CIS160
Mathematical Foundations of Computer Science
Some Notes

Jean Gallier
Department of Computer and Information Science
University of Pennsylvania
Philadelphia, PA 19104, USA
e-mail: jean@cis.upenn.edu

August 31, 2010

Chapter 1

Mathematical Reasoning, Proof Principles and Logic

1.1 Motivations, Some Problems

One of the main goals of this course is to learn how to

construct and *read mathematical proofs*.

Why?

1. Computer scientists write *programs* and build *systems*.
2. It is very important to have *rigorous methods* to check that these programs and systems behave as expected (are *correct*, have *no bugs*).

3. It is also important to have methods to *analyze the complexity* of programs (*time/space complexity*).

More generally, it is crucial to have a firm grasp of the *basic reasoning principles and rules of logic*.

This leads to the question:

What is a proof?

There is no short answer to this question!

However, it seems fair to say that a proof is some kind of *deduction (derivation)* that proceeds from a set of *hypotheses (premises, axioms)* in order to derive a *conclusion*, using some *logical rules*.

Figure 1.1: Dog Logic

A basic rule of logic is *modus ponens*:

If P implies Q holds and if P holds, then Q holds

A first important observation is that there are different *degrees of formality* of proofs.

1. Proofs can be very *informal*, using a set of loosely defined logical rules, possibly omitting steps and premises.
2. Proofs can be *completely formal*, using a very clearly defined set of rules and premises. Such proofs are usually processed or produced by programs called *proof checkers* and *theorem provers*.

Thus, a human prover evolves in a *spectrum of formality*!

It should be said that *it is practically impossible to write formal proofs*.

This is because it would be extremely tedious and time-consuming to write such proofs and these proofs would be huge and thus, very hard to read.

In principle, it is possible to write formalized proofs and sometimes it is desirable to do so if we want to have absolute confidence in a proof.

For example, we would like to be sure that a flight-control system is not buggy so that a plane does not accidently crash, that a program running a nuclear reactor will not malfunction or that nuclear missiles will not be fired as a result of a buggy "alarm system".

Thus, it is very important to develop tools to assist us in constructing formal proofs or checking that formal proofs are correct and such systems do exit (Examples: Isabelle, COQ, TPS, NUPRL, PVS, Twelf). However, 99.99% of us will not have the time or energy to write formal proofs.

Even if we never write formal proofs, it is important to understand clearly what are the rules of reasoning that we use when we construct informal proofs.

The first part of this course will be devoted to the description of a formal notion of proof, represented as a certain kind of *tree* and using logical rules described in a style known as *natural deduction*.

Having a firm proof-theoretic basis, we will see how the basic notions of set theory can be defined by formulating suitable axioms.

It will then be possible to define the set natural numbers ($\mathbb{N} = \{0, 1, 2, \ldots\}$) and then all sorts of objects used in computer science: trees, graphs, *etc.*

Let us now list various mathematical problems that will be used to illustrate and motivate the kind of material that we need to develop.

Figure 1.2: Missing luggage

Problem 1. Find formulae for the sums

$$\begin{aligned} 1+2+3+\cdots+n &= ? \\ 1^2+2^2+3^2+\cdots+n^2 &= ? \\ 1^3+2^3+3^3+\cdots+n^3 &= ? \\ \cdots\cdots\cdots\cdots & \\ 1^k+2^k+3^k+\cdots+n^k &= ? \end{aligned}$$

Jacob Bernoulli (1654-1705) discovered the formulae listed below:

If

$$S_k(n) = 1^k + 2^k + 3^k + \cdots + n^k$$

then

$$\begin{aligned}
S_0(n) &= 1n \\
S_1(n) &= \frac{1}{2}n^2 + \frac{1}{2}n \\
S_2(n) &= \frac{1}{3}n^3 + \frac{1}{2}n^2 + \frac{1}{6}n \\
S_3(n) &= \frac{1}{4}n^4 + \frac{1}{2}n^3 + \frac{1}{4}n^2 \\
S_4(n) &= \frac{1}{5}n^5 + \frac{1}{2}n^4 + \frac{1}{3}n^3 - \frac{1}{30}n \\
S_5(n) &= \frac{1}{6}n^6 + \frac{1}{2}n^5 + \frac{5}{12}n^4 - \frac{1}{12}n^2 \\
S_6(n) &= \frac{1}{7}n^7 + \frac{1}{2}n^6 + \frac{1}{2}n^5 - \frac{1}{6}n^3 + \frac{1}{42}n \\
S_7(n) &= \frac{1}{8}n^8 + \frac{1}{2}n^7 + \frac{7}{12}n^6 - \frac{7}{24}n^4 + \frac{1}{12}n^2 \\
S_8(n) &= \frac{1}{9}n^9 + \frac{1}{2}n^8 + \frac{2}{3}n^7 - \frac{7}{15}n^5 + \frac{2}{9}n^3 - \frac{1}{30}n \\
S_9(n) &= \frac{1}{10}n^{10} + \frac{1}{2}n^9 + \frac{3}{4}n^8 - \frac{7}{10}n^6 + \frac{1}{2}n^4 - \frac{3}{20}n^2 \\
S_{10}(n) &= \frac{1}{11}n^{11} + \frac{1}{2}n^{10} + \frac{5}{6}n^9 - n^7 + n^5 - \frac{1}{2}n^3 + \frac{5}{66}n
\end{aligned}$$

