Discrete Structures

Prof. Stefan Wolf
Arne Hansen

September 17, 2015

Contents

What is discrete mathematics all about?

Before venturing into formal details, let's briefly clearify what we refer to if we speak about *discrete mathematics*.

What is *mathematics*?

The pillars of mathematics are *logics* and *set theory*. While logics determins how to reason within mathematics (what is considered a proof, . . .), set theory describes the objects we deal with.

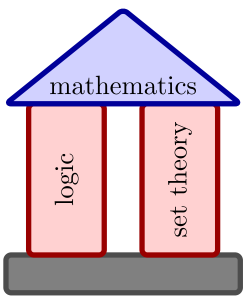
Example 0.0.1 (Set theory). It is actually possible to define all natural numbers from the emptyset:

$$\begin{aligned}0 &:= \emptyset\\ 1 &:= \{\emptyset\}\\ 2 &:= \{\{\emptyset\}, \emptyset\}\\ &\vdots\end{aligned}$$

This exemplifies how set theory serves to define mathematical objects.

What does *discrete* mean?

With *discrete* we usually refer to *finite or countably infinite sets*. While it is intuitively clear what is meant by *finite* (a set of elements we can label with



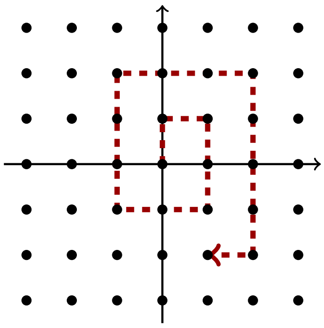


Figure 1: Matching the rational and the natural numbers

natural numbers $1, 2, 3, \ldots, N$) *countably infinite* needs slightly more explanation. A set S is called *countably infinite* if one can match each element in S with a unique natural number. More formally such a matching would be a function and we get the following definition.

Definition 1 (Countable set)**.** A set S is called *countable* if there exists a one-to-one or injective[1] function $f : S \to \mathbb{N}$. If f is also surjective[2] then S is called countably infinite.

To better understand the concept of countability, we'll consider two common examples.

Example 0.0.2 (The rational numbers are countable)*.* Even though there seem to be a lot more rational numbers than natural numbers, we can construct a matching showing that the set is countably infinite. The rational numbers can be associated with dots in a two-dimensional space, with the numerator on the x-axis and the denominator on the y-axis or vice versa. We can then number the dots in a spiral as shown in figure 1.

Example 0.0.3 (The real numbers are not)*.* We cannot find such a matching for the real numbers as one can prove by contradiction. Let's assume that there is a matching for all real numbers in the interval $[0, 1]$ with a binary representation

$$\begin{array}{ll} 1 & 0.0101011100110\ldots \\ 2 & 0.1001100101001\ldots \\ 3 & 0.0001011001010\ldots \\ \vdots & \vdots \end{array}$$

But one can construct a real number that is not contained in the list: the i^{th} digit of the binary representation is just the flipped value of the i^{th} digit of the i^{th} real number.

[1]This is to say, each element gets assigned a unique natural number, or in other words, no natural number is matched to two different elements in S

[2]That is, every natural number is matched to an element in S

$$
\begin{array}{rl}
1 & 0.\mathbf{0}1010111001 10\ldots \\
2 & 0.1\mathbf{0}01100101001\ldots \\
3 & 0.00\mathbf{0}1011001010\ldots \\
\vdots & \vdots \\
\text{constructed real number} & 0.111\ldots
\end{array}
$$

The number we constructed differs from every element in the list and is therefore not contained in the list. This yields a contradiction with the initial assumption that there existed a matching. Thus the size of the set of real numbers is strictly larger than the size of the natural number (in the sense that there is no bijective map inbetween the two.).

$$|\mathbb{R}| > |\mathbb{Q}| = |\mathbb{N}| \tag{1}$$

Why bother?

What is the relevance of discrete mathematics? On the one hand logic is discrete as the basic set is $\{TRUE, FALSE\}$. On the other hand, computer science is not only closely related to logics, but as computers have only finite states informatics is in a sense discrete.

Chapter 1

Motivation

The following examples are typical problems in discrete mathematics.

1.1 Swapping knights

Consider a reduced chess board with two knights of each color as shown in figure 1.1. Is it possible to transform the configuration on the left into the configuration on the right using regular knight moves?

The knights never reach the middle field. Further if one moves along the line of moves one finally returns back to the initial position. This can be represented nicely in a graph. Each possible field is then a *node* in the graph. The possible moves are then the *edges* of the graph. Rearranging the nodes yields one closed loop with 8 nodes. The knights can merely move around the loop but not change their order. Thus the answer is, that the transformation is impossible.

