4 possible desserts. The rule of product says that the total number of three course meals is $5 \cdot 6 \cdot 4 = 120$.

There you can start to see, that combinatorial answers usually get pretty large.[1] People are bad at understanding large numbers, which is also why people play the lottery.

Now change the problem a little bit.
b) How many 1-course (main), 2-course (main+starter or main+dessert), or 3-course meals can you order?

First solution:

- 1-course meals: 6
- main+starter: $5 \cdot 6 = 30$
- main+dessert: $6 \cdot 4 = 24$

[1] For example there are 100! possibilities to sort 100 books, which is a very large number.

- ▶ 3-course: $5 \cdot 6 \cdot 4 = 120$

Since they are mutually exclusive, total is the sum so 180.

Second solution: Add “dummy starter”, “dummy dessert”, so $6 \cdot 6 \cdot 5 = 180$.

2.2 Permutations

Let $\Omega = \{a_1, a_2, \dots, a_n\}$ be a finite set.

For example if $n = 4$ there are $4 \cdot 3 \cdot 2 \cdot 1 = 4!$ possible ways to order this set. The ! is called factorial.[2]

If we just permute 2 of the elements (2-permutation) the total number is $4 \cdot 3 = \frac{4 \cdot 3 \cdot 2 \cdot 1}{2 \cdot 1} = \frac{4!}{(4-2)!}$.

In general for permuting k elements out of n elements we have $\frac{n!}{(n-k)!}$, but to compute this better cancel them out before.

> **Example 2.1 (How many 5 letter “words” can we form from the letters in a) BROWN b) GREEN c) MATHEMATICS.)**
>
> a) $5 \overset{!}{=} 120$
>
> b) If the two “E”s were distinguishable this would be easy and also just be 5!. So lets make them distinguishable, but then we double count. We count every word exactly twice, because you can exchange the “E”s in both words. So the solution is $5!/2 \overset{!}{=} 60$
>
> c) In this case we have $\frac{11!}{2!2!2!}$

2.3 Combinatorics

Let A be a finite set with n elements $|A| = n$.

How many subsets of A with k elements are there?

If we care about order it would be $\frac{n!}{(n-k)!}$

But these can be rearanged in $k!$ ways (and still be the same subset).

So in total there are

$$\binom{n}{k} = \frac{n!}{(n-k)!k!} = C(n,k) = {}^{n}_{k}C \tag{2.1}$$

[2] He does not like the notation ! for the factorial.

different subsets. (One says "n choose k" in english, not n over k,[3] because the ladder mostly means $\frac{n}{k}$.

These are also called binomial coefficients because they are the coefficients of a binomial

$$(a+b)^n = \sum_{k=1}^{n} \binom{n}{k} a^{n-k} b^k \tag{2.2}$$

This is because $(a+b)^n = (a+b)(a+b)\ldots(a+b)$ and at each factor you choose either a or b. So in a non-commutative ring there would be 2^n summands. But using commutativity many factors are the same (e.g. $a^2ba^{n-3} = a^{n-1}b$). All the terms have the order n. But in how many terms the b is chosen exactly k times? It is $\binom{n}{k}$.

From that it also follows that

$$\sum_{k=0}^{n} \binom{n}{k} = 2^n \tag{2.3}$$

Example 2.2 (We have 10 (identical) cookies, and want to distribute them among 4 children.)

The idea is to include 3 lines so in the end there are $\frac{13!}{3!10!}$.

If every child should have at least 1 cookie first hand out one cookie to every child and then do the process with the remaining cookies.

Example 2.3 (How many integer solutions are there to $x_1+x_2+x_3+x_4 = 20$ with $x_1, x_2 \geq 0, x_3 \geq 3, x_4 \geq -1$)

We can solve this by first doing a change of variables $y_1 = x_1, y_2 = x_2, y_3 = x_3 - 3, y_4 = x_4 + 1$ then the new equation is

$$y_1 + y_2 + y_3 + y_4 = x_1 + x_2 + x_3 + x_4 - 2 = 18 \tag{2.4}$$

with $y_k \geq 0$. There then will be $\binom{18+3}{3}$ number of solutions as before.

2.4 Pigeonhole principle

The next thing is in English called the pigeonhole principle. When you have 20 pigeonholes and 21 pigeons then at least one pigeonhole must contain 2 pidgeons.

In general: **Pigeonhole principle:** if you distribute n elements in k containers with $n > k$, then at least one container must contain at least two elements.

Then he took a lot of examples.

[3] In Swedish they say "n över k" as in German, where one says "n über k"

2.5 Counting relations and functions

Definition 2.4:

Let A and B be sets. Then we can form the Cartesian product

$$A \times B = \{(a, b); a \in A, b \in B\} \tag{2.5}$$

Remark 2.5

It holds that if $|A| = n$, $|B = m|$ then $|A \times B| = n \cdot m$.

Definition 2.6:

A relation on A and B is a subset of $A \times B$.

Example 2.7

Familiar example: $A = B = \mathbb{Z}$, $\leq$. Then e.g. $(3, 4) \in \leq$, usually we write $3 \leq 4$.

Let $|A| = n, |B| = m$. How many possible relations on A and B are there?

Proposition 2.8

There are 2^{nm} relations ($= \#$ of subsets) on $A \times B$ if $|A| = n, |B| = m$.

If you want you can try to find the number of equivalence relations. (Those are reflexive, symmetric and transitive.)

How is a function defined?

Definition 2.9:

A function $f : A \to B$ is a relation on A and B, (i.e. a subset of $A \times B$) with the property that $\forall a \in A \exists! b \in B$, s.t. $(a, b) \in f$. Normally, we write $f(a) = b$.

Proposition 2.10

Let A, B be finite sets, with $|A| = n, |B| = m$. How many functions $f : A \to B$ are there?
There are m^n because we have m choices for each of the n elements in A.

Remark 2.11

Let $f : A \to \{1, 0\}$. We can identify a subset $\tilde{A} \subseteq A$ by $f(a) = \begin{cases} 1 & \text{if } a \in \tilde{A} \\ 0 & \text{if } a \notin \tilde{A} \end{cases}$.

> This is the reason that the power set of A, i.e. the set of all subsets of A is often denoted by 2^A.

2.5.1 Injective functions

Definition 2.12 (Injective functions):

$f : A \to B$ is called **injective** if

$$f(a) = f(b) \implies a = b \tag{2.6}$$

(or if you prefer $a \neq b \implies f(a) \neq f(b)$.)

Proposition 2.13

Let A, B be finite sets, $|A| = n, |B| = m$. How many injective functions $f : A \to B$ are there?

If $m < n$ there are no injective functions $A \to B$.

If $m \geq n$, then $f(a_1)$ has m possible values, $f(a_2)$ has $m - 1$ possible values. ...

The total number thus is $\frac{m!}{(m-n)!}$.

2.5.2 The principle of exclusion/inclusion

Proposition 2.14

Let A, B be finite sets, $|A| = n$, $|B| = m$.

$$|A \cup B| = |A| + |B| - |A \cap B|. \tag{2.7}$$

How about three sets?

$$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|. \tag{2.8}$$

More generally:

Proposition 2.15 (The principle of inclusion/exclusion)

More generally:

$$|A_1 \cup A_2 \cup \dots \cup A_n| = \sum_{k=1}^{n} (-1)^{k-1} \sum_{\text{all } k\text{-subsets}\{m_1,\dots,m_k\} \text{ of } \{1,\dots,n\}} \left|A_{m_1} \cap \dots \cap A_{m_k}\right| \tag{2.9}$$

Proof. Let x be in exactly r of the n sets A_i. We will show that x contributes to both sides exactly once. That x contributes to the left side exactly once is obvious. Now the right side.

1. Consider $k = 1$, then we have $+\sum_{\{m_1\} \subseteq \{1,\dots,n\}} \left|A_{m_1}\right| = r$ because x is in exactly one of the sets.
2. Consider $k = 2$, then $x \in A_{m_1} \cap A_{m_2}$ if and only if x is in both of them. There are $\binom{r}{2}$ possible ways to choose two subsets A_{m_1}, A_{m_1} out of them, therefore the contribution of $k = 2$ is equal to $-\binom{r}{2}$
3. Analogously for a general k the contribution is $(-1)^{k-1}\binom{r}{k}$.
4. Therefore the contribution of the whole right side is

$$\sum_{k=1}^{n} (-1)^{k-1} \binom{r}{k} = 1 - \sum_{k=0}^{n} (-1)^{k} \binom{r}{k} = 1 - (1-1)^r = 1. \tag{2.10}$$

□

Example 2.16 (How many integers in $\{1,\dots,100\}$ are not divisible by any of $2, 3, 5$?)

Let's count the complement instead. Let A_k be the set of integers in A that are divisible by k. So:

$$\begin{aligned}
&|A_2 \cup A_3 \cup A_5| && (2.11)\\
&= |A_2| + |A_3| + |A_5| - |A_2 \cap A_3| - |A_2 \cap A_5| - |A_3 \cap A_5| + |A_2 \cap A_3 \cap A_5| && (2.12)\\
&= |A_2| + |A_3| + |A_5| - |A_6| - |A_{10}| - |A_{15}| + |A_{30}| && (2.13)\\
&= \left\lfloor \frac{100}{2} \right\rfloor + \left\lfloor \frac{100}{3} \right\rfloor + \dots && (2.14)\\
&= 50 + 33 + 20 - 16 - 10 - 6 + 3 = 74 && (2.15)
\end{aligned}$$

Hence 26 are not.

Example 2.17

How many permutations of the letters in FRAGMENT do not contain the substrings TAG, ME, MAG.

There are 8! permutations.
How many contain the substring TAG? TAG, F, R, M, E, N so 6!
How many contain the substring ME? 7!
How many contain the substring MAG? 6!

How many contain TAG and ME? 5!
How many contain TAG and MAG? 0
How many contain ME and MAG? 0
How many contain TAG, ME and MAG? 0

Inclusion/Exclusion gives us

$$8! - 6! - 7! - 6! + 5! = 33960 \tag{2.16}$$

As an exercise do the same thing, but start with a word, that has a repeat, or two repeats, while one is in the condition and the other one not.

Example 2.18 (Derangements)

Let us compute the number of permutations of $\{1, \dots, n\}$ without fixpoints, i.e. the number k is never in the kth spot. A derangement is a permutation without a fixed point.

Let A_k be the set of all permutations fixing k.

$$\begin{aligned}|A_1 \cup A_2 \cup \dots \cup A_n| =& |A_1| + |A_2| + \dots + |A_n| && (2.17)\\ &- |A_1 \cap A_2| - |A_1 \cap A_2| - \dots && (2.18)\\ &+ |A_1 \cap A_2 \cap A_3| + |A_1 \cap A_2 \cap A_4| + \dots && (2.19)\\ &- \dots && (2.20)\end{aligned}$$

This is equal to:

$$\binom{n}{1}(n-1)! - \binom{n}{2}(n-2)! + \binom{n}{3}(n-3)! - \dots = n! - \frac{n!}{2!} + \frac{n!}{3!} - \dots = n!\left(1 - \frac{1}{2!} + \frac{1}{3!} - \frac{1}{4!} + \dots\right) \tag{2.21}$$

The total number of derangements is $n!$ minus this, so

$$n!\left(1 - 1 + \frac{1}{2!} - \frac{1}{3!} + \frac{1}{4!} - \dots\right) \approx \frac{n!}{e} \tag{2.22}$$

2.5.3 Counting surjective functions

Definition 2.19 (Surjectivity):

A function $f : A \to B$ is **surjective** if $\forall b \in B, \exists a \in A : f(a) = b$.

Proposition 2.20

Assume A, B are finite, $|A| = m, |B| = n$, $m \geq n$.

$$A = \{a_1, a_2, \dots, a_n\}, B = \{b_1, b_2, \dots, b_n\} \tag{2.23}$$

How many surjective functions $f : A \to B$ are there?

Let $X_j = \{f : A \to B, b_j \notin f(A)\}$.