Is there a pattern?

What are the mysterious numbers

$$1 \quad \frac{1}{2} \quad \frac{1}{6} \quad 0 \quad -\frac{1}{30} \quad 0 \quad \frac{1}{42} \quad 0 \quad -\frac{1}{30} \quad 0 \quad \frac{5}{66} \quad ?$$

The next two are

$$0 \quad -\frac{691}{2730}$$

Why?

It turns out that the answer has to do with the *Bernoulli polynomials*, $B_k(x)$, with

$$B_k(x) = \sum_{i=0}^{k} \binom{k}{i} x^{k-i} B^i,$$

where the B^i are the *Bernoulli numbers*.

There are various ways of computing the Bernoulli numbers, including some recurrence formulae.

Amazingly, the Bernoulli numbers show up in very different areas of mathematics, in particular, algebraic topology!

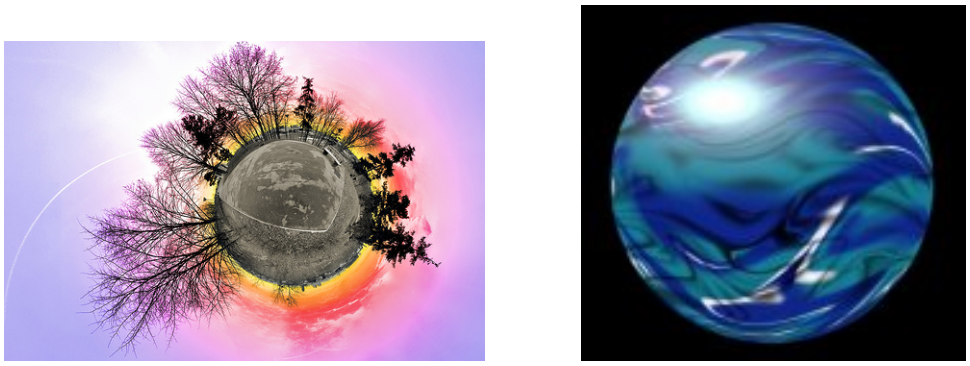

Figure 1.3: Funny spheres (in 3D)

Figure 1.4: A plane (granite slab!)

Problem 2. Prove that a sphere and a plane in 3D have *the same number of points*.

More precisely, find a one-to-one and onto mapping of the sphere onto the plane (a *bijection*)

Actually, there are also bijections between the sphere and a (finite) rectangle, with or without its boundary!

Problem 3. Counting the number of *derangements* of n elements.

A *permutation* of the set $\{1, 2, \ldots, n\}$ is any one-to-one function, f, of $\{1, 2, \ldots, n\}$ into itself. A permutation is characterized by its image: $\{f(1), f(2), \ldots, f(n)\}$.

For example, $\{3, 1, 4, 2\}$ is a permutation of $\{1, 2, 3, 4\}$.

It is easy to show that there are $n! = n \cdot (n-1) \cdots 3 \cdot 2$ distinct permutations of n elements.

A *derangements* is a permutation that leaves no element fixed, that is, $f(i) \neq i$ for all i.

$\{3, 1, 4, 2\}$ is a derangement of $\{1, 2, 3, 4\}$ but
$\{3, 2, 4, 1\}$ is *not* a derangement since 2 is left fixed.

What is the *number of derangements*, p_n, of n elements?

The number $p_n/n!$ can be interpreted as a *probability*.

Say n people go to a restaurant and they all check their coat. Unfortunately, the cleck loses all the coat tags. Then, $p_n/n!$ is the probability that nobody gets her or his coat back!

Interestingly, $p_n/n!$ has limit $\frac{1}{e} \approx \frac{1}{3}$ as n goes to infinity, a surprisingly large number.

