

A course: Mathematics and Technology*

C. Rousseau, DMS , Université de Montréal

June 2010

Abstract

Of what use is mathematics? Hasn't everything in mathematics already been discovered? These are natural questions often asked by high schools. Teachers in these schools generally work under even tight constraints and their answers are often brief and elementary. If they are able to competently respond to these questions it is probably because they received good answers from their teachers and professors. And if they do not have the answers, then whose fault is it? A remedy to this problem is to address seriously real world applications of mathematics in preservice high school teacher education. In this paper I will present the course "Mathematics and technology" which is taught at the Université de Montréal since 2001. The last sections present examples treated in the course.

1 Description of the course

1.1 The spirit of the course

The main message of the course is that *Mathematics is a living science, everywhere present in science and technology. The teacher should have experienced how science develops in the real world. He(she) can then show it.*

Hence, the objective of the course is to introduce to several applications of mathematics in technology. The applications chosen are very modern for the most part. Let's take a few examples. You open your computer:

- You use Google: how does Google work? A search engine is useless if entries are not properly indexed. What can you manage with one million entries, if the one which is of interest to you is the last? The success and supremacy of Google come from its mathematical algorithm.
- You open webpages with images: this slows down the navigation, even if the images are highly compressed. So imagine if they had not been compressed! But the compression is done cleverly, so that you cannot see any deterioration of the quality of the image on the screen. How to compress cleverly: this is done with the JPEG format, another mathematical algorithm. Similar compression is used for music in MP3 files.

*This work is supported by NSERC in Canada.

- You send your credit card number via Internet: the transmission is secured so that no eavesdropper can find your credit card number. How is the information encrypted? This is an application of number theory and the encryption procedure works because computers are unable to factor very large integers.

Now, you want to listen to a TV program: outside your house the antenna has a parabolic shape. Why? By the end of this paper, we could enlarge this list.

The applications listed above use relatively elementary mathematics. At the same time, some sophistication is needed to get extra power. For instance, the encryption methods must be safe, even against cracks of computer.

We are all facing the need to convince more high school students to go into science. The high school teacher is a model for them. He (she) is the person to whom they can ask questions about science or about becoming a scientist. A scientist is someone who

- Asks questions;
- Dares to say: I don't know;
- Has a critical mind.

One purpose of the course is to help discover the power of the mathematical method:

- mathematical modeling;
- problem solving;
- mathematical sophistication;
- use of computers (but not for all applications).

Here are some messages spread through the course:

- The questions "Why?" and "What is it useful for?" should be encouraged and deserve an answer.
- The beauty of mathematical constructions.
- Mathematics are useful and constantly developing around us.
- Mathematics are much more than numbers.

Most subjects treated are too advanced so that preservice teachers following the course can hope bring them directly to classroom. The purpose of the course is not to give them material they will bring to classroom. It is rather to teach them how to prepare such kind of material. However, a special effort is made to make extensive use of high school level mathematics, particularly Euclidean geometry. The message is that *basic high school and undergraduate mathematics form a remarkable toolkit, provided they are well understood and mastered, allowing students to readily explore their wide applications and, often for the first time, to discover their power when used together.*

1.2 The course

This course is a joint creation with my colleague Yvan Saint-Aubin. Yvan is a physicist and I am a mathematician. We knew very little of the material of the course when it was created. We now have enough material for at least two courses. The game is to take some technologies into pieces, to dismantle them in order to discover and explain the mathematics that makes them work. We play the game to prepare the course. We try to teach the students to do the same. To share the pleasure we had to do so and help others start, we wrote a book for the course [2].

Format. The course has two formats:

- “Science Flashes”: small subjects that can be explained in an hour or two,
- More elaborate subjects: between one and two weeks are spent on the subject.

The lectures are of two different types. Some explain the elementary parts and are subject matter for exams. They are completed by conference type lectures on advanced parts, which are not subject matter for exams. Each application is typically covered in 5-6 hours of class: two hours for the basic theory, two hours for examples and exercises and, if time permits, one or two hours for advanced topics. Often we are only able to touch briefly upon the advanced material, unless a second week is spent on the chapter. During a single semester we aim to cover a significant part of 6 to 8 subjects and a handful of Science Flashes.

Evaluation. The evaluation for the course takes the following form:

- Two exams with open book and personal notes. Non cumulative contents;
- A session project on an application of mathematics (by teams of two, if possible; by larger teams (4-6) otherwise);
- A half-hour oral presentation of the project.

About the exercises. We have spent a lot of time writing interesting exercises that make the students practice modelling and review their elementary maths. Finding appropriate exam questions, both interesting and not too difficult is not a trivial task! A few examples will be presented below. Others can be found in our book [2].

1.3 Science Flashes

Here is a list of Science Flashes. For several of them, we indicate in italics the mathematical concept that is discussed.

1. Antennas and radars are parabolic. Why? (Geometric definition of conics)
2. Computer vision: calculating the position of one object from its position on two photos (The parametric equations of lines in 3-dimensional space)
3. Covering a territory with antennas for a mobile phone network (Euclidean geometry) Which of the following three networks requires the less antennas (Figure 1)?