Note: f is surjektive iff $f \notin X_1 \cup \dots \cup X_n$.

$$\begin{aligned} |X_1 \cup X_2 \cup \dots \cup X_n| =& |X_1| + |X_2| + \dots + |X_n| && (2.24)\\ & - |X_1 \cap X_2| - |X_1 \cap X_2| - \dots && (2.25)\\ & + |X_1 \cap X_2 \cap X_3| + |X_1 \cap X_2 \cap X_4| + \dots && (2.26)\\ & - \dots && (2.27)\\ & = \binom{n}{1}(n-1)^m - \binom{n}{2}(n-2)^n + \binom{n}{3}(n-3)^m - \dots && (2.28) \end{aligned}$$

So the total number of surjections is

$$\binom{n}{0}n^m - \binom{n}{1}(n-1)^m + \binom{n}{2}(n-2)^n - \binom{n}{3}(n-3)^m + \dots = \sum_{k=0}^{n}(-1)^k \binom{n}{k}(n-k)^m \tag{2.29}$$

Proposition 2.21

Distribute m distinct object in n identical container, leaving no container empty. Or: In how many ways can we write $\{1, 2, \dots, m\}$ as a union of n non-empty subsets?

Solution: If the containers are distinct, this is the same as counting the number of surjective functions from $\{1, \dots, m\} \to \{1, \dots, n\}$.
But we can rearrange the containers in $n!$ ways, so the number we're looking for

is

$$\frac{1}{n!}\#\,(\text{surjections}) = \frac{1}{n!}\sum_{k=0}^{n}(-1)^k\binom{n}{k}(n-k)^m \tag{2.30}$$

These are called Stirling numbers (of the second kind) and denoted by

$$S(m,n) = \left\{ \begin{matrix} m \\ n \end{matrix} \right\}. \tag{2.31}$$

Example 2.22
Exercise: Give a combinatorial proof of

$$S(m+1,n) = S(m,n-1) + nS(m,n) \tag{2.32}$$

Solution: If we have one object more to distribute, such that no container is left empty, there is the possibility that either even without the extra object none of the containers were empty, which is the case in $S(m,n)$ cases. Then we can put the extra object in each of the n containers, hence the $nS(m,n)$ term. If before, one container was empty then the extra object must go into this container and for the others, there are $S(m,n-1)$ possibilities, that this is the case.

3 Generating functions

3.1 Motivating example

Motivating example: In how many ways can we distribute 8 apples between three (distinct) people A, B, C such that:

1. A gets an odd number of apples
2. B gets at least one apple
3. C gets two or three apples

Solution 1: Split into cases:
Case 1: $C = 2$, (6 left) $A \in \{1,3,5\}$, so three ways
Case 2: $C = 3$, (5 left) $A \in \{1,3\}$ so two ways.
So in total 5 ways.

Solution 2:
Let $A(x) = x+x^3+x^5+x^7$,[4] $B(x) = x+x^2+x^3+x^4+x^5+x^6+x^7+x^8$, $C(x) = x^2+x^3$

[4] Why this polynomials? The exponent corresponds to the number of apples, that A can possibly have, the coefficient (here 1) corresponds to the number of ways that A can have that number of apples which is here one, because the apples are indistinguishable.

Idea: Compute $A(x)B(x)C(x)$ and identify the x^8 coefficient. This will be the number of solutions.

If you just multiply them as they are this just corresponds to counting all possible cases. So for this to make sense we need a smarter way to compute the product.

One example way to do this: Add the infinitely many terms:

$$B(x) = \sum_{k=1}^{\infty} x^k = x \cdot \sum_{k=0}^{\infty} x^k = \frac{x}{1-x} \tag{3.1}$$

$$A(x) = \sum_{k=0}^{\infty} x^{2k+1} = x \cdot \sum_{k=1}^{\infty} (x^2)^k = \frac{x}{1-x^2} \tag{3.2}$$

$$C(x) = x^2(1+x) \tag{3.3}$$

So:

$$A(x)B(x)C(x) = \frac{x}{1-x^2}\frac{x}{1-x}x^2(1+x) = \frac{x^4}{(1-x)^2} \tag{3.4}$$

I want the x^8 coefficient in the expansion of $\frac{x^4}{(1-x)^2}$ which is the same thing as the x^4 coefficient in the expansion of $\frac{1}{(1-x)^2}$.

So define $g(x) = (1-x)^{-2}$ thus the coefficient is $\frac{g^{(4)}(0)}{4!}$.

In our case: $g'(x) = 2(1-x)^{-3}, g''(x) = 6(1-x)^{-4}, g'''(x) = 24(1-x)^{-5}, g^{(4)}(x) = 120(1-x)^{-6}$.

The answer to our problem is thus $\frac{g^{(4)}(0)}{4!} = \frac{120}{24} = 5$.

3.2 Terminology and basic methods

Definition 3.1:

The function (really formal power series)

$$a_0 + a_1 x + x_2 x^2 + a_3 x^3 + \dots \tag{3.5}$$

is called the **generating function** of the sequence $(a_0, a_1, a_2, \dots)$.

Example 3.2

Look at the series

$$\binom{n}{0}, \binom{n}{1}, \binom{n}{2}, \dots, \binom{n}{n}, 0, 0, \dots \tag{3.6}$$

Its generating function is

$$\binom{n}{0} + \binom{n}{1}x + \binom{n}{2}x^2 + \dots + \binom{n}{n}x^n = (1+x)^n \tag{3.7}$$

Example 3.3

The generating function of the sequence $(1, 1, \dots)$ is

$$\sum_{k=1}^{\infty} x^k = \frac{x}{1-x} \tag{3.8}$$

Example 3.4

The generating function of the sequence $(\underbrace{1, \dots, 1}_{n \text{ times}}, 0, 0, \dots)$ is

$$\sum_{k=1}^{n} x^k = x\sum_{k=0}^{n-1} x^k = x\frac{1-x^n}{1-x} \tag{3.9}$$

Definition 3.5 (Some useful operations, Shifting, Differentiation, Products):

1. **Shifting:** If $(a_0, a_1, a_2, \dots) \leftrightarrow A(x)$, then $(\underbrace{0, 0, \dots, 0}_{n \text{ zeros}}, a_0, a_1, \dots) \leftrightarrow x^n A(x)$
2. **Differentiation:** If $a_0, a_1, \dots) \leftrightarrow A(x)$, then $(a_1, 2a_2, 3a_3, \dots) \leftrightarrow A'(x)$
3. **Products:** If $(a_0, a_1, \dots) \leftrightarrow A(x), (b_0, b_1, \dots) \leftrightarrow B(x)$, then

$$A(x)B(x) = a_0b_0 + (a_0b_1 + a_1b_0)x + (a_0b_2 + a_1b_1 + a_2b_0)x^2 + \dots \tag{3.10}$$

$$= \sum_{n=0}^{\infty}\left(\sum_{k=0}^{n} a_k b_{n-k}\right)x^n \tag{3.11}$$

Example 3.6 (Exercise)

Compute the g.f. (=generating function) for $0^2, 1^2, 2^2, 3^2, \dots$.
Solution: It is

$$\sum_{k=0}^{\infty} k^2 x^k = \dots \tag{3.12}$$

My idea: Let $f(a,k) = \sum_{k=0}^{\infty} e^{ak}x^k = \frac{1}{1-xe^a}$.

Then the solution is just $\partial_a^2 f\big|_{a=0}$.

Example 3.7

In how many ways can we fill a bag with n fruits (apples, bananas, organges, pears) in such a way that

1. The number of apples is even
2. The number of bananas is a multiple of 5
3. There are at most 4 oranges
4. There is a most 1 pear

Let

$$A(x) = 1 + x^2 + x^4 + x^6 + \dots = \sum_{k=0}^{\infty}(x^2)^k = \frac{1}{1-x^2} \tag{3.13}$$

$$B(x) = 1 + x^5 + x^{10} + \dots = \frac{1}{1-x^5} \tag{3.14}$$

$$O(x) = 1 + x + x^2 + x^3 + x^4 = \frac{1-x^5}{1-x} \tag{3.15}$$

$$P(x) = 1 + x \tag{3.16}$$

Therefore

$$\frac{1}{1-x^2}\frac{1}{1-x^5}\frac{1-x^5}{1-x}1 + x = \frac{1}{(1-x)^2} \tag{3.17}$$

How to compute this?
Two Options to compute this: Option 1:

$$\frac{1}{1-x}\frac{1}{1-x}(1+x+x^2+\dots)(1+x+x^2+\dots) = 1+2x+3x^2+\dots = \sum_{n=0}^{n}(n+1)x^{n+1} \tag{3.18}$$

Hence there are $n+1$ ways to fill the bag with n fruits!

The second option is to see that the derivative of $\frac{1}{1-x}$ is $\frac{1}{(1-x)^2}$.

This method is great if the conditions are weird but not too weird. Some regularities in the conditions are needed, for example if the number of apples has to be a prime number than the generating function won't give you a closed form!

3.3 Newton's Binomial Theorem

If $n \in \mathbb{N}$ then

$$(1+x)^n = \sum_{k=0}^{n}\binom{n}{k}x^k \underset{\uparrow}{=} \sum_{k=0}^{\infty}\binom{n}{k}x^k \tag{3.19}$$

If we define the Binomial coefficient to be zero outside of its usual range.

Newtons version says that if $\alpha \in \mathbb{R}$ then

$$(1+x)^\alpha = \sum_{k=0}^{\infty} \binom{\alpha}{k} x^k, \qquad |x| < 1 \tag{3.20}$$

What is the binomial coefficient?

$$\binom{\alpha}{k} = \frac{\alpha!}{(\alpha-k)!k!} = \frac{\alpha(\alpha-1)\dots(\alpha-k+1)}{k!} \tag{3.21}$$

Note: If n is a positive integer, then

$$\binom{-n}{k} = \frac{(-n)(-n-1)(-n-2)\dots(-n-k+1)}{k!} \tag{3.22}$$

$$= (-1)^k \frac{n(n+1)(n+2)\dots(n+k-1)}{k!} \tag{3.23}$$

$$= (-1)^k \binom{n+k-1}{k} \tag{3.24}$$

Example 3.8

Assume we have 12 identical cookies and want to distribute amonst three (distinct) children. In how many ways can we do this if

(a) Each child gets at least two cookies

(b) Each child gets at least 2 and at most 5 cookies.

Focus on one child. Generating function?

$$A(x) = x^2 + x^3 + \dots + x^{12} (+x^{13} + \dots), \quad B(x), C(x) \text{ same} \tag{3.25}$$

We want to extract the x^{12} coefficient in the expansion of

$$A(x)^3 = \left(\frac{x^2}{1-x}\right)^3 = \frac{x^6}{(1-x)^3} \tag{3.26}$$

or the x^6 coefficient of

$$\frac{1}{(1-x)^3} = \sum_{k=0}^{\infty} \binom{-3}{k} (-x)^k = \sum_{k=0}^{\infty} (-1)^k \binom{-3}{k} x^k = \sum_{k=0}^{\infty} (-1)^k (-1)^k \binom{3+k-1}{k} x^k \tag{3.27}$$

> So the number of solutions is
>
> $$\binom{3+6-1}{6} = \binom{8}{6} = \binom{8}{2} = 28 \tag{3.28}$$
>
> The solution of (b) is an exercise and in the lecture notes.

3.4 “Partitions” of integers

$$4 = 4 = 3+1 = 2+2 = 2+2+1+1 = 1+1+1+1 \tag{3.29}$$

How many partitions of n are there?

$$\left(1+x+x^2+x^3+\dots\right)\left(1+x^2+x^4+\dots\right)\left(1+x^3+x^6+\dots\right)\left(1+x^4+x^8+\dots\right)\dots \tag{3.30}$$

$$= \frac{1}{1-x}\frac{1}{1-x^2}\frac{1}{1-x^3}\cdots \tag{3.31}$$

$$= \prod_{k=1}^{\infty}\frac{1}{1-x^k} \tag{3.32}$$

We cannot simplify this expression.

But simplified versions an be solved by hand.

