Review of the book

"Mathematics and Technology"

by Christiane Rousseau and Yvan Saint Aubin

SPRINGER

2008

ISBN: 978-0-387-69215-9

Eric Diehl

Security & Content Protection Labs, Technicolor

2011-04-13

What the book is about

How often have you heard the question "What are mathematics used for?" This book provides a well documented answer. It illustrates how technologies use different fields of mathematics. Its authors, Christiane Rousseau and Yves Saint-Aubin, are professors of mathematics at the University of Montréal. Each chapter is a multi-hour lecture on a given theme, which addresses several fields such as Euclidean geometry, probability, or finite field theory. The introduction of each chapter lists what fields of mathematics will be explored and provides an estimated duration for teaching the chapter. At the end of the chapter, the authors propose a set of exercises. The exercises are clear. Unfortunately, they are not solved. This would have been useful if you were a student.

What the book is like

Chapter 1: *Positioning on Earth and in Space*

As you may guess, this chapter explains how the Global Positioning System (GPS) works. The authors explain how with three geostationary satellites you may find your precise position on Earth. They demonstrate that you need a fourth satellite because the GPS receiver's is not synchronized with the satellites' clock. They briefly explain the many subtleties needed to reach the expected accuracy. They use an interesting example of triangulation used for detecting lightning strikes in the province of Quebec. Using a network of 13 detectors, and the same principle of time measurement than GPS, Hydro-Quebec can locate lightning strike with an accuracy of 500 meters.

As GPS uses random sequences for identification of individual satellites, section 1.4 describes Line Shift Registers (LSR). This section is redundant with Chapter 8 that gives a deeper inside view. Of course, the theme of positioning was a natural path to cartography. Section 1.5 introduces the conception of projection to a plane on to different 3D objects. This chapter is simple to understand.

Chapter 2: *Friezes and Mosaics*

Using linear friezes and 2D mosaics, this chapter gives a good, entertaining introduction to geometric transformations such as symmetry, translation, and rotation. It uses affine transformations and the usual matrix-based representation. The chapter is simple to understand. Would you have imagined so many problems when contemplating a mosaic?

Chapter 3: *Robotic Motion*

This chapter uses a 6-degree of freedom robotic arm to illustrate positioning and transformation of objects in 3D space. As such, it is a natural extension of previous chapter, which was dedicated to the plane. At the beginning, the authors define what a degree of freedom is, and they intuitively demonstrate that any object has at max six degrees of freedom. Then, they go through the usual orthogonal transformations. They show that notion of frame of reference and change of basis allows a simple mapping of the robotic arm.

Chapter 4: *Skeletons and Gamma-Ray radiosurgery*

This chapter presents a mix between pure mathematics and algorithmic-approach. The chapter introduces the concepts of vector and Euclidian distance. It proposes an interesting geometrical problem: Skeleton is the set of points of a geometric shape whose distance is minimal from all borders. One practical application is to define the optimal treatment for applying radiotherapy on cancer tumors. The definition of the skeleton is mathematically accurate. How to apply it to radiotherapy treatment, which uses circles of fixed dimension? Pure mathematics cannot solve this problem. An algorithmic approach is used to approximate the solution. The implemented solution and corresponding rationales are described.

This chapter is interesting because it highlights that real products require compromises.

Chapter 5: *Saving and Loans* is, as we could imagine, the simplest chapter of this book. It demonstrates how geometric series are used in the banking domain. At least, after having read this chapter, the reader will have a better understanding of the mortgage vocabulary.

Chapter 6: *Error-Correcting Codes*

The chapter summarizes the characteristics of F_2 and finite fields. It describes in details the C(7,4) Hamming–code, and generalizes to the other Hamming codes. They conclude with the mathematics of Reed Solomon codes. Picture 6.4 visually explains the behavior of Reed Solomon.

Chapter 7: *Public Key Cryptography: RSA* is a good introduction to the mathematics behind the famous algorithm. This chapter explores the problem of factorization of large numbers and the question of testing the primality of a number. It also gives a glimpse on Schor's test. This is a good excuse for briefly introducing quantum computing. For people used to handle RSA, this chapter has a special taste. Being written by non-security aware mathematicians, their view of the problem is different from the view that security experts are used to. For instance, it is strange to never speak of the size of a key or brute force

attack. Clearly, security is not an issue. I am not sure that the non-security aware reader will have understood the interest of public key cryptosystem.

Chapter 8: *Random Number Generators* thoroughly explains the design of pseudo random number generators using linear shift registers. It is simple to understand, although I have some doubts about the clarity of the section dedicated to multiple, combined, recursive generators. Unfortunately when reading this chapter, randomness seems reduced to increasing the period. It would have been interesting to explore some methods to evaluate randomness.

Chapter 9: *Google and the PageRank algorithm*

The chapter provides a good introduction explaining why each search engine on the Web is different from search engine in libraries for instance. Heterogeneity is the keyword in the first case, whereas homogeneity is the one in the second case. It introduces Markov chains and derives definitions of PageRank algorithm.