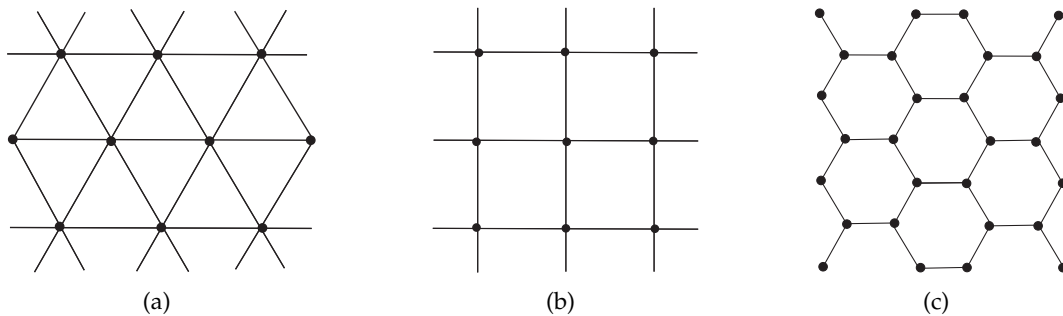


Figure 1: Three networks.

A calculation shows that it is the triangular network. The calculation shows that the number of antennas is exactly twice less the number of antennas in the hexagonal network. Why? Superimposing the two networks yields the explanation: on each horizontal line there are two antennas of the hexagonal network for each antenna of the triangular network (Figure 2).

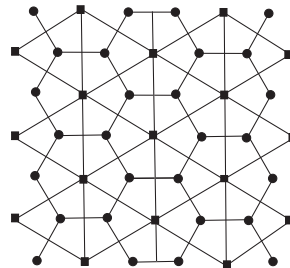


Figure 2: Comparing the triangular and hexagonal networks.

Corresponding question at the exam. We fill a large planar region with nonoverlapping disks of radius r . We use two methods: in the first method we place the centers of the disks on a square network and in the second method we place them on a regular triangular network of equilateral triangles. Which method gives the denser filling (Figure 3)? Suggestion: compute the proportion of each square covered by portions of disks in case (a) and the proportion of each triangle covered by portions of disks in case (b).

4. Physics : unifying the laws of reflection and refraction. The laws of nature follow optimization principles. Applications : short waves, optical fiber.
5. Short look in the architecture of computers describing logic circuits.
6. The regular tiling of the sphere with twelve spherical pentagons (Figure 4): the solution becomes easy of one remarks that there are five cubes inscribed on a dodecahedron (Spherical geometry, platonic solids).

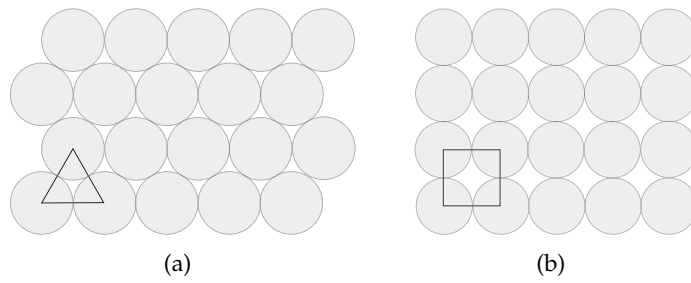


Figure 3: Two fillings of the plane.

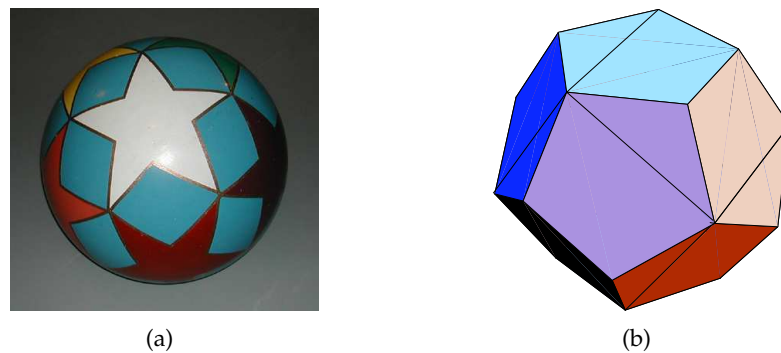


Figure 4: Two fillings of the plane.

- Voronoi diagrams: given antennas at fixed places, divide the plane into regions, such that in each region each point of a region is closer to its antenna than to any other antenna (see Figure 5) (Euclidean geometry)

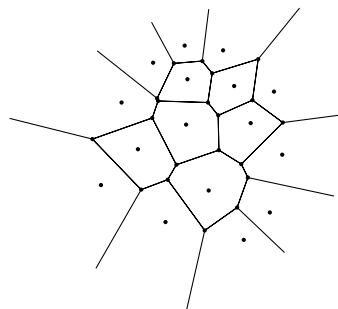


Figure 5: A Voronoi diagram.

1.4 More elaborate subjects

In parentheses we write the mathematics discussed through the subject.