For example: How many partitions of n are there, if we only allow 1’s and 2’s?

$$= \frac{1}{1-x}\frac{1}{1-x^2} \tag{3.33}$$

$$= \frac{1}{2}\frac{1}{(1-x)^2} + \frac{1}{4}\frac{1}{1-x} + \frac{1}{4}\frac{1}{1+x} \tag{3.34}$$

$$= \sum_{k=0}^{\infty}\frac{1}{2}\binom{-2}{k}(-x)^k + \frac{1}{4}x^k + \frac{1}{4}(-x)^k \tag{3.35}$$

Here we can fairly easily conpute the coefficient of x^n.

3.5 Exponential generating functions

Good at solving counting problems where we want do distribute identical objects in distinct containers.

> **Example 3.9 (How many 4 letter “words” can we form out of AAABBC??)**
>
> If it where 6 letter word the answer would be $\frac{6!}{3!2!}$.

But 4 letter words are more tricky because we then do not know, out of how many of which letters they consist of. One could try cases, but this is tedious and error prone, because there will be a lot of cases.

One idea would be to solve $a+b+c=4$, with $0 \leq a \leq 3, 0 \leq b \leq 2, 0 \leq c \leq 1$. For each such solution, there are $\frac{4!}{a!b!c!}$ possibilities. So sum over all solutions!

Think of a generating function

$$\left(1+\frac{x}{1!}+\frac{x^2}{2!}+\frac{x^3}{3!}\right)\left(1+\frac{x}{1!}+\frac{x^2}{2!}\right)\left(1+\frac{x}{1!}\right) \tag{3.36}$$

The total number of 4 letter words is 4! times the coefficient of x^4 in the expansion.

Example 3.10

What is the exponential generating function of the sequence $1, -2, 2^2, -2^3, x^4, -x^5, \ldots$? It is

$$1+\frac{(-2)}{1!}x+\frac{(-2)^2}{2!}x^2+\frac{(-2)^3}{3!}x^3+\cdots=e^{-2x} \tag{3.37}$$

Example 3.11

Assume we have 48 flags: 12 red, 12 blue, 12 white, and 12 black.

How many signals can we send using 12 flags on a flagpole if

(a) there are an even number of red flags

(b) there is at least one flag of each colour

a): The generating function of the red flags is

$$\left(1+\frac{x^2}{2}+\frac{x^4}{4!}+\cdots+\frac{x^{12}}{12!}\right) \tag{3.38}$$

But since if we had more than 12 red flags it wouldn't matter, because we are only using 12 flags in total, we can add the infinitely many terms for that to get an infinite series, which is much better for computation.
The same goes for the other colors. So the generating function of the whole problem is

$$\begin{aligned} f(x) &= \left(1+\frac{x^2}{2}+\frac{x^4}{4!}+\cdots+\frac{x^{12}}{12!}+\frac{x^{14}}{14!}+\ldots\right)\left(1+\frac{x^1}{1!}+\frac{x^2}{2!}+\ldots\right)^3 && (3.39)\\ &= \frac{e^x+e^{-x}}{2}e^{3x}=\frac{1}{2}\left(e^{4x}+e^{2x}\right) && (3.40)\end{aligned}$$

The number we are looking for is 12! times the x^{12}-coefficient in the expansion.

$$\frac{1}{2}(e^{4x}+e^{2x}) = \frac{1}{2}\sum_{k=0}^{\infty}\frac{(4x)^k}{k!}+\frac{(2x)^k}{k!} \tag{3.41}$$

so the x^{12} coefficient is $\frac{1}{2}\left(\frac{4^{12}}{12!}+\frac{2^{12}}{12!}\right)$

So the number of signals is: $\frac{1}{2}\left(4^{12}+2^2\right)$.

b) The generating function is

$$\left(\frac{x}{1!}+\frac{x^2}{2!}+\frac{x^3}{3!}+\ldots\right)^4 = (e^x-1)^4 = e^{4x}-4e^{3x}+6e^{2x}-4e^x+1 \tag{3.42}$$

$$= \left(\sum_{k=0}^{\infty}\frac{(4x)^k}{k!}-4\frac{(3x)^k}{k!}+6\frac{(2x)^k}{k!}-4\frac{x^k}{k!}\right)-1 \tag{3.43}$$

In particular, the x^{12} coefficient is

$$\frac{4^{12}}{12!}-4\frac{3^{12}}{12!}+6\frac{2^{12}}{12!}-4\frac{1}{12!} \tag{3.44}$$

So the number of signals is 12! times this, i.e. $4^{12}-43^{12}+62^{12}-4$.

3.6 Summing a sequence

If $(a_0, a_1, a_2, \ldots)$ has the ordinary generating function (ogf)

$$f(x) = a_0 + a_1x + a_2x^2 + \ldots \tag{3.45}$$

What is then the generating function for $a_0, a_0+a_1, a_0+a_1+a_2, a_0+a_1+a_2+a_3$:

$$\left(a_0+a_1x+a_2x^2+\ldots\right)\underbrace{\left(1+x+x^2+\ldots\right)}_{=\frac{1}{1-x}} = a_0+(a_0+a_1)x+(a_0+a_1+a_2)x^2+\ldots \tag{3.46}$$

So the sequence of the partial sums has the generating function $\frac{f(x)}{1-x}$

Example 3.12

What is $0^2+1^2+2^2+\cdots+n^2$?
What is the generating function for $0^2, 1^2+2^2+3^2, \ldots$?
It is

$$f(x) = \frac{x(x+1)}{(1-x)^3} \qquad \text{(Exercise!)} \tag{3.47}$$

The partial sums then have the generating function

$$\frac{f(x)}{1-x} = \frac{x(1+x)}{(1-x)^4} = (x+x^2)(1-x)^{-4} \tag{3.48}$$

We want the coefficient of x^n in the expansion of this!

$$(x+x^2)\sum_{k=0}^{\infty}\binom{-4}{k}(-x)^k \tag{3.49}$$

So the coefficient of x^n is

$$\begin{aligned}\binom{-4}{n-1}(-1)^{n-1} + \binom{-4}{n-2}(-1)^{n-2} &= \binom{n+2}{n-1}(-1)^{n-1}(-1)^{n-1} + \binom{n+1}{n-2}(-1)^{n-2}(-1)^{n-2} && (3.50)\\ &= \binom{n+2}{3} + \binom{n+1}{3} && (3.51)\\ & \frac{(n+2)(n+1)n}{6} + \frac{(n+1)n(n-1)}{6} && (3.52)\\ &= \frac{1}{6}n(n+1)(2n+1) && (3.53)\end{aligned}$$

4 Recurrence relations

Example 4.1

$1, 1, 2, 3, 5, 8, 13, ...$ This is the fibonacci sequence where $F_{n+2} = F_{n+1} + F_n, n \geq 1$ (or $F_n = F_{n-1} + F_{n-2}, n \geq 3$.

The good thing with difference equations is that contrary to differential equations, it is at least obvious that there exists a solution.

Example 4.2

$(n+1)! = (n+1)n!, 0! = 1$

We will mostly focus on linear recurrence relations (often of order 1 and 2).
Order 1: $a_{n+1} + g_n a_n = f_n$ (usually g_n =constant, because otherwise very hard to solve.
Order 2: $a_{n+2} + p_n a_{n+1} + q_n a_n = f_n$.

There are at least three reasonable ways so solve such equations.

4.1 Method 1: Generating function

Example 4.3

$$a_{n+2} - a_{n+1} - 2a_n = -4, \quad a_0 = 0, a_1 = 1 \tag{4.1}$$

Let $f(x) = a_0 + a_1 x + a_2 x^2 + \ldots$. Multiply eq. (4.1) by x^{n+2} and sum!

$$\sum_{n=0}^{\infty} \left(a_{n+2}x^{n+2} - a_{n+1}x^{n+2} - 2a_n x^{n+2}\right) = \sum_{n=0}^{\infty} -4x^{n+2} = \frac{-4x^2}{1-x} \tag{4.2}$$

$$\left(f(x) - a_0 - a_1 x\right) - x\left(f(x) - a_0\right) - 2x^2 f(x) = \tag{4.3}$$

Solve for $f(x)$!

$$f(x)\left(1 - x - 2x^2\right) - x = \frac{-4x^2}{1-x} \tag{4.4}$$

So

$$f(x) = \frac{-5x^2 + x}{(1-x-2x^2)(1-x)} \underset{\substack{\uparrow \\ \text{partial fraction}}}{=} \frac{2}{1-x} - \frac{1}{x+1} - \frac{1}{1-2x} - \frac{1}{1-2x} \tag{4.5}$$

this is the sum of three geometric series so it is easy to see the nth coefficient.

4.2 Method 2: Linear Algebra

Mostly useful for the homogeneous case (RHS=0).

Example 4.4

$$a_{n+2} - a_{n+1} - 2a_n = 0, \quad a_0 = -2, a_1 = -1 \tag{4.6}$$

Let

$$X_n = \begin{pmatrix} a_{n+1} \\ a_n \end{pmatrix}, \tag{4.7}$$

then

$$X_{n+1} = \begin{pmatrix} a_{n+2} \\ a_{n+1} \end{pmatrix} = \begin{pmatrix} a_{n+1} + 2a_n \\ a_{n+1} \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a_{n+1} \\ a_n \end{pmatrix} = A \cdot X_n \tag{4.8}$$

So we know that $X_n = A^n X_0$. If we can diagonalize A, i.e. find matrices P, D s.t. $A = PDP^{-1}$ where D is a diagonal matrix, then

$$X_n = A^n X = (PDP^{-1})^n X_0 = PDP^{-1}PDP^{-1} \ldots PDP^{-1}X_0 = PD^n P^{-1} X_0 \tag{4.9}$$

where in fact $D = \begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix}$ and λ_1, λ_2 are eigenvalues and $P = \begin{pmatrix} \vec{u}_1 & \vec{u}_2 \end{pmatrix}$ where u_1, u_2 are the corresponding eigenvectors.

In our example $A = \begin{pmatrix} 1 & 2 \\ 1 & 0 \end{pmatrix}$, $\lambda_1 = 2$, $u_1 = \begin{pmatrix} 2 \\ 1 \end{pmatrix}$, $\lambda_2 = -1$, $u_2 = \begin{pmatrix} -1 & 1 \end{pmatrix}$
So

$$A = \begin{pmatrix} 2 & -1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 2 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} \frac{1}{3} & \frac{1}{3} \\ -\frac{1}{3} & \frac{2}{3} \end{pmatrix} \tag{4.10}$$

thus

$$X_n = PD^nP^{-1}X_0 = \begin{pmatrix} 2 & -1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 2^n & 0 \\ 0 & (-1)^n \end{pmatrix} \begin{pmatrix} \frac{1}{3} & \frac{1}{3} \\ -\frac{1}{3} & \frac{2}{3} \end{pmatrix} \begin{pmatrix} -1 & -2 \end{pmatrix} = \cdots = \begin{pmatrix} -2 \cdot 2^n + (-1)^n \\ -2^n - (-1)^n \end{pmatrix} \tag{4.11}$$

Hence $a_n = -2^n - (-1)^n$.

In general we see that the solution will be of the form $A\lambda_1^n + B\lambda_2^n$ (assuming $\lambda_1 \neq \lambda_2$).

4.3 Method 3: The characteristic equation

In practice the quickest way to solve this is "Method 3".

Example 4.5

$$a_{n+2} - 5a_{n+1} + 6a_n = 0, \quad a_0 = a_1 = 1 \tag{4.12}$$

We look for solutions of the type r^n.
If $a_n = r^n$ then $a_{n+1} = r^{n+1} = rr^n, a_{n+2} = r^{n+2} = r^2r^n$. Hence

$$r^2 \cdot r^n - 5rr^n + 6r^n = 0 \quad r^n \underbrace{(r^2 - 5r + 6)}_{\text{The characteristic equation}} = 0 \tag{4.13}$$

So

$$r^2 - 5r + 6 = (r-2)(r-3) = 0, \Longrightarrow r_1 = 2, r_2 = 3 \tag{4.14}$$

So $a_n = C2^n + D3^n$ is a solution to the recurrence relation (for every choice of $C, D.$). In fact every solution is of this form.

We also need to match the initial conditions: $1 = a_0 = C + D, 1 = a_1 = 2C + 3D$, therefore $C = 2, D = -1$.