Chapter 10: *Why 44,100 Samples per Second?*

This chapter is different from the other ones. The author must be a musician. In the first part, the author introduces the relationship between frequency and notes and of course he presents the harmonic scale. The notion of well-tempered scale is interesting. Then, the Fourier analysis is introduced. The chapter even gives a glimpse to the complexity of human hearing physiology. The last part presents the Nyquist frequency. As most humans do not to hear frequency higher than 20 KHz, the sampling rate had to be higher than 40 KHz. The chapter illustrates how some decisions are influenced by cost rather than by science. This lesson is a good one for future engineers.

Chapter 11: *Image Compression: Iterated Function Systems*

The chapter presents fractal compression, or how you can modelize an image using iterative functions. It starts with affine transformations in the plane, introduces iterated function systems, iterated contractions, attractors, and fixed points. Then, the authors apply these notions to images. At the end, they briefly compare iterative compression with JPEG.

Chapter 12: *Image Compression: the JPEG standard*

The purpose of this section is to present another method of image compression. For that purpose, it uses the widely used JPEG format (the one with .jpg extension file). The introduction explains the difference between lossless compression and lossy compression. It would have been interesting to cite some lossless multimedia compression formats such as FLAC. Then it explains how using coding based on cosine transform it is possible to describe the image with matrices of real numbers. This part is rather hard to follow. The last part explains how carefully chosen quantization allows to null many coefficients, thus allowing efficient compression. The parameters of choice of quantization are not explored. It would have been interesting to show the visual impact of these parameters with examples of the same picture at different compression ratio. With this section, the reader will have a good idea of how most multimedia compression formats work.

The authors use the same picture for illustrating both chapters on image compression. This smartly illustrates the difference of approach between the two methods.

Chapter 13: *The DNA Computer*

This chapter is different from the other ones. It explores a very futuristic vision: DNA computing. The authors, two post-graduate students, first describe the Hamiltonian Path and how Leonard Adleman (yes, the one of RSA) solved it for a simple problem with DNA strands. Then, they introduce Turing machines and recursive functions. They demonstrate the equivalence of Turing machine and DNA insertion and deletion program. They conclude by highlighting the huge challenges for making real DNA computing.

This is probably my preferred chapter. It explores a very exciting but futuristic domain. Nevertheless, an extremely refreshing chapter to read. After having read this chapter, you may want to read more on this topic.

Chapter 14: *Calculus of Variations and Applications*

The goal of this chapter is to introduce the problem of optimization of differential equations. The first proposed problem is to define what is the quickest path between two points when only using gravity. It introduces the Euler-Lagrange equation, Fermat's principle, and non differentiable solutions. Once the answer found (a cycloid), it tackles a more complex, theoretic problem: the shortest tunnel using only gravity between two points on a sphere (a hypocycloid). Then it presents the Huygens's pendulum, which is more accurate than regular pendulum (at least in theory with null friction). The next problem is to define the shape that a flexible film would take when on an arbitrary structure (for instance shape of a soap bubble with two square holes). Then the authors explore many isoperimetric problems such as the shape of a suspended cable, or a self-supporting arch. They conclude with an innovative application: liquid mirrors. Rotating liquid creates a perfect paraboloïd that can be used by telescopes.

Chapter 15: *Science Flashes*

This chapter is a collection of short topics, called science flashes. They should take less than two hours. The first one explores the mathematics driving reflection and refraction. The second topic explores the proprieties of parabola (to focus waves), ellipse, and hyperbola. The third science flash is about quadratic surfaces in architecture. The use was not obvious. The fourth flash compares the efficiency of triangular, square, and octagonal meshing. The fifth topic introduces Voronoi cells: the set of points that are closer to one given than to a set of points. It explains its application to cellular networks. The sixth science flash (extremely short) describes how to calculate the depth information using two pictures (at least in ideal conditions). The next flash introduces binary operations. I am not sure that a neophyte will understand the explanations about actual implementations with transistors. The eighth subject how to draw five-point stars in a tiled-manner onto a sphere. The last science flash uses simple trigonometry to route a curve.

Recommendation

Clearly, the primary audience of this book is mathematic professors. If you want a way to illustrate the use of given mathematic field in real applications, this book will give the elements to build such lecture as well as exercises. If you are a student, this book can be used as a course text. It is a good way to diversify your training with new exercises. Unfortunately, they are not solved and you are at your own. For other categories of reader, the book may be interesting to challenge your basics if you feel somewhat rusted. Some chapters are extremely interesting to read, for instance Chapter 13: DNA computing. Nevertheless, if you are looking to seriously refresh your basics in a given field, you should rather read a textbook dedicated to this topic. If you are only interested in security, read other books.

The reviewer is the head of Technicolor's Security & Content Protection Laboratories.