Lessons learnt from the example above:

Modelling Find the right model to represent the problem.

Graph are often a good structure to model discrete problems

Abstraction Concentrate on the relevant and get rid of the irrelevant.

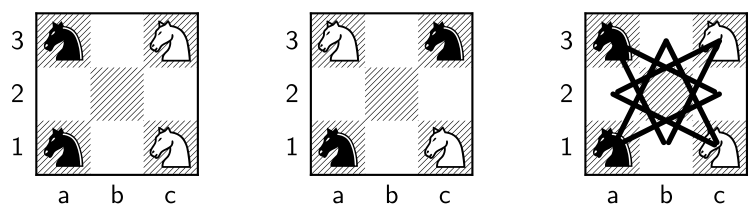


Figure 1.1: Reduced chessboard with knights

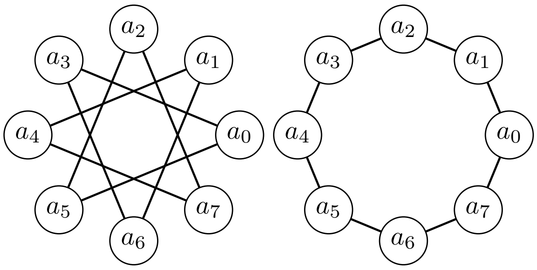


Figure 1.2: Graphs corresponding to the knights swapping problem

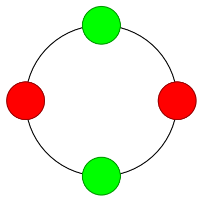


Figure 1.3: Necklace with further symmetries, but p not being prime.

1.2 Combinatorics

Imagine you want to create a necklace with p pearls, with p being prime. There are pearls of a different colors available. How many different necklaces can you make? If we can distinguish the pearls, there would be a^p different possible necklaces. But the necklace has a rotational symmetry. That is two necklaces that are made up from the same sequence of pearls except that they are rotated by an angle are indistinguishable. Just diving by p does not yield the right solution though, as the one-colored necklaces just appear once. As p is a prime number these are they only exceptions. Configuration like in 1.3 cannot occur. Therefore the right answer is

$$N = \frac{a^p - a}{p} + a \tag{1.1}$$

More generally we obtain for a prime number p, $a^p - a$ is divisable by p. This is called Fermat's small theorem and plays a role in cryptography, namely the public-key protocol RSA.

1.3 Connections without crossings

Imagine a settlement with three houses and three plants (power, waste water, ...) as shown in figure 1.4. The question is, whether it is possible to connect the three houses to each of the plants without crossing other connections.

This problem can again be turned into a graph, namely $K_{3,3}$ as shown in figure 1.5. The question is then: can the associated graph be drawn that edges merely meet in nodes? If so the graph is called *planar*. An example of a planar graph is K_4 shown in figure 1.6.

So we ultimately want to show, that $K_{3,3}$ is not planar. To do so we first try to better understand the properties of planar graphs.

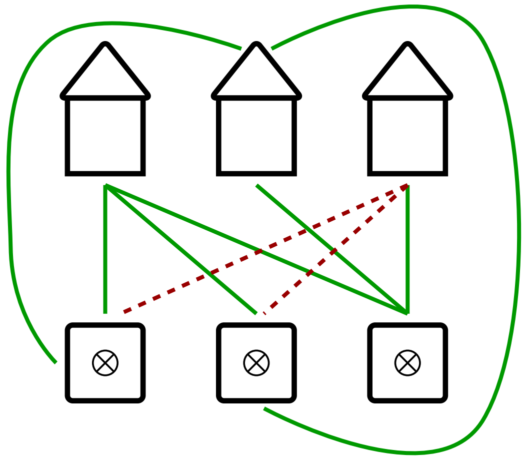


Figure 1.4: Houses with connections. The third house cannot be connected anymore without intersecting other connections.

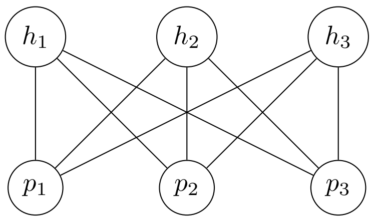


Figure 1.5: The "houses connection problem" can be associated to the graph $K_{3,3}$