Our solution is

$$a_n = 2 \cdot 2^n + (-1)3^n. \tag{4.15}$$

Now we want to generalize this method. There are three cases (also generalizations to higher order recurrence relations).

The characteristic equation can have

1) Two distinct real roots r_1, r_2: Solution $Cr_1^n + Dr^n$

2) Two complex roots $r_1, \overline{r_1}$: Solution $Cr_1^n + D\overline{r_1}^n$
Sometimes we want "real" solutions. $r_1 = \rho e^{i\theta}$ ($\rho \geq 0, 0 \leq \theta \leq 2\pi$), then $r_2 = \overline{r_1} = \rho e^{-i\theta}$. So

$$\begin{aligned} a_n &= C\left(\rho e^{i\theta}\right)^n + D\left(\rho e^{-i\theta}\right)^n && (4.16)\\ &= C\rho^n e^{in\theta} + D\rho^n e^{-in\theta} && (4.17)\\ &= C\rho^n\left(\cos(n\theta) + i\sin(n\theta)\right) + D\rho^n\left(\cos(n\theta) - i\sin(n\theta)\right) && (4.18)\\ &= \underbrace{(C+D)}_{\tilde{C}}\rho^n\cos(n\theta) + \underbrace{i(C-D)}_{\tilde{D}}\rho^n\sin(n\theta) && (4.19)\\ &= \tilde{C}\rho^n\cos(n\theta) + \tilde{D}\rho^n\sin(n\theta) && (4.20)\end{aligned}$$

3) Double root r. One solution is r^n. But we need a second "linearly independent" solution.

> **Example 4.6**
> Exercise: Try solving
>
> $$a_{n+2} - 2a_{n+1} + a_n = 0, \qquad a_0 = 0, a_1 = 1 \tag{4.21}$$
>
> in a very naive way! (Compute the first terms by hand.)

It turns out, that in case 3, a second solution is given by $a_n = nr^n$. So look at

$$a_{n+2} + pa_{n+1} + qa_n = 0 \tag{4.22}$$

and

$$r^2 + pr + q = 0 \tag{4.23}$$

has a double root r_1, i.e.

$$(r - r_1)^2 = r^2 + pr + \quad \Longrightarrow \quad -2r_1 = p, \quad r_1^2 = q \tag{4.24}$$

Claim: $a_n = nr_1^n$ is a solution. Then $a_{n+1} = (n+1)r_1^{n+1} = r_1(n+1)r_1^n$, $a_{n+2} = (n+2)r_1^{n+2} = r_1^2(n+2)r_1^n$

Plug in

$$\begin{aligned} &r_1^2(n+2)r_1^n + pr_1(n+1)r_1^n + qnr_1^n && (4.25)\\ &\qquad = r_1^n\left(nr_1^2 + nr_1p + qn + 2r_1^2 + pr_1\right) && (4.26)\\ &\qquad = r_1^n\left(nr_1^2 - 2nr_1^2 + r_1^2n + 2r_1^2 - 2r_1^2\right) && (4.27)\\ &\qquad = 0 && (4.28)\end{aligned}$$

So the general solution to this case is

$$Cr_1^n + Dnr_1^n \tag{4.29}$$

How to generalize this to higher (or lower) orders?

Higher (or lower) order linear recurrence relations with constant coefficients:

$$a_{n+k} + c_1 a_{n+k-1} + c_2 a_{n+k-2} + \cdots + c_n a_n = 0 \tag{4.30}$$

Looking for solutions r^n we get the characteristic equation

$$r^k + c_1 r^{k-1} + c_2 r^{k-2} + \cdots + c_n = 0. \tag{4.31}$$

Every root (real or complex) gives a solution r^n. If r is a root of multiplicity $m > 1$, we get solutions $r^n, nr^n, n^2r^n, \dots, n^{m-1}r^n$.

How about non-homogeneous recurrence relations?

4.4 Non-homogeneous recurrence relations

In general to solve

$$a_{n+2} + pa_{n+1} + qa_n = f(n), \tag{4.32}$$

we do the following.[5]

1) Solve the corresponding homogeneous equation.
2) Find one particular solution by judicious guessing.
3) The general solution is then 1) + 2).
4) Match initial conditions

Here are some general guesses for the particular solution 2).

$f(n)$	ansatz
constant	constant
poly of degree d	poly of degree d
S^n	constant $\cdot S^n$
(polynomial of degree d) $\cdot S^n$	(polynomial of degree d) $\cdot S^n$

[5] Similarly to differencial equations

Example 4.7

Solve:

a) $a_{n+2} - 5a_{n+1} + 6a_n = 0$

b) $a_{n+2} - 5a_{n+1} + 6a_n = n$

c) $a_{n+2} - 5a_{n+1} + 6a_n = (-1)^n$

d) $a_{n+2} - 5a_{n+1} + 6a_n = 2^n$

Sol. a) Char equation:

$$r^2 - 5r + 6 = 0 = (r-2)(r-3) \tag{4.33}$$

So

$$a_n = C2^n + D3^n \tag{4.34}$$

Sol. b) Natural ansatz is $a_n^P = En + F$, hence

$$E(n+2) + F - 5(E(n+1) + F) + 6(En + F) = n \tag{4.35}$$

$$2En + (-3E + 2F) = n \tag{4.36}$$

Therefore $2E = 1, -3E + 2F = 0$, so $E = \frac{1}{2}, F = \frac{3}{4}$, thus $a_n^p = \frac{1}{2}n + \frac{3}{4}$ is a particular solution.

Sol. c) Do it yorself. Ansatz: $a_n^p = E(-1)^n$

Sol. d) The natural ansatz would be $a_n^p = E \cdot 2^n$.
This can't work! (Since $E \cdot 2^n$ solves the corresponding homogeneous equation!)

Maybe we can try "n times the natural ansatz", $a_n^p = En2^n$.

$$4E(n+2)2^n - 10E(n+1)2^n + 6En2^n = 2^n \iff -2E \cdot 2^n = 2^n \tag{4.37}$$

i.e. $E = -\frac{1}{2}$, i.e. $a_n^p = -\frac{1}{2}n2^n$.

Example 4.8

How many strings of length n using the symbols A, B, C are there with no consecutive A's or B's?

Let us denote by a_n the number of such strings.

Let's also denote by b_n the number of such strings that end in A or B, and by c_n the number of such strings that end with C.

Of course $a_n = b_n + c_n$.

What is b_{n+1}, c_{n+1}?

$$b_{n+1} = b_n + 2c_n \qquad c_{n+1} = b_n + c_n (= a_n) \tag{4.38}$$

The right equation follows from the fact, that when one letter is fixed, then the rest of the word can be changed freely. The left equation from the fact, that if the string of length n starts with A or B then there is one possibility to make it to length $n+1$ (add the other one) but if it starts with C then there are to possiblities to make it to length $n+1$ (add A or B).

So:

$$a_{n+1} = b_{n+1} + c_{n+1} = 2a_n + c_n = 2a_n + a_{n-1} \tag{4.39}$$

Thus

$$a_{n+1} - 2a_n - a_{n-1} = 0 \tag{4.40}$$

The characteristic equation is

$$r^2 - 2r - 1 = 0 \quad \Longrightarrow \quad r = 1 \pm \sqrt{2} \tag{4.41}$$

So

$$a_n = A(1+\sqrt{2})^n + B(1-\sqrt{2})^n \tag{4.42}$$

We can work out the initial conditions from the question: $a_0 = 1, a_1 = 3, (a_2 = 7)$. ($a_0$ comes from the empty world.) Therefore

$$1 = A+B \quad 3 = A(1+\sqrt{2})+B(1-\sqrt{2}) = A+B+\sqrt{2}(A-B) = 1+\sqrt{2}(A-B) \tag{4.43}$$

Therefore $A = \frac{1+\sqrt{2}}{2}, B = \frac{1-\sqrt{2}}{2}$.

So the answer to our problem is

$$a_n = \frac{1+\sqrt{2}}{2}\left(1+\sqrt{2}\right)^n + \frac{1-\sqrt{2}}{2}\left(1-\sqrt{2}\right)^n = \tfrac{1}{2}\left(\left(1+\sqrt{2}\right)^{n+1} + \left(1-\sqrt{2}\right)^{n+1}\right) \tag{4.44}$$

5 Graph Theory

Definition 5.1 (Graph):

A **Graph** G consists of a set of vertices V and a (multi-)set of edges E (which are 2-subsets of V or pairs for directed graphs).

Definition 5.2:

Let G be a graph and x, y vertices in G ($x = y$ is allowed).

- ▶ A **walk** from x to y is a sequence

$$x = v_0, e_1, v_1, e_2, \dots, e_n, v_n = y \tag{5.1}$$

alternating between vertices and edges, such that e_k is between v_k and v_{k-1}.

- ▶ A walk from x to y where $x = y$ is called a **closed walk**.
- ▶ A walk with no repeated edges is called a **trail**.
- ▶ A closed trail is called a **circuit**.
- ▶ A walk with no repeated vertices is called a **path**.
- ▶ A circuit that is also a path, i.e. a closed walk with no repeated edges and no repeated vertices, is called a **cycle**.
- ▶ A circuit, which visits every edge exactly once, is called an **Euler circuit.**

Definition 5.3 (connectivity):

An undirected graph G is called **connected** if each pair of vertices is connected with a walk.

Definition 5.4 (Subgraph):

Subgraph: "obvious" definition. preferences? And is it okay with you if pic A subgraph is called **spanning** if it has the same verties as the original graph.

Definition 5.5 (Subtraction of vertices):

If v is a vertex in G, then $G - v$ is the graph I obtain by removing v and all connected edges.

Definition 5.6 (Completeness):

A **complete** graph on n vertices is a graph where every pair of vertices has an edge.

Definition 5.7 (Isomorphy):

Two graphs, $G = (V, E)$ and $\tilde{G} = (\tilde{V}, \tilde{E})$ are called **isomorphic** if there is a bijective $f : V \to \tilde{V}$ such that $e \in \{a, b\} \in E \iff \{f(a), f(b)\} \in \tilde{E}$.

Definition 5.8 (Degree of a vertex):

If v is a vertex in G, then the **degree** of v, $d(v)$ or $\deg(v)$ is the number of edges connected to v.

Lemma 5.9 (The handshaking Lemma)

$$\sum_{v \in V} d(v) = 2|E| \tag{5.2}$$

Is there a graph of 6 vertices with degree sequence, $4, 4, 4, 3, 2, 2$? No, because the sum of all these is 19 which is not even.

Theorem 5.10 (Existence of Euler circuits)

Let $G = (V, E)$ be an undirected (multi-)graph.

The G has an Euler circuit iff

- G is connected
- Every vertex of G has even degree

Proof. $\Longrightarrow$ If G has an Euler circuit, clearly G is connected.
Traverse the circuit. Each vertex that we enter, we want to leave again. So when we come back to the starting point, we've goe through an even number of edges at every vertex.
$\Longleftarrow$ Induction on the number of edges.
It clearly is true for a graph with $|E| = 0$ and $|E| = 1$.
Assume true for all graphs with $< n$ edges. We want to show that it is true for n edges. Take any connected graph G where all vertices have an even degree. Take any vertex v, and look at the (longest) trail in G starting at v. Walk along new edges until we're stuck. Then $v_k = v$, because to be stuck before an odd number of edges must have been removed which is only the case for the starting vertex. So we have found a circuit. Look at $G - \underbrace{\{e_1, \ldots, e_k\}}_{\text{the circuit we found}} = H$. Then H is a union of connected graphs where all vertices have even degree, so by the inductive hypothesis, each such component has an Euler circuit, which can be "spliced in" to give an Euler circuit for G. □

Corollary 5.11

K_n has an Euler circuit iff n is odd.

Corollary 5.12

G has an Euler trail iff G is connected and all vertices except at most two have an even degree.

Definition 5.13 (Hamilton cyles):

Let $G = (V, E)$ be an undirected (multi-)graph. A Hamilton cycle in G is a cycle containing every vertex.

However in graphs with "lots of edges" we can guarantee the existance of Hamilton paths/cycles.

Theorem 5.14

Let $G = (V, E)$ be a loop-free undirected graph with $|V| = n \geq 2$.

