Codes et turbocodes

Springer
Paris
Berlin
Heidelberg
New York
Hong Kong
Londres
Milan
Tokyo

Ouvrage écrit sous la direction de
Claude Berrou

Codes et turbocodes

Springer

Claude Berrou
École Nationale Supérieure des Télécommunications de Bretagne
CS 83818
29238 Brest Cedex 3

ISBN 13 : 978-2-287-32739-1 Springer Paris Berlin Heidelberg New York

Printed in France
Springer-Verlag France est membre du groupe Springer Science + Business Media

SPIN: 11682165

Maquette de couverture : Jean-François MONTMARCHÉ
Illustration de couverture : Jean-Noël JAFFRY

Liste des contributeurs

Cet ouvrage a été rédigé sous la direction de Claude Berrou avec la contribution de :

Karine Amis,
Matthieu Arzel,
Catherine Douillard,
Alain Glavieux †,
Frédéric Guilloud,
Michel Jézéquel,
Sylvie Kerouédan,
Charlotte Langlais,
Christophe Laot,
Raphaël Le Bidan,
Émeric Maury,
Samir Saoudi,
Yannick Saouter,
tous de l'École nationale supérieure des télécommunications de Bretagne,

Gérard Battail,
de l'École nationale supérieure des télécommunications,

Emmanuel Boutillon,
de l'Université de Bretagne Sud,

et avec le concours précieux de Mohamed Koubàa et de Nicolas Puech.

« Les deux mots les plus brefs et les plus anciens, oui et non, sont ceux qui exigent le plus de réflexion »

Pythagore, V^{e} siècle av. J.C.

À nos regrettés collègues et amis Alain Glavieux et Gérard Graton.

Avant-propos

C'est un double *big bang* qui a ouvert ce que l'on appelle communément aujourd'hui l'ère de l'information. Nous sommes en 1948 et les États-Unis d'Amérique continuent d'investir massivement dans la recherche de haute technologie, dont ils ont tiré les premiers bénéfices durant le conflit mondial. Dans les *Bell Telephone Laboratories*, installés dans le New Jersey, au sud de New York, plusieurs équipes se sont constituées autour de brillants chercheurs, pour beaucoup formés au MIT (*Massachusetts Institute of Technology*). Cette année-là se produisent deux découvertes exceptionnelles, l'une technologique, l'autre théorique, qui vont profondément marquer le $20^{\text{ème}}$ siècle. C'est en effet à quelques mois d'intervalle et dans le même établissement que John Bardeen, Walter Brattain et William Shockley inventent le transistor et que Claude Elwood Shannon établit la théorie de l'information et des communications numériques. Prodigieuse coïncidence qui fait naître comme presque jumeaux le composant semi-conducteur qui, suivant son état de conduction (ouvert ou fermé), est capable de représenter matériellement une information binaire (0 ou 1) et le *shannon* ou *bit* (contraction de *b*inary un*it*), unité de mesure de l'information.

On mesure bien aujourd'hui toute l'importance de ces deux inventions qui ont permis le formidable essor de l'informatique et des télécommunications, entre autres. Depuis 1948, les fulgurants progrès de l'électronique, puis de la micro-électronique, ont offert aux ingénieurs et chercheurs du monde des télécommunications le support de leurs innovations, pour accroître, toujours et toujours, les performances de leurs systèmes. Qui aurait pu imaginer, il y a peu, qu'un programme de télévision pourrait être transmis par une paire de fils téléphoniques ? En somme, Shockley et ses collègues, à travers la loi de Gordon Moore (doublement, tous les 18 mois, du nombre de transistors dans une même surface de silicium), ont apporté petit à petit les moyens de répondre aux défis lancés par Shannon, grâce à des algorithmes qui ne pouvaient être que de plus en plus complexes. Un exemple typique en est l'invention, plutôt tardive, des turbocodes et des traitement itératifs dans les récepteurs, qui ne purent être imaginés que parce que les dizaines ou centaines de milliers de transistors requis étaient disponibles.