1. **Positioning in space:** GPS, GPS signal, cartography, localization of thunderstorms (Geometric locus, differential geometry, theory of finite fields).
2. **How is a musical CD engraved:** why 44100 numbers per second? (Elementary Fourier analysis).
3. **Public key cryptography** (Elementary number theory: congruences).
4. **Error correcting codes:** Hamming codes and Reed-Solomon codes (Linear algebra, finite fields).
5. **Image compression:** iterated function systems (Affine transformations of the plane).
6. **The JPEG format (.jpg)** (Elementary Fourier analysis).
7. **Robots** (Rotations in 3-dimensional space, change of reference frame).
8. **Friezes and tilings** (Symmetries - linear algebra).
9. **Google and the Pagerank algorithm** (Markov chains - linear algebra).
10. **The skeleton and the gamma-knife surgery** (Geometry).
11. **Turing machines and DNA computers** (The hierarchy of functions starting from the basic ones).
12. **Random number generators** (Finite fields).
13. **Calculus of variations** (Multi-variable calculus).
14. **Sparing and borrowing money** (Geometric sequences, exponential function).

1.5 Some students projects

In order to have sufficiently many subjects we allow applications in science and technology, especially when the mathematics are interesting for future high school teachers.

1. The search of boundaries in a photo.
2. Morphing IMAGES
3. Text compression.
4. Mathematical morphology in treating images of Rollercoasters.
5. Benford law of significant digit.
6. How to complete the hole in Escher's painting. "Print Gallery"?
7. Polyhedra and fullerenes.
8. Voronoi diagrams and Delaunay triangulation in image analysis.
9. Sphere packings and honeycombs.

10. The best skateboard track.
11. Other cryptographic methods.
12. Reed-Miller error-correcting codes.
13. Knots and the action of enzymes on DNA.
14. Digital fingerprinting.
15. Image compression: from fractals to practical applications.
16. Penrose tilings.
17. The seasons, the locus of the sunrise and sunset at a given date, the length of day at a given date, ...
18. Calculation of astronomic distances, from the ancient Greeks to now.
19. The eclipses.
20. The shape of sand dunes.
21. Phyllotaxy (how to explain spirals in sunflowers, etc.).
22. Population growth under constraints.
23. Mathematical modelling of epidemics.
24. Chaos.
25. The Mathematics of Origami.

2 A flash science: the optic property of the parabola

All rays parallel to the axis are reflected to a single point, which is the focus of the parabola (Figure 6).

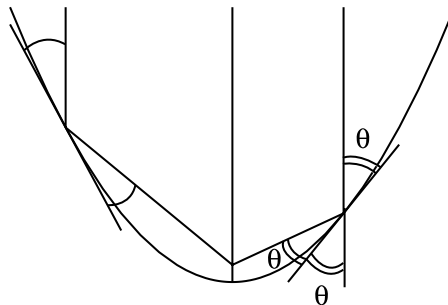


Figure 6: The optic property of the parabola.

This remarkable property has a simple geometric proof using the geometric definition of the parabola as the locus of points which are at equal distance from a point and a line.

The applications are numerous. The shape of many objects is parabolic among which:

- Parabolic antennas.
- Telescope mirrors:

Figure 7 illustrates a Schmidt-Cassegrain telescope. The reflected beam of light is directed to the focus of the parabola. But, before it reaches the focus it is reflected by a secondary mirror. This secondary mirror is hyperbolic and one of its foci coincides with the focus of the parabola. Indeed, the remarkable property of the hyperbola guarantees that the beam will be reflected to the other focus of the hyperbola.

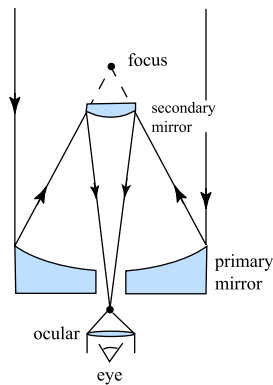


Figure 7: A Schmidt-Cassegrain telescope.

A related exam question. Describe the shape of all mirrors of the Alpaca telescope to be built in Chili and explain how are placed their foci (see Figure 9). (Here all three mirrors are parabolic. The primary mirror is a liquid mirror with mercury.)

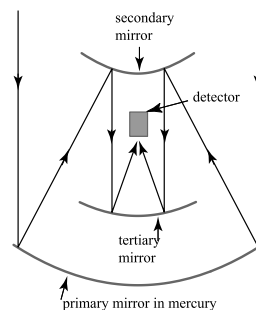


Figure 8: The Alpaca telescope in Chili.

- Radars
- Head-lights

- Solar furnaces The photo represents the solar furnace in Odeillo, in the French Pyrenees. It is directed to the North and 64 heliostats reflect the sun to the mirror.



Figure 9: The solar furnace in Odeillo.

All three conics have such remarkable optic properties. The corresponding property of the ellipse is the following: on an elliptic mirror, any ray issued from one focus is reflected to the other focus (Figure 10).

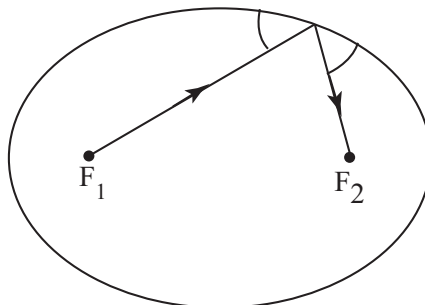


Figure 10: The optic property of the ellipse.