If

$$d(x) + d(y) \geq n - 1 \tag{5.3}$$

for all x, y $(x \neq y)$ then G has a Hamilton path.

Proof.

1. We first show that G is connected.
   a) If its not connected, then we can split the graph in a way that there are no edges between the two parts G_1, G_2.
   b) Then for $x \in V_1, y \in V_2$ we know that $d(x) \leq |V_1| - 1$, $d(y) \leq |V_2| - 1$ so
   $$d(x) + d(y) \leq |V_1| - 1 + |V_2| - 1 = n - 2 \tag{5.4}$$
2. Take (one of) the longest path in G.
   $$v_1 \rightarrow v_2 \rightarrow v_3 \rightarrow \cdots \rightarrow v_k \tag{5.5}$$
3. If $k = n$, we have a Hamilton path. So assume $k < n$.
4. In fact I claim that these vertices are one a cycle of length k.
   a) If v_k is adjacent to v_1 $(v_k \sim v_1)$ this is definitely true.
   b) Otherwise $v_k \nsim v_1$.

c) Note that all edges from v_1 and v_k go to other vertices in the path (otherwise there is a longer path!).

d) If $v_1 \sim v_m$ and $v_k \sim v_{m-1}$ for any m we have a cycle. (Go $v_1 \sim v_2 \sim \cdots \sim v_{m-1} \sim v_k \sim v_{k-1} \sim v_{k-2} \sim \cdots \sim v_m \sim v_1$.)

e) If this is not the case $d(v_k) \leq k-1-d(v_1)$. (every edge from v_1 prevents one edge from v_k and it can't be connected to anything outside of the path, because then the graph would be longer.) So $d(v_1)+d(v_k) \leq k-1 < n-1$ Contradiction!

f) So: We have a cycle

5. But since $k < n$, we have extra vertices and they are connected to the cycle which would give us a longer path.

6. Again this is a contradiction, so $k = n$.

□

How about Hamiltonian cyles?

Theorem 5.15 (Ore, 1960)

If $G = (V, E)$ is an undirected loop-free graph satisfying

$$d(x) + d(y) \geq n \tag{5.6}$$

for every pair x, y $(x \sim y)$. Then G has a Hamilton cycle.

How about Hamilton paths in directed graphs?

Definition 5.16 (Tournament):

A tournament on n vertices (K_n^*) is "a directed version of the complete graph K_n".

Theorem 5.17

Every tournament has a (directed) Hamiltonian path.

Proof. Let $v_1 \to v_2 \to \cdots \to v_k$ be (one of) the longest directed paths in K_n^*. If $k = n$, then we have a Hamilton path.
Look at an vertex v not in the path. We know that $v \to v_1$ is not allowed (longer path) so $v_1 \to v$. Now $v \to v_2$ is not allowed ($v_1 \to v \to v_2 \to \ldots$ would be a longer path), so $v_2 \to v$. Analogously $v \to v_3$ is not allowed ($v_1 \to v_2 \to v \to v_3 \to \ldots$ longer path) and so on. For last edge both $v \to v_k$ is not allowed (same argument as before), and also $v_k \to v$ (also longer path). Either way we have a contradiction! So $k = n$. □

6 Rings and Fields

Definition 6.1 (Ring):

A **ring** is a set R equipped with two binary operations $+ : R \times R \to R$ and $\cdot : R \times R \to R$ satisfying the ring axioms:
For all $a, b \in R$:

(A1) $a + b \in R$

(A2) $(a + b) + c = a + (b + c)$

(A3) $a + b = b = a$

(A4) $\exists 0 \in R : a + 0 = a$

(A5) $\forall a \in R \exists - a : a + (-a) = 0$

(M1) $a \cdot b \in R$

(M2) $(a \cdot b) \cdot c = a \cdot (b \cdot c)$

(D) $a \cdot (b + c) = a \cdot b + a \cdot c$

Example 6.2

1. $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, M_n(\mathbb{R}), \mathbb{R}[x], \{f : A \to R\}, 2\mathbb{Z}, \langle 2^A, \Delta, n\rangle$

Remark 6.3
Many Rings have extra structure:

1. [(M3)] $a \cdot b = b \cdot a$
2. [(M4)] $\exists 1 \in R : 1 \cdot a = a \cdot 1 = a$ (“unity”)

Definition 6.4:

If R is a commutative ring with unity such that $\forall a \in R \setminus \{0\} \, \exists a^{-1} : a \cdot a^{-1} = 1$ is called a **field**.

6.1 The ring $\mathbb{Z}_n$

Let $n \geq 2$, define an equivalence relation on $\mathbb{Z}, \sim$ by

$$a \sim b \Longleftrightarrow a \mid a - b \tag{6.1}$$

So we get equivalence classes:

$$\begin{aligned}
[0] &= \{\dots, -2n, -n, 0, n, 2n, 3n, \dots\} \\
[1] &= \{\dots, -n+1, 1, n+1, 2n+1, \dots\} \\
\vdots &= \vdots \\
[n-1] &= \{\dots, -n-1, -1, n-1, 2n-1, 3n-1, \dots\}
\end{aligned}$$

We will make a ring out of

$$\mathbb{Z}_n = \{[0], [1], \dots, [n-1]\}. \tag{6.2}$$

We define addition and multiplication by

$$[a] + [b] = [a+b] \qquad [a] \cdot [b] = [a \cdot b]. \tag{6.3}$$

We need to check that this is well defined, i.e. if $a \sim a'$, $b \sim b'$ (i.e. $a = a' + kn, b = b' + ln$):

$$[a]+[b] = [a+b] = [a'+kn+b'+ln] = [a'+b'+(k+l)n] = [a'+b'] = [a']+[b'] \tag{6.4}$$

same for multiplication.

Example 6.5

In $\mathbb{Z}_{12}$ we have $[2]+[7]=[9], [6][6]=[0], [3][8]=[0]$.

Wo $\mathbb{Z}_{12}$ has zero divisors. Is it possible to find a multiplicative inverse of [3] in $\mathbb{Z}_{12}$? Because we $[3][8] = [0]$ we know that if $[3]^{-1}$ exists, then $[3]^{-1}[3][8] = [3]^{-1}[0]$, i.e. $[8] = [0]$ which is a contradiction. So $\mathbb{Z}_{12}$ is **not** a field.

But in $\mathbb{Z}_5$, $[1][1] = [1], [2][3] = 1, [4][4] = 1$ so all non-zero numbers in $\mathbb{Z}_5$ have multiplicative inverses, i.e. $\mathbb{Z}_5$ is a field!

Theorem 6.6

$[a] \in \mathbb{Z}_n$ has a multiplicative inverse iff $\gcd(a,n) = 1$.

Proof. $\Longrightarrow$: Assume $d = \gcd(a,n) > 1$ then $a = da', n = dn'$, then $a = da', n = dn'$

$$[a][n'] = [da'n'] = [a'n] = [0] \tag{6.5}$$

so $[a]$ can't have multiplicative inverse.
$\Longleftarrow$: Look at the diophantine equation

$$ax + ny = 1 \tag{6.6}$$

has a solution (Bezcuit's theorem) if $\gcd(a,n)=1$. Then $ax=1-ny$, i.e. $[a][x]=[1-ny]=[1]$. □

Example 6.7

Find the multiplicative inverse of $[7]$ in $\mathbb{Z}_{30}$.

$30=4\cdot 7+2 \Longrightarrow 7=3\cdot 2-1$

Backwards $1=7-3\cdot 2=7-3\cdot(30-4\cdot 7)=13\cdot 7-3\cdot 30$.

Thus modulo 30: $[1]=[13][7]$ or $[7]^{-1}=[13]$.

Example 6.8

Solve $7x\equiv 5 \pmod{30}$.
Multiply bu $[7]^{-1}=13$, $x=13\cdot 7x\equiv 13\cdot 5=65\equiv 5$.

Corollary 6.9

$\mathbb{Z}_n$ is a field iff n is prime.

Definition 6.10 (Ideal):

Assume R is a commutative ring (with 1). Then an **ideal** I in R is a subset such that:

$$a,b\in I\Longrightarrow a+b\in I,\quad r\in R, a\in I\Longrightarrow ra\in I \tag{6.7}$$

Example 6.11

1. $n\mathbb{Z}=\{na : a\in\mathbb{Z}\}$ is an ideal in $\mathbb{Z}$.
2. $\langle x^2+1\rangle=\big\{(x^2+1)p(x) : p\in\mathbb{R}[x]\big\}$ is an ideal in $\mathbb{R}[x]$.

As in the construction of $\mathbb{Z}_n$ if I is an ideal in R, we can define an equivalence relation on R by $a\sim b\Longleftrightarrow a-b\in I$.

We can make $R/I=$ the set of equivalence classes into a ring by defining $[a]+[b]=[a+b]$, $[a]\cdot[b]$.

Example 6.12

$\mathbb{Z}/n\mathbb{Z}=\mathbb{Z}_n$.

What is $\mathbb{R}[x]/\langle x^2+1\rangle$?

Take any $p(x)\in\mathbb{R}[x]$, $p(x)=(x^2+1)q(x)+r(x)$, so $[p(x)]\sim[r(x)]$.
We can think of elements in $\mathbb{R}[x]/\langle x^2+1\rangle$ as degree 1 polynomials $a+bx$.
e.g. $(1+x)(2+x)=2+3x+x^2=1+3x$

Note $[0] = [x^2+1] \iff [x^2] = [-1]$ in other words $x^2 = -1$, i.e. $\mathbb{R}[x]/\langle x^2+1\rangle$ is actually $\mathbb{C}$ (or at least "isomorphic" to $\mathbb{C}$).

6.2 Homomorphisms and Isomorphisms of rings

Let $\langle R, +_R, \cdot_R\rangle, \langle S, +_S, \cdot_S\rangle$ be rings. A homomorphism is a map $f : R \to S$ such that

$$f(a +_R b) = f(a) +_S f(b) \qquad f(a \cdot_R b) = f(a) \cdot_S f(b) \tag{6.8}$$

and if R, S have unity $f(1_R) = 1_S$.

A bijective homomorphism is called an isomorphism.

Example 6.13

Let $\sigma : \mathbb{C} \to \mathbb{C}$, where $\sigma(z) = \overline{z}$. Then

$$\sigma(z+w) = \overline{z+w} = \overline{z}+\overline{w} = \sigma(z)+\sigma(w), \quad \sigma(z\cdot w) = \overline{z\cdot w} = \overline{z}\cdot\overline{w} = \sigma(z)\cdot\sigma(w), \sigma(1) = \overline{1} = 1. \tag{6.9}$$

$\sigma^{-1} = \sigma$ (so σ is an isomorphism)

Example 6.14

Let $M = \left\{ \begin{pmatrix} a & -b \\ b & a \end{pmatrix}, a, b \in \mathbb{R} \right\}$. Check that this is a ring!

Define $f : M \to \mathbb{C}$, $f(\begin{pmatrix} a & -b \\ b & a \end{pmatrix}) = a + bi$.

This is a homomorphism!

Fairly easy to see that f is a bijection, i.e. f is an isomorphism.

Example 6.15

Nonexample: $f : \mathbb{Z} \to 2\mathbb{Z}$, where $f(a) = 2a$ because $f(ab) = 2ab \neq 2a2b = f(a)f(b)$.

Example 6.16

Exercise: Determine all the ring homomorphisms $\mathbb{Z} \to \mathbb{Z}_n$.

6.3 Fermat's little Theorem

If R is a (commutative) ring, we let R^* be the set of invertible elements in R. Note that if F if a field, then $F^* = F \setminus \{0\}$.

Theorem 6.17 (Fermat's little theorem)

If F is a finite field with q elements, and $a \in F, a \neq 0$, then

$$a^{q-1} = 1. \tag{6.10}$$

Proof. $F^* = \{x_1, x_2, \dots, x_{q-1}\}$, define $F^* \to F^*$ by $f(x) = a \cdot x$.

1. $ax \in F^*$, $x^{-1}a^{-1}(ax) = 1$
2. f is injective: $ax = ay \implies a^{-1}ax = a^{-1}ax \implies x = y$.
3. f is surjective: If $x \in F^*$ is there a $y : f(y) = x$? Yes, $y = a^{-1}x$ is this.