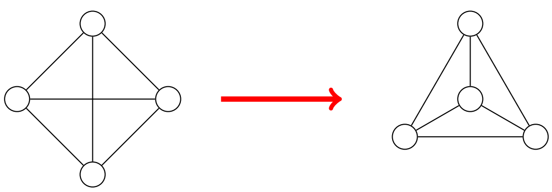


Figure 1.6: The graph K_4 is an example of a planar graph

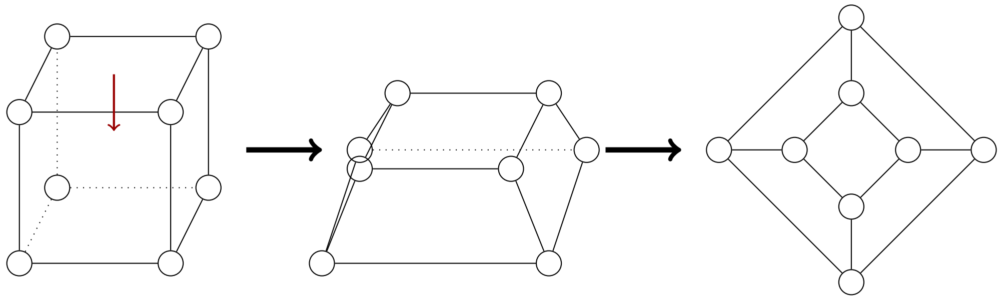


Figure 1.7: A cube can be transformed into a graph by removing the bottom (turns into outer region) and pressing the top down while spreading out the lower nodes.

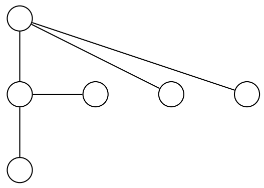


Figure 1.8: A simple tree

Graphs and polyhedrons There is an interesting analogy between graphs and polyhedrons. A polyhedron can be associated with a graph: Imagine the polyhedron was made out of elastic rubber. One could now remove one face and press the remaining part on a piece of paper. This would yield a planar graph. Edges of the Polyhedron become edges of the graph, corners turn into nodes of the graph. Note that the face that was initially removed corresponds now to the infinite region outside the graph (which as always considered as a proper region). Figure 1.7 shows the graph corresponding to a cube.

Looking at different polyhedra (or at planar graphs) it becomes apparant that the number of vertices (nodes) n, the number of edges e and the number of faces f (regions) are closely reelated. Indeed *Euler's polyhedron formula* states, for any polyhedron (and equivalently for planar graphs) it holds

$$n - e + f = 2 \tag{1.2}$$

Before looking at a sketch of the proof we can apply it to $K_{4,4}$ to answer our initial question. Indeed $n - e + f = 6 - 9 + 13 = 10 \neq 2$.

Proof sketch The proof consists of two parts: First we will show the proposition for trees, which form a simpler class of graphs. Then we will generalize this to arbitrary planar paths.

Euler for trees A tree is a path without any cycles. As it contains only one region, namely the outer one, it is always planar. We can now show by induction that Euler's law is always satisfied for trees.

If there is just one node, then the formula is satisfied as $n = 1$, $e = 0$ and $f = 1$. For the *induction step* we now assume that the law holds for a tree with

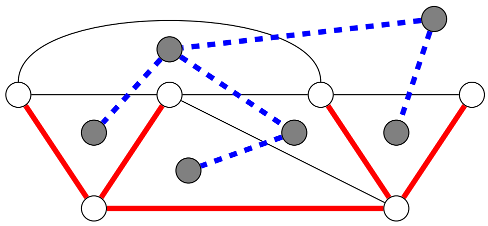


Figure 1.9:

n nodes and follow that it will hold for a tree with $n+1$ nodes. Adding node requires to add an edge as well. So the new tree will have $e+1$ edges and $n+1$ nodes and therefore

$$\underbrace{\tilde{n}}_{=n+1} - \underbrace{\tilde{e}}_{=e+1} + \underbrace{\tilde{f}}_{=1} = n - e + f = 2 \tag{1.3}$$

where the second equality holds due to the induction assumption.

Generalization A general planar graph can now be characterized by a spanning tree and the dual graph. A spanning tree is a subgraph, connecting all nodes, that is at the same time a tree. The dual graph to a given spanning tree is the constructed by placing a node in each region and connecting them without crossing the spanning tree.

The spanning tree is has the same number of nodes as the original graph $n_d = n$ and the number of edges just one less $e_s = n_s - 1$. The number of nodes in the dual tree are just the same as the number of regions in the graph, $n_d = f$. Further each edge of the graph is either part of the spanning tree or crossed by one of the edges of the dual tree. Putting all this together we obtain

$$e = e_s + e_d = (n_s - 1) + (n_d - 1) = n - 1 + f - 1 = n + f - 2 \tag{1.4}$$

which is just Euler's formula. The subsequent example will employ the formula as well.