Again there are applications in acoustic phenomena and elliptic mirrors

- Elliptic mirrors for instance behind the lamp of a cinema projector
- Accoustic phenomena: for instance Paris' subway

You hear better the conversation of someone on the other side than of someone next to you!

3 Google and the PageRank algorithm

Considering the enormous number of webpages, a search engine is useless if it does not order pages properly. Why is Google so efficient? We will explain on an example a simplified version of the PageRank algorithm at the basis of Google's success.

Consider the small web with five pages appearing on the figure 11. We start on one page,

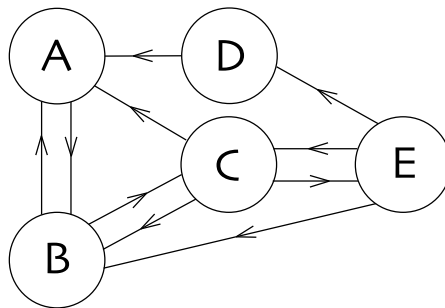


Figure 11: A simple web.

for instance page C. At each click we choose one link at random. If we are on page C, there are three links leaving page C, so each of them has probability $1/3$ of being chosen. If we are on page A, we have no choice than to be on page B after one click. We do this for all pages and we summarize this information in a matrix

$$P = \begin{matrix} & \begin{matrix} A & B & C & D & E \end{matrix} \\ \begin{matrix} A \\ B \\ C \\ D \\ E \end{matrix} & \begin{pmatrix} 0 & \frac{1}{2} & \frac{1}{3} & 1 & 0 \\ 1 & 0 & \frac{1}{3} & 0 & \frac{1}{3} \\ 0 & \frac{1}{2} & 0 & 0 & \frac{1}{3} \\ 0 & 0 & 0 & 0 & \frac{1}{3} \\ 0 & 0 & \frac{1}{3} & 0 & 0 \end{pmatrix} \end{matrix}$$

Each initial page is represented by a column and each page after one click by a line. Let's look at the second column. It says that if we start on page B, we have probability $1/2$ on being on page A and $1/2$ of being on page C after one click. Same for the other columns. So where are we after two clicks? It requires a little gymnastic to figure that this is represented by the matrix

$$P^2 = \begin{matrix} & \begin{matrix} A & B & C & D & E \end{matrix} \\ \begin{matrix} A \\ B \\ C \\ D \\ E \end{matrix} & \begin{pmatrix} \frac{1}{2} & \frac{1}{6} & \frac{1}{6} & 0 & \frac{11}{18} \\ 0 & \frac{2}{3} & \frac{4}{9} & 1 & \frac{1}{9} \\ \frac{1}{2} & 0 & \frac{5}{18} & 0 & \frac{1}{6} \\ 0 & 0 & \frac{1}{9} & 0 & 0 \\ 0 & \frac{1}{6} & 0 & 0 & \frac{1}{9} \end{pmatrix} \end{matrix}$$

Here again, each initial page is represented by a column and each page after two clicks by a line. So if we start on page A we have probability $1/2$ on being on page A and $1/2$ of being on page C after two clicks, something which is easily verified on the web. Already for page C, we see that the calculations are more elaborate and become difficult to do by hand. It becomes a great advantage to reduce them to pure matrix multiplications.

Where are we after n clicks? For n sufficiently large we have

$$p^{32} = \begin{pmatrix} & \text{A} & \text{B} & \text{C} & \text{D} & \text{E} \\ \text{A} & 0.293 & 0.293 & 0.293 & 0.293 & 0.293 \\ \text{B} & 0.390 & 0.390 & 0.390 & 0.390 & 0.390 \\ \text{C} & 0.220 & 0.220 & 0.220 & 0.220 & 0.220 \\ \text{D} & 0.024 & 0.024 & 0.024 & 0.024 & 0.024 \\ \text{E} & 0.073 & 0.073 & 0.073 & 0.073 & 0.073 \end{pmatrix}$$

All columns are identical! The probability of being on a given page is independent on the initial page! We see that we have probability 0.39 of being on page B. This is the highest probability of all. Hence, page BB will be ranked first. The pages of our small web will be ranked as B, A, C, E, D.

Why does it work? Because the sum of all entries in all columns of is equal to 1, so P is the transition matrix of a Markov chain. We will not give the details of the proof here, but these can be explained to a student mastering linear algebra.

4 Image compression

The easiest way to store an image inside the memory of a computer is to store the color of each pixel. This requires an enormous quantity of memory! Can we do better?

Let us suppose we have drawn a city (Figure 12). We store in memory

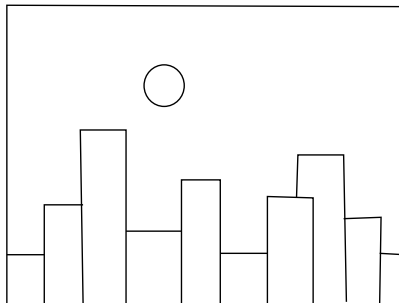


Figure 12: A city.

- Line segments
- Circles arcs
- Etc.

which approximate our image.

We approximate our image with known geometric objects. To store a line segment in memory it is sufficient to store:

- the two endpoints of the line segment;
- a program explaining to the computer how to draw a line segment with given endpoints.

The geometric objects are our *alphabet*.