In other words f is bijection, so a permutation of the elements, but also

$$f(x_1) \cdot f(x_2) \cdot \dots \cdot f(x_{q-1}) = (ax_1)(ax_2)\dots(ax_{q-1}) = a^{q-1}x_1x_2\dots x_{q-1} \underset{\substack{\uparrow \\ \text{permutation}}}{\overset{!}{=}} x_1x_2\dots x_{q-1} \tag{6.11}$$

Therefore $a^{q-1} = 1$. □

In particular $\mathbb{Z}_p$ is a field if p is prime, so if $p \nmid a$ then $a^{p-1} \equiv 1 \mod p$

Example 6.18

Compute $19^{122} \mod 13$. We know $19^{12} \equiv 1 \mod 13$ by Fermat.

$$19^{122} = (19^{12})^{10}19^2 = 19^2 = 6^2 = 36 = 10 \mod 13 \tag{6.12}$$

We can generalize Fermat's little theorem. If $n \in \mathbb{Z}$, let $\Phi(n)$ = the number of Integers between 1 and n that have no common factor with n ($\gcd(a, n) = 1$), so the number of invertible elements in $\mathbb{Z}_n$ is $\Phi(n)$.

Example 6.19

If p is a prime, that $\Phi(p) = p - 1$.
If p_1, p_2 are primes, then $\Phi(p_1p_2) = p_1p_2 - p_1 - p_2 + 1 = (p_1 - 1)(p_2 - 1)$.

More generally for the Eulerian φ-function φ the following theorem holds.

Lemma 6.20 (Properties of φ-function)

Let $\varphi(n) := |\{a \mid 1 \leq a \leq n, \gcd(a, n) = 1\}|$ be the Eulerian φ function.

- Then for $\gcd(n, m) = 1$ it holds that

$$\varphi(nm) = \varphi(n)\varphi(m). \tag{6.13}$$

▶ In general if $n = p_1^{k_1} \dots p_l^{k_l}$ is the prime factorization of n then

$$\varphi(n) = p_1^{k_1-1}(p_1-1)\dots p_l^{k_l-1}(p_l-1) \tag{6.14}$$

Proof. We will first show the first property, so eq. (6.13).

1. Let $M_n := \{a \mid 1 \leq a \leq n, \gcd(a,n) = 1\}$, so $\varphi(n) = |M_n|$.
2. Then define $A := M_n$, $B := M_m$, $C := M_{nm}$.
3. Then every element in A is invertible modulo $\mathbb{Z}_n$, in B modulo $\mathbb{Z}_m$ and in C modulo $\mathbb{Z}_{nm}$.
4. Since $\gcd(n,m) = 1$, by the Chinese remainder theorem (which will come later in the script) the system

$$x \equiv a \mod n, \quad x \equiv b \mod m \tag{6.15}$$

has a unique solution $\mod mn$ for all $a \in A, b \in B$. Also the $\gcd(x, mn) = 1$.

5. In other words, there is a bijection between $A \times B$ and C, therefore

$$\varphi(n)\varphi(m) = |A||B| = |A \times B| \underset{\substack{\uparrow \\ \text{Bijection}}}{=} |C| = \varphi(nm). \tag{6.16}$$

Now we can proof eq. (6.14) using this.

1. First observe that $\varphi(p^k) = p^{k-1}(p-1)$:
   a) We notice that $\gcd(a, p^k) = 1 \iff \gcd(a,p) = 1$.
   b) Therefore the integers a with $\gcd(a, p^k) \neq 1$ are the multiples of p.
   c) There are exactly p^{k-1} multiples of p which are $\leq p^k$. So

$$\varphi(p^k) = p^k - p^{k-1} = p^{k-1}(p-1). \tag{6.17}$$

2. Now use the multiplicative property eq. (6.13) to obtain the result.

□

Theorem 6.21 (Euler)

Let R be a finite commutative ring. If $a \in R$ is invertible then

$$a^{\#\text{invertible elements}} \equiv 1 \mod n \tag{6.18}$$

.

In particular if R is $\mathbb{Z}_n$ then it holds that if $\gcd(a, n) = 1$, then

$$a^{\Phi(n)} \equiv 1 \mod n \tag{6.19}$$

.

Proof. The same as Fermat's little theorem. □

In particular if p is prime then

$$a^p \equiv a \mod p \tag{6.20}$$

for all a. Similarly, if p, q prime, then if $\gcd(a, pq) = 1$

$$a^{(p-1)(q-1)} \equiv a^{\Phi(pq)} \equiv 1 \mod pq \tag{6.21}$$

Therefore

$$a^{(p-1)(q-1)m} = 1 \mod pq \tag{6.22}$$

Therefore

$$a^{(p-1)(q-1)m+1} \equiv a \mod pq \tag{6.23}$$

even if a happens to be divisible by p or q. (Fill in the details.)

This observation is in fact the key idea behind RSA.

1. Take two (large) primes p, q and choose d s.t. $\gcd(d, (p-1)(q-1)) = 1$.
2. Compute $n = pq$, and $e = d^{-1}$ (in $\mathbb{Z}_{(p-1)(q-1)}$)
3. Make n and e public, but keep p, q, d secret.
4. Assume you want to send me a message i.e. a secret number C. ($1 \leq C \leq n-1$) Do this by computing and sending $D = C^e \mod n$ as a message.
5. How do I recreate C?

$$D^d = (C^e)^d = C^{ed} = C^{(p-1)(q-1)m+1} \underset{\substack{\uparrow \\ \text{Euler}}}{\equiv} C \mod pq. \tag{6.24}$$

6.4 The Chinese remainder theorem

How do we solve a system of congruences (with respect to different moduli)?

For example

$$x \equiv 3 \mod 5, \qquad x \equiv 1 \mod 7, \qquad x \equiv 2 \mod 11 \tag{6.25}$$

Theorem 6.22

Let $n_1, n_2, \dots, n_k \in \mathbb{Z}$ be pairwise relatively prime. Then the system

$$x \equiv a_1 \mod n_1, \qquad x \equiv a_2 \mod n_2 \quad \dots \quad x \equiv a_k \mod n_k \tag{6.26}$$

has a unique solution mod $n_1 n_2 \dots n_k$.

Proof. Let $N = n_1 n_2 \dots n_k$, $N_j = \frac{N}{n_j}$.
Start with uniqueness.

1. Assume $x, \tilde{x}$ are solutions mod N. Then $x - \tilde{x} \equiv a_1 - a_1 \equiv 0 \mod n_1$, so $n_1 \mid x - \tilde{x}$.
2. Same holds for the other ns, so $n_j \mid x - \tilde{x}$ for $j \in \{1, \dots, k\}$.
3. Since these are relatively prime, that means that $N \mid x - \tilde{x}$. This is equivalent to $x \equiv \tilde{x} \mod N$.

Now to the existance of a solution

1. From the definitions it follows, that $\gcd(N_j, n_j) = 1$
2. So
$$s_j N_j + t_j n_j = 1 \tag{6.27}$$
is solvable (for s_j, t_j).[a]
3. Multiply by a_j:
$$a_j s_j N_j + a_j t_j n_j = a_j \tag{6.28}$$
So
$$a_j s_j N_j = a_j - a_j t_j n_j \tag{6.29}$$
4. Look at this $\mod n_l$
$$a_j s_j N_j \equiv \begin{cases} 0 \mod n_l & l \neq j \\ a_j \mod n_j & l = j \end{cases} \tag{6.30}$$
5. Let $x = a_1 s_1 N_1 + a_2 s_2 N_2 + \dots + a_k s_k N_k$.
This is our solution!

□

[a] We will see an example soon.

Example 6.23

$$x \equiv 3 \mod 5, \qquad x \equiv 1 \mod 7, \qquad x \equiv 2 \mod 11 \tag{6.31}$$

Here $N = 5 \cdot 7 \cdot 11 = 385$, $N_1 = 77, N_2 = 55, N_3 = 35$. So we need t solve:

$$s_1 \cdot 77 + t_1 \cdot 5 = 1, \qquad s_2 \cdot 55 + t_2 \cdot 7 = 1, \qquad s_3 \cdot 35 + t_3 \cdot 11 = 1 \tag{6.32}$$

So $77 = 15 \cdot 5 + 2$, $5 = 2 \cdot 2 + 1$, therefore

$$1 = 5 - 2 \cdot 2 = 5 - 2 \cdot (77 - 15 \cdot 5) = -2 \cdot 77 + 31 \cdot 5 \tag{6.33}$$

so $a_1 s_1 N_1 = 3 \cdot (-2) \cdot 77 = -462$.

Do the same for the other equations:

$$a_2 s_2 N_2 = 1 \cdot (-1) \cdot 55 = -55 \qquad a_3 s_3 N_3 = 2 \cdot (-5) \cdot 35 = -350$$

Therefore $x = -462 - 55 - 350 \equiv \cdots \equiv -97 \mod 385 \equiv 288 \mod 385$.

6.5 Fields and vector spaces

We can do linear algebra over any field. A **vector space** V over a field F with an operation (vector addition) $+ : V \times V \to V$ and an operation (multiplication by scalar) $\cdot : F \times V \to V$ that fullfill certain axioms.

Example 6.24

Assume that F is a field and $K \subseteq F$ is a subfield. Then we can view F as a vector space over K.

Example 6.25

For example viewing $\mathbb{C}$ as a vector space over $\mathbb{R}$ then $1, i$ would be a basis. Viewing $\mathbb{R}$ as a vector space over $\mathbb{Q}$ a basis cannot be easily written down, because it is an (uncountable) infinite dimensional vector space.

In particular if F is finite, then F is a finite dimensional vector space over K. There is a basis $e_1, e_2, \dots, e_n \in F$ s.t. every $x \in F$ can be written uniquely as $x = \alpha_1 e_1 + \alpha_2 e_2 + \dots + \alpha_n e_n$ where $\alpha_j \in K$.

So $|F| = |K|^n$

We can do better!

Start with any finite field F and let

$$K = \{1, 1+1, 1+1+1, \dots\} = \{1 \cdot 1, 2 \cdot 1, 3 \cdot 1, \dots\} \subseteq F \tag{6.34}$$

Since K is finite, $r \cdot 1 = s \cdot 1$ for some $r < s$. So $(s - r) \cdot 1 = 0$.

Let n be the smallest possible integer, s.t. $n \cdot 1 = 0$. This must be a prime! (Because if $n = ab$, then $(ab)1 = 0 = a(b1) = 0$.)

Therefore $|F| = |K|^n = p^n$.

Conversely, if p is prime and $n \geq 1$ is an integer, there exists a field with p^n elements. (And this field is actually unique up to isomorphy.)

We are not going to prove this in full generality, but the idea is to do like we did when we "constructed $\mathbb{C}$" as $\mathbb{R}[x]/\langle x^2+1\rangle$ last week.

Let us do a concrete example.

Example 6.26

Let $R = \mathbb{Z}_5[x]/\langle x^2+2\rangle$, then F is a commutative ring with unity but in fact F is a field!

The elements in F can be identified with degree ≤ 1 polynomials $a + bx$ where $a, b \in \mathbb{Z}_5$, and

$$(a+bx)(c+dx) = ac + (bc+ad)x + bdx^2 = ac - 2bd + (bc+ad)x \tag{6.35}$$

And if $a + bx$ is not the zero polynomial in F (i.e. not both of a and b are zero) then we can solve

$$ac - 2bd = 1, \quad bc + ad = 0 \tag{6.36}$$

since $\det \begin{pmatrix} a & -2b \\ b & a \end{pmatrix} = a^2 + 2b^2 \neq 0$.

This shows that F is a field and clearly $|F| = 5^2 = 25$.

(The reason this construction works is actually that x^2+2 is **irreducible** over $\mathbb{Z}_5$, i.e. cannot be written as a product of lower degree polynomials.)

