Codes and Turbo Codes

Springer

Paris
Berlin
Heidelberg
New York
Hong Kong
Londres
Milan
Tokyo

Claude Berrou (Ed.)

Codes and Turbo Codes

Springer

Claude Berrou

Télécom Bretagne
CS 83818
29238 Brest Cedex 3
France

ISBN : 978-2-8178-0038-7 Springer Paris Berlin Heidelberg New York

Printed in France
Springer-Verlag France is a member of the group Springer Science + Business Media

First edition in French © Springer-Verlag France 2007
ISBN: 978-2-287-32739-1

Cover design: Jean-François MONTMARCHÉ
Cover illustration: Jean-Noël JAFFRY

Codes and Turbo Codes

under the direction of Claude Berrou (Télécom Bretagne)

The following have contributed to this work:
- Karine Amis,
- Matthieu Arzel,
- Catherine Douillard,
- Alain Glavieux †,
- Alexandre Graell i Amat,
- Frédéric Guilloud,
- Michel Jézéquel,
- Sylvie Kerouédan,
- Charlotte Langlais,
- Christophe Laot,
- Raphaël Le Bidan,
- Émeric Maury,
- Youssouf Ould-Cheikh-Mouhamedou,
- Samir Saoudi,
- Yannick Saouter,
all at Télécom Bretagne,
- Gérard Battail,
at Télécom ParisTech,
- Emmanuel Boutillon,
at the Université de Bretagne Sud,

with the invaluable assistance of Josette Jouas, Mohamed Koubàa and Nicolas Puech.

Translation: Janet Ormrod (Télécom Bretagne).

Cover illustration: Jean-Noël Jaffry (Télécom Bretagne).

Any comments on the contents of this book can be sent to this e-mail address:
turbocode@mlistes.telecom-bretagne.eu

"The oldest, shortest words — yes and no —
are those which require the most thought"

Pythagoras, fifth century BC

To our late lamented colleagues and friends,
Alain Glavieux and Gérard Graton.

Foreword

What is commonly called the information age began with a double big bang. It was 1948 and the United States of America was continuing to invest heavily in high-tech research, the first advantages of which had been reaped during the Second World War. In the *Bell Telephone Laboratories*, set up in New Jersey, to the south of New York, several teams were set up around brilliant researchers, many of whom had been trained at MIT (*Massachusetts Institute of Technology*). That year two exceptional discoveries were made, one technological and the other theoretical, which were to mark the 20th century. For, a few months apart, and in the same institution John Bardeen, Walter Brattain and William Shockley invented the transistor while Claude Elwood Shannon established information and digital communications theory. This phenomenal coincidence saw the birth of near-twins: the semi-conductor component which, according to its conduction state (on or off), is able to materially represent binary information ("0" or "1") and the *Shannon* or *bit* (short for *b*inary un*it*), a unit that measures information capacity.

Today we can recognize the full importance of these two inventions that enabled the tremendous expansion of computing and telecommunications, to name but these two. Since 1948, the meteoric progress of electronics, then of micro-electronics, has provided engineers and researchers in the world of telecommunications with a support for their innovations, in order to continually increase the performance of their systems. Who could have imagined, only a short while ago, that a television programme could be transmitted via a pair of telephone wires? In short, Shockley and his colleagues, following Gordon Moore's law (which states that the number of transistors on a silicon chip doubles every 18 months), gradually provided the means to solve the challenge issued by Shannon, thanks to algorithms that could only be more and more complex. A typical example of this is the somewhat late invention of turbo codes and iterative processing in receivers, which could only be imagined because the dozens or hundreds of thousands of transistors required were available.

Experts in micro-electronics foresee the ultimate limits of CMOS technology at around 10 billion transistors per square centimetre, in around 2015. This is about the same as the number of neurons in the human brain (which will, however, remain incomparably more powerful, due to its extraordinary network of connections - several thousand synapses per neuron). Billions of transistors on the same chip means that there will be easily enough room for algorithms that require the greatest calculating resources, at least among those algorithms that are known today. To repeat the slogan of one integrated circuit manufacturer, "the limit lies not in the silicon but in your imagination". Even so, and to be honest, let us point out that designing and testing these complex functions will not be easy.