How can we keep in memory a complex landscape? We use the same principle with a larger alphabet of geometric forms. We add the fractals to our alphabet. We approximate our landscape with fractals objects, for instance the fern (Figure 13)



Figure 13: A fern.

We store in memory a program to draw the fern. Because the fern is auto similar, the program is very short. For instance here is such a program on Mathematica:

```
choixT := (r = Random[Integer, {1, 100}];
  If[r <= 85, 1,
    If[r <= 92, 2,
      If[r <= 99, 3, 4]]])

t = { (* { transformation lineaire, translation } *)
  {{{0.85, 0.04}, {-0.04, 0.85}}, {0., 1.6}},
  {{{0.2, -0.26}, {0.23, 0.22}}, {0., 1.6}},
  {{{-0.15, 0.28}, {0.26, 0.24}}, {0., 0.44}},
  {{{0., 0.}, {0., 0.16}}, {0., 0.}}
};

transfoAff[t_, pt_] := t[[1]].pt + t[[2]]

nIteration = 20000; A = {{0., 0.}}; Do[AppendTo[A,
transfoAff[t[[choixT]], Last[A]]], {nIteration}]

ListPlot[A, AspectRatio -> Automatic, Axes -> False]
```

How does that such a complex object, with so many small details can be drawn with such a simple program! It comes from a hidden simplicity of the fern. Let's put our mathematical glasses to reveal it.

The structure of the fern: The fern is a union

- of a tail,
- of 3 smaller ferns: the left lower branch (labeled L on figure), the right lower branch (labeled R on figure), and the fern minus the two lower branch.

We can reconstruct the fern from 4 affine transformations:

- the transformation T_1 which sends the large fern to the fern minus the two smaller branches;
- the transformation T_2 which sends the large fern to the small left fern;
- the transformation T_3 which sends the large fern to the small right fern;
- the transformation T_4 which sends the large fern to the tail: this transformation is a projection on a vertical line composed with a homothety.

The program contains these transformations. For instance, T_1 is given by

$$(x, y) \mapsto (0.85x + 0.04y, 0.04x + 0.85y + 1.6).$$

It suffices to keep this information in memory to reconstruct the fern! The method is called "Iterated functions systems" (or IFS) and was first introduced by Barnsley [1].

Algorithm.

- We start with P_0 on the fern.
- We choose at random $i_1 \in \{1, 2, 3, 4\}$; we draw $P_1 = T_{i_1}(P_0)$.
- We choose at random $i_2 \in \{1, 2, 3, 4\}$. We draw $P_2 = T_{i_2}(P_1)$.
- Etc.

Why does it work? Let us experiment with a simpler fractal: the Sierpinski carpet (Figure 14).

It is of course a union of three Sierpinski carpets and it is easy to figure what are the affine transformations T_1, T_2, T_3 sending the large carpet to the three small carpets. For any subset B of the plane we will send B to the union $T_1(B) \cup T_2(B) \cup T_3(B)$. We will iterate this operation. Starting from B_0 , we will compute:

$$B_{n+1} = T_1(B_n) \cup T_2(B_n) \cup T_3(B_n).$$

Let us see what we obtain if we start with the square B_0 : we get (Figure 15)

This works with any initial set: let's try another one (Figure 16)!

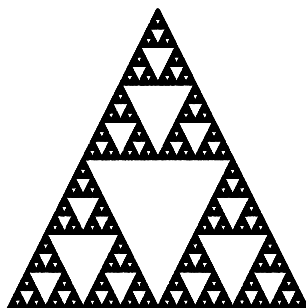


Figure 14: A sierpinski carpet.

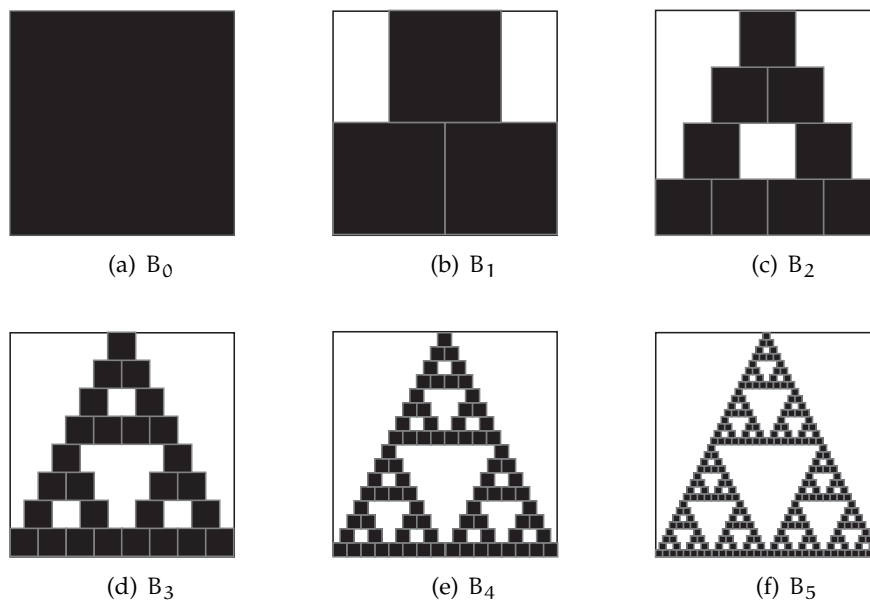


Figure 15: B_0 and the first five iterates B_1 - B_5

The explanation is that the Sierpinski carpet is the unique fixed point of our operator W which consists in sending B to the union $W(B) = T_1(B) \cup T_2(B) \cup T_3(B)$, and that this fixed point is an “attractor”.