7 Introduction to Coding theory

Generally **coding** means representing information in different forms. Examples:

- turning speech into written text
- digital representation of images (e.g. jpeg)
- More code
- Translation into a different language
- Turning an algorithm into a computer program

From a mathematical perspective probably the most important types of codes are

- data compression codes:
  "shrinking a message to some storage space or transmission time". Usually with a loss of information.
- Cryptographic codes:
  turning information into a form that only the intendent recipient can recreate. (Variang: digital signatures)
- Error-detecting and error correcting codes:
  Adding redundant information which allows recovery from some transmission errrors.

We will in this course focus on the third kind.

Example 7.1 (Control digits)

For example Swedish personal identification number are error detecting, at least in the sense that swpping consecutive digits make the pin invalid.

How does this work?

For example, look at (the valid) PIN 941208-6390 and do the following: Take the digits, multiply alternatively by 2 and 1 and replace the product with sum of digits.

```
941208639x
2121212121

942208339x
```

Now sum: 9+4+2+2+0+8+3+3+9+x=40+x.

x should be choses to make this sum equal to 0 (mod 10), here x=0, so the original pin was valid.

You can check that swapping two consecutive digits in a valid PIN makes it invalid (with one exception, swapping 09 goes unnoticed.)

This is an example of a code that can detect one error (of a particular type). But if we swap more than two numbers or make other errors, they may go unnoticed. There is also no way to see exactly which two digits were swapped (unless we create a non-valid date).

7.1 Some definitions

Definition 7.2:

In most general context, a **coding function** is an injective function $f : F^m \to F^n$ for some field F and $m > n$. The image

$$C = f(F^m) = \{y \in F^n : y = f(x) \text{ for some } x\} \tag{7.1}$$

is called a **code**.

Example 7.3

$F = \mathbb{Z}_7, f : \mathbb{Z}_7^3 \to \mathbb{Z}_7^4$ where $f(x_1, x_2, x_3) = (x_1, x_2, x_3, x_1 + x_2 + x_3)$ is a (linear) code and $C = f(\mathbb{Z}_7^3$ containes $7^3 = 343$ words.

For example $f(2, 3, 4) = (2, 3, 4, 2)$ is a code word, but $(2, 3, 4, 5)$ is not.

Example 7.4

$F = \mathbb{Z}_2[x]/\langle x^2 + x + 1\rangle$ is a field of four elements. Define $f : F^2 \to F^3$ by $f(p_1, p_2) = p_2, xp_1, p_1 - p_2$ is a code. Verify injectivity!

In order to study error-detection and error-correction systematically, we neet to measure the "distance" between code words.

Definition 7.5 (Hamming distance):

The **Hamming distance**, $d(x, y)$ between $x = (x_1, \dots, x_n)$ and $y = (y_1, \dots, y_n)$, $x, y \in F^n$ is the number of indices j such that $x_j \neq y_j$.

Example 7.6

In $\mathbb{Z}_7^4$, $d\left((2, 3, 4, 2), (2, 1, 5, 1)\right) = 3$.

Definition 7.7 (Separation of a code):

Let C be a code in F^n. The **separation** of C, $d(C)$ is defined by

$$d(C) = \min\left\{d(x, y) : x, y \in C, x \neq y\right\}. \tag{7.2}$$

Example 7.8

In $\mathbb{Z}_2^3$, what is the largest possible separation of a code containing (exactly) two code words? Three words?

For $|C| = 2$, we can take $C = \{000, 111\}$ and this is obviously optimal. $(d(C) = 3)$

For $|C| = 3$, $d(C) = 3$ is impossible. (why?) Can we have $d(C) = 2$?

Yes, for example, $C = \{000, 110, 101\}$. In fact, we can even have $|C| = 4$ with $d(C) = 2 : C = \{000, 110, 101, 011\}$.

Now this C is an example of a code that can detect some error.

For example, if we receive the signal 010, we know its not a code word (unless the transmission had more than one mistake). Similarly, if we receive 000, we can be sure, it's correct (or has more than one mistake).

If we do the same for the code $C = \{000, 111\}$ where $d(C) = 3$ we get a code that can correct one error. If we receive 010, it contains an error, but the only valid code word at distance 1 is 000.

Similarly we get the following result

Theorem 7.9

Let C be a code with separation $d(C)$.

1. If $d(C) \geq k + 1$ then C can detect up to k errors.
2. If $d(C) \geq 2k + 1$, then C can correct up to k errors.

Proof. 1 if $c \in C$ and changed into c', s.t. we've made at most k changes, i.e. $d(c, c') \leq k$, then $c' \notin C$ since $d(C) = k + 1$.
2 If $c \in C$ is changed into c', $d(c, c') \leq k$, then c is the only code word in C with distance $\leq k$ from it, since, if $\tilde{c}$ was another such word, then

$$d(c, \tilde{c}) \leq d(c, c') + d(c', \tilde{c}) \leq k + k = 2k. \tag{7.3}$$

which contradicts the assumption, that the separation of C is $2k+1$. (This uses the triangular inequality, which holds, since the Hamming distance is a metric.) □

7.2 Perfect codes

Let F be a finite field with q elements. Assume that we want a code $C = f(F^m) \subseteq F^n$ with separation $2k + 1$ (i.e. a code that is capaple of correcting up to k errors), how many code words can C (have a most)?

Note that if $x \in C$, then the "ball"

$$B(x, k) = \{y \in F^n : d(x, y) \leq k\} \tag{7.4}$$

cannot contain any other code words from C (other than x). How many elements are there in $B(x, k)$?

$$|B(x, k)| = \sum_{j=0}^{k} \binom{n}{j} (q - 1)^j \tag{7.5}$$

(Why?)

Hence we have the following estimate on the number of possible code words in C.

Theorem 7.10

If F has q elements and $C \subseteq F^n$ contains M words, and $d(C) = 2k+1$, then

$$M \cdot \left(\sum_{j=0}^{k} \binom{n}{j} (q-1)^j \right) \leq q^n. \tag{7.6}$$

Example 7.11

Let $C = \{0000, 0112, 0221, 1011, 1120, 1202, 2022, 2101, 2210\} \subseteq \mathbb{Z}_3^4$. We can check that $d(C) = 3$, so each $x \in C$ has a ball $B(x,1)$ not containing additional elements from C.

$$|B(x,1)| = \binom{4}{0} + \binom{4}{1}(3-1) = 9. \tag{7.7}$$

Hence the nine code words in C, together with these "forbidden balls" comprise $9 \cdot 9 = 81$ elements in $\mathbb{Z}_4^3$. But $|\mathbb{Z}_4^3| = 3^4 = 81$, so every element in $\mathbb{Z}_4^3$ is accounted for!

Definition 7.12 (perfect codes):

Such codes, i.e. codes where the estimate in the last theorem is sharp (i.e. $\leq$ is in fact $=$) are called **perfect codes**.

Example 7.13

Is there a perfect code of separation 5 in $\mathbb{Z}_7^4$?
By the above ($q = 7, n = 4, k = 2$) such a code satisfies

$$M \cdot \left(\binom{4}{0} + \binom{4}{1} 6 + \binom{4}{2} 6^2 \right) \leq 7^4, \tag{7.8}$$

where $M = |C|$. Hence $M \leq \frac{7^4}{241} \leq 9.96$, so there is no such perfect code!
And any separation 5 code in $\mathbb{Z}_7^4$ can have no more than 9 elements.

7.3 Linear codes

Definition 7.14 (Linear code):

A code $C \subseteq F^n$ is called **linear** if it is a linear subspace of F^n (recall that F^n is a vector space over F, i.e. with scalars in F)

If $\dim(C) = m$, then C is called an $[n, m]$ code.

Example 7.15

The code $C = \{0000, 0112, 0221, 1011, 1120, 1202, 2022, 2101, 2212\} \subseteq \mathbb{Z}_3^4$ (which we saw above) is a linear code generated by (1011) and (0112), i.e. a linear $[4, 2]$ code.

For linear codes it is easy to compute their separation.

Definition 7.16:

The **weight** of code word $x \in F^n$ is the number $w(x)$ of non-zero coordinates. Similarly, the weight of a (linear) code C is

$$w(C) = \min\{w(x) : x \in C, x \neq 0\} \tag{7.9}$$

Theorem 7.17

For a linear code, $d(C) = w(C)$

Proof. If $x, y \in C$, then $x - y \in C$ (by linearity) and $d(x, y) = w(x - y)$. □

Example 7.18

The linear code in $\mathbb{Z}_3^4$ generated by (1011) and (0112) consists of all elements of the form $a(1011) + b(0112)$, where $a, b \in \mathbb{Z}_3$, i.e.

$a\backslash b$	0	1	2
0	0000	0112	0221
1	1011	1120	1202
2	2022	2101	2210

Note that all the non-zero elements in C have weight 3, so $d(C) = 3$.

Definition 7.19 (generator matrix):

A **generator matrix** for a linear $[n, m]$ code in F^n is an $m \times n$ matrix whose rows for a basis for C.

Example 7.20

The $[4, 2]$ code above has a generator matrix $\begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 2 \end{pmatrix}$

Remark 7.21

Performing elementary row operations on a generator matrix does not change the code it generates.

Therefore after a sequence of row operations we can assume that generator matrices are of **normal form**, i.e. of the form

$$[\mathbb{1}_m | A] \tag{7.10}$$

as above. (Possibly column swaps may be necessary, which corresponds to a permutation of the code letters.

For linear codes there are efficient algorithms for detecting and correcting errors. For a description of how this works we need te concept of the *dual code.*

Definition 7.22:

Let C be a linear code in F^n. The **dual code** of C, $C^{\perp}$ is the linear code

$$C^{\perp} = \{y \in F^n : x \cdot y = 0, \forall x \in C\} \tag{7.11}$$

where $x \cdot y$ is the standard scalar product on F^n.

Remark 7.23

If G is a generator matrix for C then $C^{\perp}$ is the nullspace of G. (and C is the row space.)

By the dimension theorem from linear algebra, $\dim C^{\perp} = n - \dim = n - mC$.

If $C = C^{\perp}$, the code C is called **self-dual**. One example is given by

$$G = \begin{pmatrix} 2 & 0 & 2 & 0 \\ 0 & 2 & 0 & 1 \end{pmatrix} \tag{7.12}$$

in $\mathbb{Z}_5^4$

Definition 7.24:

A generator matrix for $C^{\perp}$ is called a **control matrix** for C.

Remark 7.25

If H is a control matrix for C, then $x \in C \iff xH^T = 0$.

This gives us an efficient way to detect errors!

Theorem 7.26

If $G = [\mathbb{1}_m|A]$ is a generator matrix (of normal form) for the $[n, m]$ linear code C, then

$$H = [-A^T|\mathbb{1}_{n-m}] \tag{7.13}$$

is a control matrix for G.

Proof. Since $\dim C^{\perp} = n - m$, the matrix H should be an $(n - m) \times n$ matrix. Also any matrix $\tilde{H}$ of this size with linearly independent rows satisfying $G\tilde{H}^T = 0$ must

be a control matrix for C. (Since it has $n-m$ linearly independent rows, that are orthogonal to the row space of G, i.e. in $C^{\perp}$.)
Clearly $H = [-A^T|\mathbb{1}_{n-m}]$ has the correct size, and

$$GH^T = [\mathbb{1}_m|A] \cdot \begin{bmatrix} -A \\ \mathbb{1}_{n-m} \end{bmatrix} = -\mathbb{1}_m A + A\mathbb{1}_{n-m} = -A + A = 0. \tag{7.14}$$

□

Example 7.27

Our favorite (perfect) code in $\mathbb{Z}_3^4$ whose generator matrix is

$$G = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 2 \end{pmatrix} \tag{7.15}$$

has a control matrix

$$H = \begin{pmatrix} -1 & -1 & 1 & 0 \\ -1 & -2 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 2 & 1 & 0 \\ 2 & 1 & 0 & 1 \end{pmatrix} \tag{7.16}$$

7.4 Finding the separation from the control matrix

Theorem 7.28

A linear code C with control matrix H has separation s iff there are s linearly dependent columns in H, but any $s-1$ columns are linearly independent.