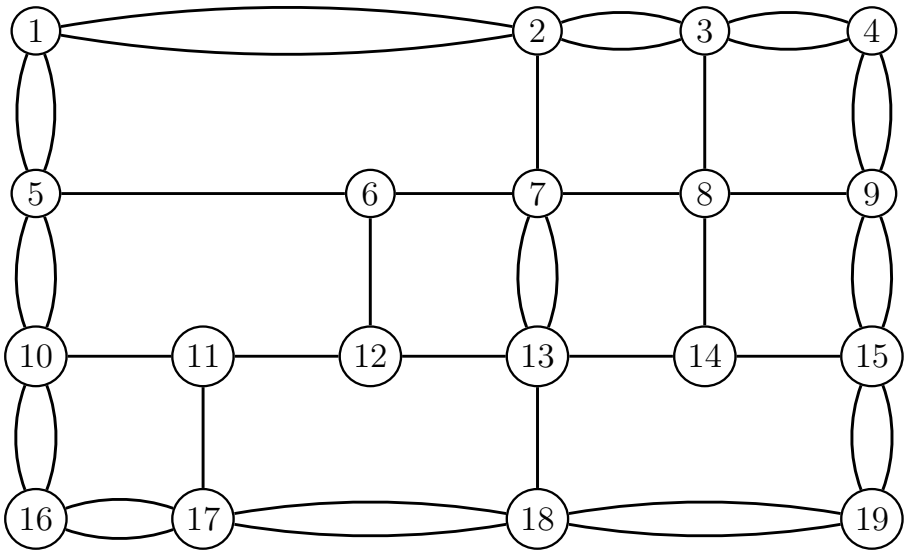

Figure 1.5: An undirected graph modeling a city map

Problem 4. Finding *strongly connected components* in a directed graph.

The *undirected graph* of Figure 1.5 represents a map of some busy streets in a city.

The city decides to improve the traffic by making these streets *one-way* streets.

However, a good choice of orientation should allow one to travel between any two locations. We say that the resulting *directed graph* is *strongly connected*.

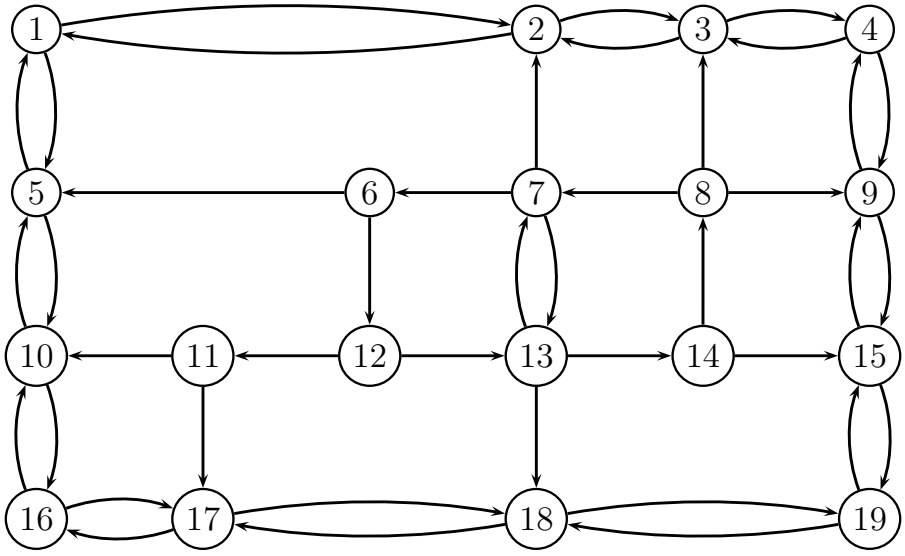

Figure 1.6: A choice of one-way streets

A possibility of orienting the streets is shown in Figure 1.6.

Is the above graph strongly connected?

If not, how do we find its *strongly connected components*?

How do we use the strongly connected components to find an orientation that solves our problem?