But how do we encode a photo in general? The principle above is powerful, but it does not seem very practical. Well, we adapt the idea. We replace any small square by the image of a similar larger square under a homothety of ratio $1/2$ composed with one of eight transformations (Figure 17:

- Identity plus 3 rotations;
- 4 symmetries.

Moreover we adjust contrast and we make a translation of the level of grey, so that the image of the large square looks like the small square. See for instance Figure 17.

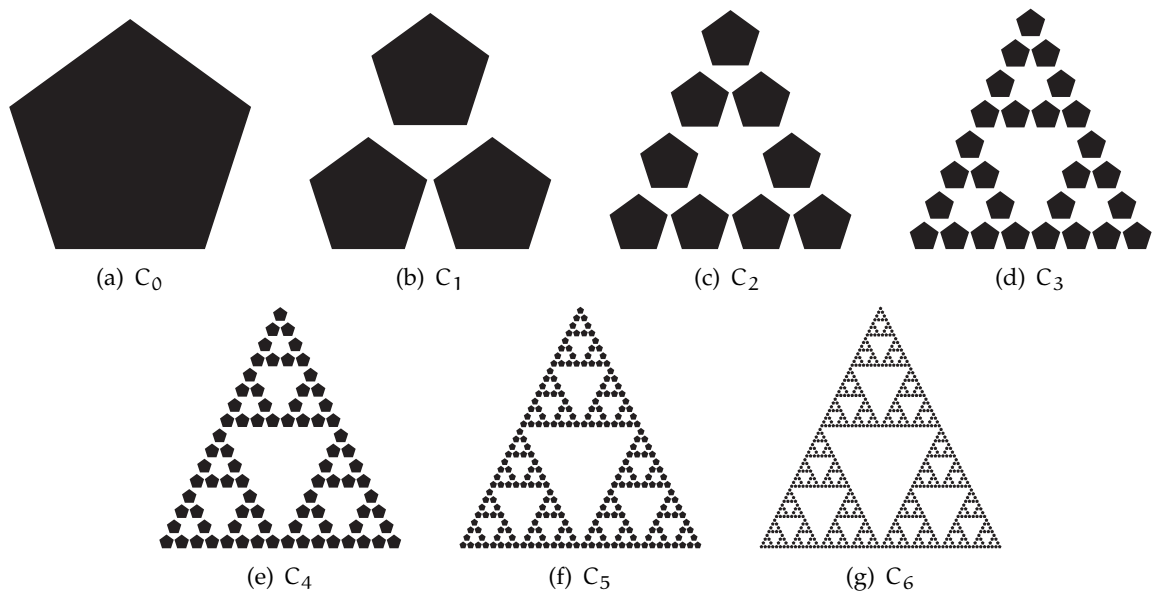


Figure 16: C_0 and the first six iterates C_1 - C_6

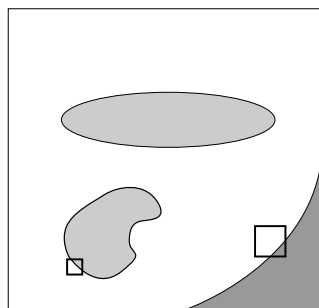


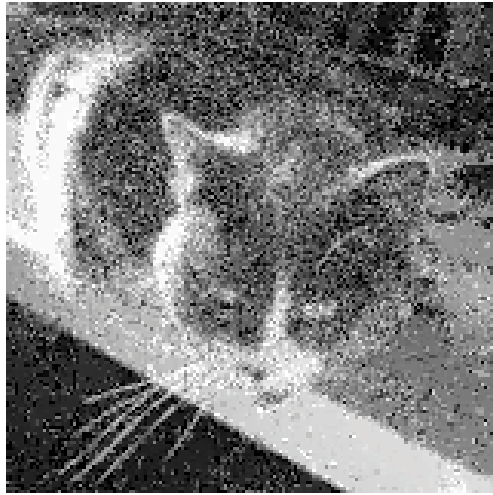
Figure 17: Choice of a large square similar to a small square

Yvan Saint-Aubin has programmed it with a photo of his cat (Figure 18). He started with a uniform gray level. After one step he got the left picture, and after six steps the right picture.

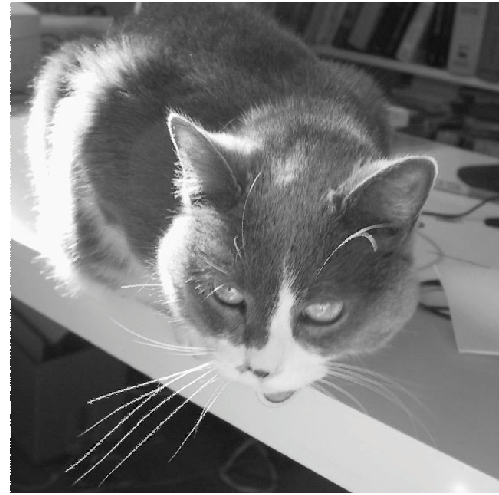
This example illustrates how a simple idea can be powerful.