Proof. Every word $x \in C$ satisfies $xH^T = 0 \implies Hx^T = 0$, i.e. every code word x corresponds the the coefficients in a linear dependence of the columns in H.
If x is a word of minimal weight s, then exactly s of the coefficients in this depedence are non-zero. And if there were $s-1$ linearly dependent column vectors in H, there would be a code word of weight $s-1$, contradicting our choice of x. □

Example 7.29

Let G be a generator matrix in $\mathbb{Z}_2^5$,

$$G = \begin{pmatrix} 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 \end{pmatrix} \tag{7.17}$$

The related control matrix H is given by

$$H = \begin{pmatrix} -1 & -0 & 1 & 0 & 0 \\ -0 & -1 & 0 & 1 & 0 \\ -1 & -1 & 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 \end{pmatrix} \tag{7.18}$$

Here $c_2 + c_4 + c_5 = 0$ (corresponding to the code word $(01011) \in C$. But it's not hard to see that any pair of columns are linearly independent, so the separation of C is 3.

Example 7.30

Exercise: Find a code word in C of weight 3.

7.5 Detection and correction of linear codes

Let C be a linear code with generator matrix G and control Matrix H.

Recall $x^T H = \vec{0} \iff x \in C$ which gives us an efficient algorithm for detecting errors.

How about correction?

We still start by computing $x^T H$ (which is a row vector of length $n - m$).

This is called the syndrome of x.

To correct x, we look at all $y \in F^n$ with the same syndrome as x. (Since $xH^T = yH^T \iff (x-y)H^T = \vec{0} \iff x - y \in C$.

We want to alter x as little as possible so we look for the y with lowest weight (i.e. least number of non-zero elements) such that $yH^T = xH^T$. Such a y is called a **coset leader** (and the whole set $\left\{y \in F^n : yH^T = xH^T\right\}$ is called a **coset**.)

Finally, we replace x by (the code word) $x - y$ which is then the code word closest to x!

Example 7.31

In our perfect $[4,2]$ code over $\mathbb{Z}_3^4$, generated by (1011) and (0112), we know that a control matrix is given by

$$H = \begin{pmatrix} 2 & 2 & 1 & 0 \\ 2 & 1 & 0 & 1 \end{pmatrix} \tag{7.19}$$

Since every word in $\mathbb{Z}_3^4$ is within distance one from a code word (because this is a perfect code with separation 3), it is enough to look at the columns in H to find the coset leaders.

For example the syndrome (10) has the coset leader (0010) corresponding to the third column of H.

We get the full table of syndroms by

syndrome	00	01	02	10	11	12	20
coset leader	0000	0001	0002	0010	2000	0200	0020

Note that all the coset leaders have weight 1 (which is what we expect!)

In particular if we receive the words (0110), (0221), (1111) what was the intended message? (of course assuming that each word contains at most one error)

The syndroms are (01), (00), (21).[a]

The corresponding coset leaders are (0001), (0000), (0100), so the indented message was (0112), (0221), (1011).

[a] For example $(0,1,1,0)\begin{pmatrix}2&2\\2&1\\1&0\\0&1\end{pmatrix}=(01)$.

Remark 7.32
If the code is not perfect, it might happen that a syndrome doesn't have a unique coset leader.

For example, in a non-perfect code with separation 3, some words with 2 errors may still be possible to correct (if the syndrome has a unique coset leader) but others may not.

7.6 Hamming codes

Definition 7.33:

A **Hamming code** is a perfect code of separation 3.

(For example our favorite example.)

As in the example, it follows that the control matrix H contains multiples of all possible syndromes in its columns!

(Since every word is within distance 1 from a valid code word.)

In particular, over $\mathbb{Z}_2$, the control matrix must have some columns containing all possible nonzero words of length $n-m$!

Example 7.34
For example, let

$$H=\begin{pmatrix}1&0&1&1&1&0&0\\1&1&1&0&0&1&0\\1&1&0&1&0&0&1\end{pmatrix} \tag{7.20}$$

where the columns are all non-zero words in $\mathbb{Z}_2^3$. (Note that for convenience, I chose the order so $H=[A|\mathbb{1}_3]$!)

This is the control matrix for a perfect $[7,4]$ code whose generator matrix is given by

$$G = [\mathbb{1}_4| - A^T] \underset{\substack{\uparrow \\ \text{since } -x = x \text{ in } \mathbb{Z}_2}}{=} [\mathbb{1}_4|A^T] = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{pmatrix}. \tag{7.21}$$

Example 7.35

Correct the word (1010111) in this code (assuming ≤ 1 error).

$$[1010111] \cdot H^T = \begin{bmatrix} 1 \\ 1 \\ 0 \end{bmatrix} \tag{7.22}$$

which is the third column in H, so the error is in the third coordinate and (1000111) is the intended message.

We can do the same for syndroms of arbitrary length. Look at an $[n, m]$ code over $\mathbb{Z}_2$. Then

$$\begin{aligned} n &= \#\text{ of columns in } H &(7.23)\\ &= \#\text{ of possible syndromes} &(7.24)\\ &= 2^{\text{length of syndrome}} - 1 &(7.25)\\ &= 2^{n-m} - 1 &(7.26)\end{aligned}$$

(the length of a syndrome is the number of rows in H, i.e. $n - m$.)

So with $r = n - m$ (the codimension of the code, or the length of the syndromes if you prefer), then

$$n = 2^r - 1, \quad m = n - r = 2^r - 1 - r \tag{7.27}$$

i.e. this gives us a perfect (why?) $[2^r - 1, 2^r - 1 - r]$ code over $\mathbb{Z}_2$.

Remark 7.36

We can construct Hamming codes over any finite field in a similar way by choosing H so its columns contain multiples of every possible syndrome.

7.7 Reed-Solomon codes

Another interesting class of codes are given by **Reed-Solomon codes**.

Say we want to construct a code over the finite field F with given separation σ.

To do this, we want a control matrix H with the property that every choice of $\sigma - 1$ columns in H are linearly independent, but (some choice of) σ columns are not.

One way to do this, is to choose distinct values $\beta_1, \beta_2, \dots, \beta_n \in F \setminus \{0\}$ (for $n \geq \sigma$) and let

$$H = \begin{pmatrix} 1 & 1 & \dots & 1 \\ \beta_1 & \beta_2 & \dots & \beta_n \\ \vdots & \vdots & \ddots & \vdots \\ \beta_1^{\sigma-2} & \beta_2^{\sigma-2} & \dots & \beta_n^{\sigma-2} \end{pmatrix} \tag{7.28}$$

(note that it has size $(\sigma - 1) \times n$) and take this as our control matrix.

Clearly, if we take σ columns, they must be linearly dependent because all columns are in $F^{\sigma-1}$.

Now choose any $\sigma - 1$ columns, which gives us a square matrix

$$\begin{pmatrix} 1 & \dots & 1 \\ \beta_{i_1} & \dots & \beta_{i_{\sigma-1}} \\ \beta_{i_1}^2 & \dots & \beta_{i_{\sigma-1}}^2 \\ \vdots & \ddots & \vdots \\ \beta_{i_1}^{\sigma-2} & \dots & \beta_{i_{\sigma-1}}^{\sigma-2} \end{pmatrix} \tag{7.29}$$

If the columns are linearly dependent, then so are the rows, i..e we could find scalars $c_1, \dots, c_{\sigma-1} \in F$, not all equal to 0 such that

$$\sum_{k=0}^{\sigma-2} c_k (\beta_{i_1}^k, \dots, \beta_{i_{\sigma-1}}^k) = \vec{0} \tag{7.30}$$

i.e. each β_{i_n} solves the equation

$$\sum_{k=0}^{\sigma-2} c_k x^k = 0 \tag{7.31}$$

which means we have $\sigma - 1$ different solution to a polynomial equation of degree $\sigma - 2$, which is a contradiction! (over any field! why?)

Hence H as constructed above is the control matrix of a linear code of separation σ.

Example 7.37

Take $\sigma = 3$, $F = \mathbb{Z}_7$ and n as large as possible:

$$H = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 2 & 3 & 4 & 5 & 6 \end{pmatrix} \tag{7.32}$$

which is the control matrix of a linear [6,4] code (codimension $\sigma - 1 = 2$) which can correct one error.

The error correction algorithm is simple!

If we want to send $x = (x_1, \dots, x_6)$ but $w = (x_1, \dots, x_k + e_k, \dots, x_6)$ is received instead, then the syndrome is

$$wH^T = xH^T + (0, \dots, e_k, \dots, 0)H^T = \begin{pmatrix} e \\ ke \end{pmatrix} \tag{7.33}$$

where e is the error and k is the position of the error! $(xH^T = \vec{0})$.

For example, if we receive $w = (210504)$ we can compute the syndrome $wH^T = (12, 48) = (5, 6)$ in $\mathbb{Z}_7$, i.e. $e = 5, ke = 6$ therefore $k = 5^{-1} \cdot 6 = 3 \cdot 6 = 4$.

So what we received was $x + (0005000) = (210504)$ and the intended message thus was $x = (210004)$.

If we want to correct two errors, we need $\sigma = 6$ and H has two more rows

$$H = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 2 & 3 & 4 & 5 & 6 \\ 1^2 & 2^2 & 3^2 & 4^2 & 5^2 & 6^2 \\ 1^3 & 2^3 & 3^3 & 4^3 & 5^3 & 6^3 \end{pmatrix} \tag{7.34}$$

which gives us a $[6, 2]$ code of separation 5.

These Reed-Solomon codes are, for example, used in CD and DVD records! Two dimensional bar codes (QR codes for example) also use a Reed-Solomon code.

7.8 Reed-Muller codes

Theorem 7.38

If C_1 and C_2 are linear $[n, m_1]$ and $[n, m_2]$ codes of separation σ_1 and σ_2, then $C = \left\{(x, x + y) \in F^{2n}; x \in C_1, y \in C_2\right\}$ is a linear $[2n, m_1 + m_2]$ and separation $\min(2\sigma_1, \sigma_2)$.

Proof.

1. That C is linear is clear.
2. Dimension: Let $\left\{e_1, \dots, e_{m_1}\right\}$ and $\left\{f_1, \dots, f_{m_2}\right\}$ be bases for C_1 and C_2. Then $\left\{(e_1, e_1), (e_2, e_2), \dots, (e_{m_1}, e_{m_1}), (0, f_1), (0, f_2) \dots, (0, f_{m_2})\right\}$ is a basis for C. So the dimension is $m_1 + m_2$.
3. As for the separation (=weight) we can look at the words in C.
   a) If $a = (x, x) \in C$, then $w(a) = 2w(x)$ (in C_1).
   b) If $a = (x, x + y), y \neq 0$ then $w(a) \geq w(y)$. Because if $y_i \neq 0$ then either $x_i \neq 0$ or $x_i + y_i \neq 0$.

c) And in fact the smallest possible weight of such a word is $\sigma(y_2)$, because we can take $x = 0$, and $y \in C_2$ of minimal weight.

□

Remark 7.39

This setup can be used to construct "big codes". (Reed-Muller codes)

1. Start with C_1 generated by (10) and (01) in $\mathbb{Z}_2^2$ (This is the "trivial code".!), i.e. a $[2, 2]$ code of separation 1. And C_2 generated by (11) which is a $[2, 1]$ code of separation 2.
2. Combine as in the theorem!
3. We get $C' \subseteq \mathbb{Z}_2^4$ generated by $\{(1010), (0101), (0011)\}$ which is a $[4, 3]$ code of separation $\min(2 \cdot 1, 2) = 2$.
4. Repeat! Combine C' with the $[4, 1]$ code generated by (1111).
5. We get $C'' \subseteq \mathbb{Z}_2^8$ generated by $\{(10101010), (01010101), (00110011), (00001111)\}$, i.e. an $[8, 4]$ code of separation 4.
6. Next step $[16, 5]$ code of separation 8, then $[32, 6]$ code of separation 16...

Remark 7.40 (Perfect codes)

We know that there are lots of perfect codes of separation 3 over any finite field (the Hamming codes). Are there perfect codes capable of correcting more than one error?

In 1949, Golay constructed a perfect $[11, 6]$ code over $\mathbb{Z}_3$ and $[23, 12]$ codes over $\mathbb{Z}_2$ with separation 7.

In 1973 it was shown that these are the only ones!