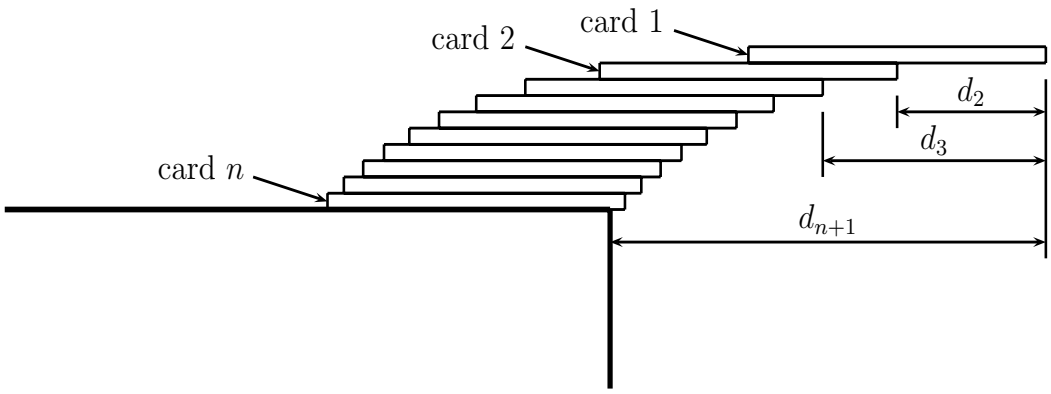

Figure 1.7: Stack of overhanging cards

Problem 5. The *maximum overhang* problem.

How do we stack n cards on the edge of a table, respecting the law of gravity, and achieving a maximum overhang.

We assume each card is 2 units long.

Is it possible to achieve any desired amount of overhang or is there a fixed bound?

How many cards are needed to achieve an overhang of d units?

Problem 6. *Ramsey Numbers*

A version of *Ramsey's Theorem* says that for every pair, (r, s), of positive natural numbers, there is a least positive natural number, $R(r, s)$, such that for every coloring of the edges of the complete (undirected) graph on $R(r, s)$ vertices using the colors *blue* and *red*, either there is a complete subgraph with r vertices whose edges are all *blue* or there is a complete subgraph with s vertices whose edges are all *red*.

So, $R(r, r)$, is the smallest number of vertices of a complete graph whose edges are colored either *blue* or *red* that must contain a complete subgraph with r vertices whose edges are all of the same color.

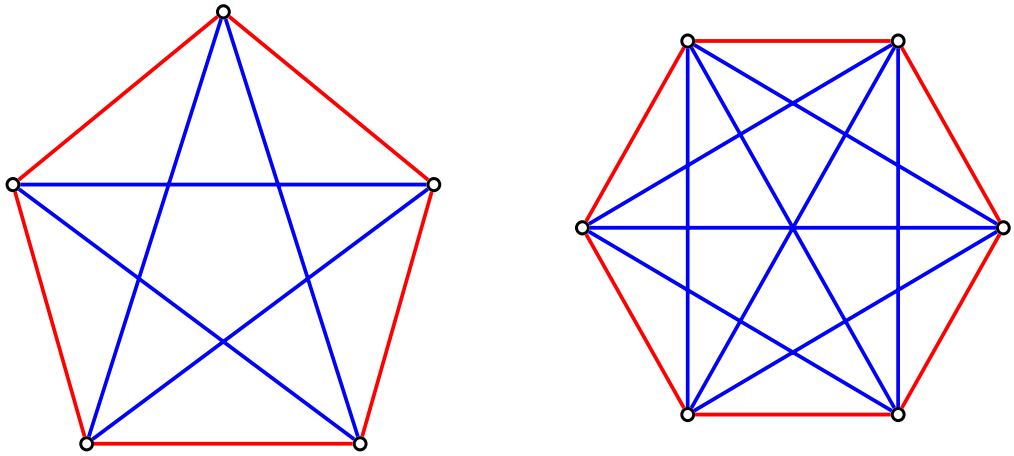

Figure 1.8: Left: A 2-coloring of K_5 with no monochromatic K_3; Right: A 2-coloring of K_6 with several monochromatic K_3's

The graph shown in Figure 1.8 (left) is a complete graph on 5 vertices with a coloring of its edges so that there is no complete subgraph on 3 vertices whose edges are all of the same color.

Thus, $R(3,3) > 5$.

There are

$$2^{15} = 32768$$

2-colored complete graphs on 6 vertices. One of these graphs is shown in Figure 1.8 (right).

It can be shown that all of them contain a triangle whose edges have the same color, so $R(3,3) = 6$.

The numbers, $R(r, s)$, are called *Ramsey numbers*.

It turns out that there are *very few* numbers r, s for which $R(r, s)$ is known because the number of colorings of a graph grows very fast! For example, there are

$$2^{43\times 21} = 2^{903} > 1024^{90} > 10^{270}$$

2-colored complete graphs with 43 vertices, a huge number!

In comparison, the universe is *only* approximately 14 billions years old, namely 14×10^9 years old.

For example, $R(4, 4) = 18$, $R(4, 5) = 25$, but $R(5, 5)$ *is unknown*, although it can be shown that
$43 \leq R(5, 5) \leq 49$.

Finding the $R(r, s)$, or, at least some sharp bounds for them, is an *open problem*.