The exercises. They force to practice affine transformations, a subject to be mastered by high school teachers. Several exercises take the following form: choose a coordinate system and find the affine transformations involved in the construction of the following fractals appearing in Figure 19.

It is interesting to discuss with the students that the solution is not necessarily unique, even for a given coordinate system!

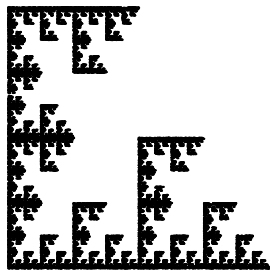


(a) The first iterate

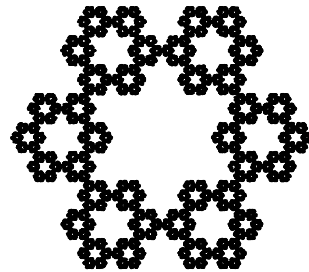


(b) The sixth iterate

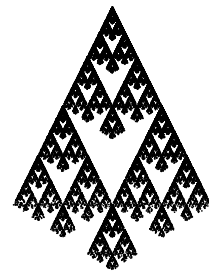
Figure 18: The reconstruction of a photo as the attractor of an IFS.



(a)



(b)



(c)

Figure 19: Some fractals to construct as attractors of IFS.

5 The GPS (Global positioning system)

The system was completely developed only in 1995 by the Ministry of Defense in U.S.A. who allows the public to use it. It consists of a network of 24 satellites which move on orbits around the world, so that anyone on earth can catch the signals of at least 4 satellites (Figure 20). At each time, the position of the satellites is known.

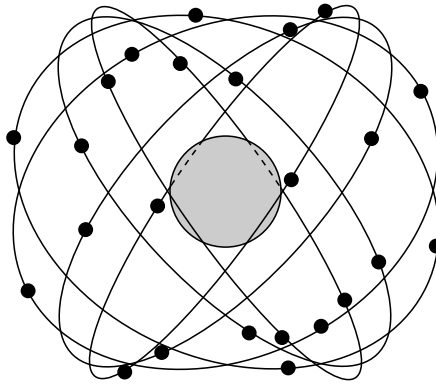


Figure 20: The network of satellites.

The GPS gives one's position on Earth. The principle is that the small receiver in one's hand measures the time necessary for a signal emitted by the satellite to travel from the satellite to the receiver. Given that the signal travels at the speed of light this allows to measure the distance from the satellite to the receiver: since the geometric locus of points at a fixed distance from a point is a sphere, from this we know that the receiver is located on a sphere centered at the satellite. We measure the travel time of the signal from three different satellites to the receiver. Hence the receiver is located at the intersection of three spheres. Since two spheres intersect on a circle, then the intersection of three spheres is the same as the intersection of a sphere with a circle, namely two points. Still too much! But in practice it is easy to eliminate one intersection point because it is much too far from the surface of the Earth and hence unrealistic. A morale which applies to any positioning problem: we had three unknowns which were the coordinates (x, y, z) of the receiver. So we needed three data, namely the travel times of three signals to get a finite number of solutions.

This is the theory. In practice the satellites have expensive atomic clocks which are perfectly synchronized while the receiver has a cheap clock. Then there is a fourth unknown: the clock offset, additional to the three unknowns for the position. Then the receiver needs a fourth measurement of the travel time from a fourth satellite to the receiver (the clock offset is the same for the 4 satellites). Here again we have a system of 4 equations with 4 unknowns which has two solutions, one of which is unrealistic. With this method, a precision of 20 meters can be attained. In teaching the subject, a lot of emphasis is put on the question of "dimension of the project": having the same number of equations as unknowns.

The applications are numerous:

- Finding one's way in wilderness.

- Drawing a map.
- Managing a fleet of vehicles.
- Measuring Mount Everest and observing its growth.
- Helping blind people.
- Find one's way on the road.
- Landing a plane in the fog.
- Etc.

A related exam question. Let's see a related exam question: Meteorites regularly enter the atmosphere, rapidly heat up, disintegrate, and finally explode before hitting the surface of the Earth. This explosion generates a shock wave that travels in all directions at the speed of sound v . The shock wave is detected by seismographs installed at various locations on the surface of the Earth. If four stations (equipped with perfectly synchronized clocks) note the moment that the shock wave arrives, explain how to calculate both the position and time of the explosion.

This is the elementary theory. More advanced topics can be studied inside a project. Let us discuss one here, since it illustrates the many links between different subjects and how a single clever idea can have many different applications.

Structure of the signal generated by the satellites. Each satellite has its own signal. These signals are generated by shift registers using finite fields, which are studied in error correcting codes. These same devices are excellent random number generators! Let's look at such a device (Figure 21).

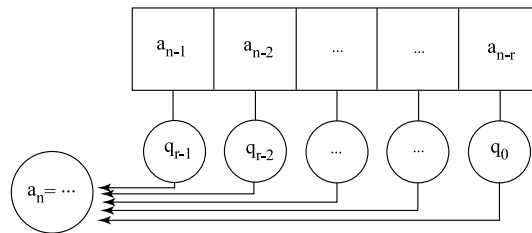


Figure 21: A shift register.