1.4 Coloring maps

Imagine we were given a map showing countries and their borders[1]. Every two countries sharing a border are considered neighbors. So how many colors are needed to color the map in a way that no neighbors have the same color? Three colors are not enough as can be seen in figure 1.10.

Again the problem can be translated to planar graphs without multi-nodes[2]. Each country is replaced by a node and neighbouring countries are connected by edges. So can the nodes be colored with 4 colors requiring that neighbors are always colored differently? The answer is yes as a computer-aided proof showed. As the proof can never be verified directly by human being there has

[1]For simplicity we'll assume that there are no exclaves like Campione d'Italia.
[2]Multi-nodes are nodes with more than one edge connecting the two.

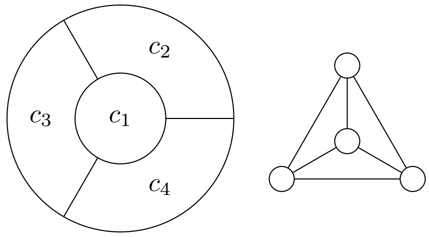


Figure 1.10: The figure on the left shows, that it is possible to arrange four countries such that they are all neighbors to one another. Thus we need at least four colors. The corresponding graph is shown on the right.

been some suspision towards the validity of the proof. A shorter proof shows that 5 colors are sufficient. In the following we sketch a proof for 6 colors.

Proposition 1.4.1 (6-Coloring). Six colors suffice to color a map (or equivalently the nodes of a planar, non-multi graph).

Proof. As there is a finite number of nodes (countries) we will prove the proposition by induction.

Base case For 6 or less nodes the proposition holds, as there are at least as many colors as nodes.

Induction hypothesis We will assume that the proposition holds for k nodes.

Induction step The major part of the proof is now to show that, given the induction hypothesis, the proposition hold also for $k+1$ nodes. The idea to do that is as follows

- Elimininate a node v
- By the induction hypothesis there exists a coloring for the reduced graph.
- One needs to find a coloring for the node v such that the proposition still holds. The goal choose the node v such that it has 5 or less neighbors and we can still choose one color.

While the first two points are clear, we still need to prove the last one — essentially the following lemma.

Lemma 1.4.1. *In every planar graph without multi-nodes there exists at least one node v with 5 or less neighbors.*

Lemma. We will prove the lemma by contradiction. We will assume that the lemma was actually false, i.e. that each (!) node has at least 6 neighbors. Based on this assumption we will construct a contradiction with Euler's formula.

As every node has at least 6 neighbors and each edge connects two nodes the edges and the nodes are related as follows

$$2e \geq 6n \tag{1.5}$$

Similarly the regions and the edges are related. Every region is bounded by at 3 edges (NB: two edges only suffice for multi-graphs). So we obtain

$$2e \geq 3f \tag{1.6}$$

Putting all this together we obtain

$$n + f \leq \frac{e}{3} + \frac{2}{3}e = e \quad \Rightarrow \quad n + f - e \leq 0 \tag{1.7}$$

This is in contradiction with Euler's formula and therefore completes the proof of the lemma. □

The proof of the lemma is the last missing piece. We now know that we can always find a node v with 5 or less neighbors to reduce a graph with $k+1$ nodes to a graph with k nodes. This completes the induction step and thus the proof of the proposition.

□

Appendices

Appendix A

Proof techniques

In this appendix we will briefly review common proof techniques used throughout the course.

A.1 Proof by contradiction

In order to prove a proposition to be true, one can show that the assumption of the proposition being false leads to a contradiction. So the usual approach is to negate the proposition and then construct a contradiction.

Example A.1.1 ($\sqrt{2}$ is irrational).

Proposition A.1.1. The squareroot of 2 is irrational.

Proof. The negative of the proposition is "$\sqrt{2}$ is rational".

Given the negative proposition we will now construct a contradiction. If $\sqrt{2}$ is rational there is an irreducible fraction

$$\frac{a}{b} = \sqrt{2} \quad a, b \in \mathbb{N} \quad \Rightarrow \quad a^2 = 2b^2 \tag{A.1}$$

As a^2 is even, a has to be even. Thus $a^2 = 4a'^2$ for some other natural number $a' \in \mathbb{N}$. Therefore $b^2 = 2a'^2$ and consequently b is even as well. This contradicts a/b being an irreducible fraction. □

A.2 Proof by induction

If the proposition is a statement for all natural numbers, *induction* is usually a convenient approach.

One shows first that the proposition holds for a first natural number (the base case). Then one proves that assuming the proposition holds for a general natural number n it also holds for $n + 1$. The second part of the proof is called the *induction step*. Applying the induction step over and over again starting from 1 one obtains that the proposition holds for 2,3,4,... and eventually all natural numbers.