However, we are already a long way from the era when Andrew Viterbi, concluding the presentation of his famous algorithm in 1967, showed scepticism that matched his modesty: "Although this algorithm is rendered impractical by the excessive storage requirements, it contributes to a general understanding of convolutional codes and sequential decoding through its simplicity of mechanization and analysis" [1]. Today, a Viterbi decoder takes up a tenth of a square millimetre in a cellphone.

Among the results presented by Shannon in his founding paper [2], the following is particularly astonishing: *in a digital transmission in the presence of perturbation, if the average level of the latter does not exceed a certain power threshold, by using appropriate coding, the receiver can identify the original message without any errors.* By coding, here and throughout this book, we mean error-correcting coding, that is, the redundant writing of binary information. Source coding (digital compression), cryptographic coding, and any other meaning that the term coding might have, are not treated in *Codes and Turbo codes.*

For thousands of researchers and engineers, the theoretical result established by Shannon represented a major scientific challenge since the economic stakes are considerable. Improving the error correction capability of a code means, for the same quality of received information (for example, no more than one erroneous bit out of 10,000 received in digital telephony), enabling the transmission system to operate in more severe conditions. It is then possible to reduce the size of antennas or of solar panels and the weight of power batteries. In space systems (satellites, probes, etc.), the savings can be measured in hundreds of thousands of dollars since the weight of the equipment and the power of the launcher are thus notably reduced. In mobile telephone (cellphone) systems, improving the code also enables operators to increase the potential number of users in each cell. Today, rare are those telecommunications systems that do not integrate an error-correcting code in their specifications.

Another field of application for error-correcting codes is that of mass memories: computer hard drives, CD-ROMs, DVDs and so on. The progress made in the last few years in miniaturizing the elementary magnetic or optical memorization patterns has been accompanied by the normal degradation of energy available when the data is being read and therefore a greater vulnerability to perturbations. Added to this are the increased effects of interference between neighbours. Today, it is essential to use tried and tested techniques in telecommunications systems, especially coding and equalization, in order to counter the effects induced by the miniaturization of these storage devices. Although *Codes and Turbo codes* does not explicitly tackle these applications, the concepts developed and the algorithms presented herein are also a topical issue for mass memory providers.

This book therefore deals mainly with error-correction coding, also called channel coding, and with its applications to digital communications, in association with modulation. The general principles of writing redundant information and most of the techniques imagined up until 1990 to protect digital transmissions, are presented in the first half of the book (chapters 1 to 6). In this first part, one chapter is also dedicated to the different modulation techniques without which the coded signals could not be transported in real transmission environments. The second part (chapters 7 to 11) deals with turbo codes, invented more recently (1990-93), whose correction capability, neighbouring on the theoretical limits predicted by Shannon, have made them a coding standard in more and more applications. Different versions of turbo codes, as well as the important family of LDPC codes, are presented. Finally, certain techniques using the principles of turbo-decoding, like turbo-equalization and multi-user turbo-detection, are introduced at the end of the book.

A particular characteristic of this book, in comparison with the way in which the problem of coding may be tackled elsewhere, is its concern with applications. Mathematical aspects are dealt with only for the sake of necessity, and certain results, which depend on complex developments, will have to be taken as given. On the other hand, practical considerations, particularly concerning the processing algorithms and circuits, are fully detailed and commented upon. Many examples of performance are given, for different coding and coded modulation schemes.

The book's authors are lecturers and researchers well-known for their expertise in the domain of algorithms and the associated circuits for communications. They are, in particular, the inventors of turbo codes and responsible for generalizing the "turbo principle" to different functions of data processing in receivers. Special care has been taken in writing this collective work vis-à-vis the unity of point of view and the coherence of notations. Certain identical or similar concepts may, however, be introduced several times and in different ways, which – we hope – does not detract from the pedagogy of the work, for pedagogy is the art of repetition. The aim of *Codes and turbo codes* is for it to be a book not only for learning about error-correction coding and decoding, a precious source of information about the many techniques imagined since the middle of the twentieth century, but also for addressing problems that have not yet been completely resolved.

[1] A. J. Viterbi, "Error Bounds for Convolutional Codes and an Asymptotically Optimum Decoding algorithm", *IEEE Trans. Inform. Theory*, vol. IT-13, pp. 260-269, Apr. 1967.

[2] C. E. Shannon, "A Mathematical Theory of Communication", *Bell System Technical Journal*, Vol. 27, July and October 1948.

Contents