The coefficients q_i are bits 0 or 1. The shift register generates a sequence 0's and 1's recursively. Given initial conditions a_0, \dots, a_{r-1} , each subsequent a_n is generated according to the rule

$$a_n = a_{n-r}q_0 + a_{n-r+1}q_1 + \dots + a_{n-1}q_{r-1}.$$

Since the number of initial conditions is finite, the signal is periodic of period M . The receptor also generates the signal of each satellite and compares them with those of the satellites. For that, it counts the number of bits in match minus the number of mismatch during a period: this is called the correlation. If the correlation is equal to M , it knows it has captured

the signal of the satellite. But even if it has captured the signal of the satellite, they may be a shift between the two identical signals, thus yielding a correlation different from M . Hence the receptor translates the signal by one bit and calculates the correlation again. But errors are not uncommon in the transmission of signals through the atmosphere. So each signal must be very different from its translated signals. The signals generated by shift registers have this property if we choose well the q_i . Let us look at an example.

Example: we take $(q_0, q_1, q_2, q_3) = (1, 1, 0, 0)$ and initial conditions $0, 0, 0, 1$. This generates the sequence

000100110101111

of length 15. Let's compare this sequence with its 15 cyclic translates.

```

0 0 0 1 0 0 1 1 0 1 0 1 1 1 1
0 0 1 0 0 1 1 0 1 0 1 1 1 1 1 0
0 1 0 0 1 1 0 1 0 1 1 1 1 0 0
1 0 0 1 1 0 1 0 1 1 1 1 0 0 0
0 0 1 1 0 1 0 1 1 1 1 1 0 0 0 1
0 1 1 0 1 0 1 1 1 1 0 0 0 1 0
1 1 0 1 0 1 1 1 1 0 0 0 1 0 0
1 0 1 0 1 1 1 1 0 0 0 1 0 0 1
0 1 0 1 1 1 1 0 0 0 1 0 0 1 1
1 0 1 1 1 1 0 0 0 1 0 0 1 1 0
0 1 1 1 1 0 0 0 1 0 0 1 1 0 1
1 1 1 1 0 0 0 1 0 0 1 1 0 1 0
1 1 1 0 0 0 1 0 0 1 1 0 1 0 1
1 1 0 0 0 1 0 0 1 1 0 1 0 1 1
1 0 0 0 1 0 0 1 1 0 1 0 1 1 1

```

They all agree in 7 places and disagree in 8 places (bits in bold) for a correlation of -1 in all cases!

6 Error correcting codes

Principle. We lengthen a message so that the information is contained in several places. An error correcting code is efficient only if there are few errors.

Example: we repeat each bit 3 times. If the 3 bits received are different we correct using the law of the majority, i.e. as if only one error has occurred. Then we recover the message if zero or one error has occurred. We say that the code corrects one error. If we want to send a word of 4 bits we send 12 bits. Since two different words have at least three different bits, we get the right word if one error or less occurred.

We can do much better!

Hamming code: We want to send a word of 4 bits: $u_1u_2u_3u_4$. We send a word of seven bits.

We add

$$u_5 = u_1 + u_2 + u_3$$

$$u_6 = u_2 + u_3 + u_4$$

$$u_7 = u_1 + u_2 + u_4.$$

This code corrects one error. Indeed,

No error	u_5, u_6, u_7 compatible
1 error in u_1	u_5, u_7 incompatible
1 error in u_2	u_5, u_6, u_7 incompatible
1 error in u_3	u_5, u_6 incompatible
1 error in u_4	u_6, u_7 incompatible
1 error in u_5	u_5 incompatible
1 error in u_6	u_6 incompatible
1 error in u_7	u_7 incompatible

Example: to send the message 0010 we lengthen it to 0010110. We receive 1010110. We calculate $u_5 u_6 u_7$ for the received $u_1 u_2 u_3 u_4$. We get 011 and we compare with the received 110. The bits u_5 and u_7 are incompatible. We conclude that u_1 was erroneously transmitted and we change it from 1 to 0. We forget the last three bits and recover the message 0010. Of course, had there been more than one error, we would have erroneously corrected. Remember that an error corrected code is efficient if there are few errors.

7 Conclusion

This is the end of our guided tour. For us, this adventure has become a passion and we are always eager to dismantle and understand new applications of mathematics, and our book [2] is a starting point for someone who is not used to such a game, same as we were a few years ago. After a while, you will play the game yourself. To be fair, while several students told us it is the best course they ever had, not 100% of our students are so enthusiastic with the course. The course is difficult and requires a lot of work, something not so popular these days. But we are confident that nearly all students have learnt things they will remember longer than in many other courses, and that it may influence positively their future teaching.

References

- [1] M. Barnsley, *Fractals everywhere*, Academic Press, 1988.
- [2] C. Rousseau and Y. Saint-Aubin, *Mathematics and Technology*, Springer-Verlag, SUMAT Series, 2008. A French version of the book, *Mathématiques et technologie*, is also published by Springer-Verlag in the same series.