Les experts de la micro-électronique prévoient comme butée finale de la technologie CMOS, vers 2015, autour de trois milliards de transistors par centimètre carré. C'est l'ordre de grandeur du nombre de neurones dans le cerveau humain (qui restera cependant incomparablement plus puissant, du fait de son extraordinaire réseau de connexions - plusieurs milliers de synapses par neurone). Des milliards de transistors dans une même puce, cela veut dire que les algorithmes les plus exigeants en ressources calculatoires, au moins parmi ceux qui sont connus aujourd'hui, y trouveront leur place sans jouer des coudes. Pour reprendre le slogan d'un fabricant de circuits intégrés : « la limitation n'est pas dans le silicium, elle est dans votre imagination ». Pour être honnête, précisons quand même que la conception et le test de ces fonctions complexes seront loin d'être aisés.

Cependant nous sommes déjà bien loin de l'époque où Andrew Viterbi, pour conclure la présentation de son fameux algorithme, en 1967, affichait un scepticisme à la mesure de sa modestie : « Bien que cet algorithme soit irréaliste du fait des contraintes excessives de mémorisation, il contribue à une compréhension générale des codes convolutifs, à travers sa simplicité opératoire et son analyse » [1]. Un décodeur de Viterbi, c'est aujourd'hui seulement un dixième de millimètre carré de silicium dans un téléphone portable.

Parmi les résultats présentés par Shannon dans la publication fondatrice [2], celui-ci est particulièrement étonnant : *dans une transmission numérique en présence de perturbation, si le niveau moyen de celle-ci ne dépasse pas un certain seuil de puissance et en utilisant un codage approprié, le récepteur peut identifier le message d'origine sans aucune erreur.* Par codage, on entend ici, comme dans la totalité du livre, codage correcteur d'erreurs, c'est-à-dire écriture redondante de l'information binaire. Le codage de source (compression numérique), le codage cryptographique, ou tout ce que le mot codage peut avoir comme autre signification, ne sont pas traités dans *Codes et turbocodes*.

Le résultat théorique établi par Shannon a constitué pour des milliers de chercheurs et d'ingénieurs un défi scientifique majeur car l'enjeu économique est considérable. Améliorer le pouvoir de correction d'un code, c'est à même qualité d'information reçue (par exemple, pas plus d'une information binaire fausse sur 10.000 reçues en téléphonie numérique), permettre au système de transmission de fonctionner dans des conditions plus sévères. Il est alors possible de réduire la taille des antennes, le poids des batteries d'alimentation ou l'encombrement des panneaux solaires. Dans les systèmes spatiaux (satellites, sondes, ...), l'économie peut se chiffrer en dizaines de millions de dollars, car le poids des équipements et la puissance du lanceur s'en trouvent notablement réduits. Dans les systèmes cellulaires de téléphonie mobile, améliorer le code, c'est aussi permettre à l'opérateur d'augmenter le nombre d'utilisateurs potentiels dans la cellule. Aujourd'hui, rares sont les systèmes de télécommunications qui n'intègrent pas dans leur spécification un code correcteur d'erreurs.

Un autre domaine d'applications des codes correcteurs est celui des mémoires de masse : disques durs d'ordinateurs, CD-ROM, DVD, ... Les progrès réalisés ces dernières années sur la miniaturisation des motifs élémentaires de mémorisation, magnétiques ou optiques, se sont accompagnés d'une dégradation inévitable des énergies disponibles lors de la lecture des données et donc d'une plus grande vulnérabilité aux perturbations. A cela s'ajoutent des effets accrus d'interférences entre voisins. L'utilisation de techniques déjà éprouvées dans les systèmes de télécommunications, codage et égalisation notamment, s'avère aujourd'hui indispensable pour contrer les effets induits par la miniaturisation de ces dispositifs de stockage. Bien que *Codes et turbocodes* n'aborde pas explicitement ces applications, les concepts qu'on y trouve développés, les algorithmes qui y sont présentés sont aussi d'une grande actualité dans l'industrie des mémoires de masse.

Cet ouvrage est donc principalement consacré au codage correcteur d'erreurs, encore appelé codage de canal, et à ses applications aux communications numériques, en association avec les modulations. Les principes généraux de l'écriture redondante de l'information et la plupart des techniques imaginées jusqu'en 1990 pour protéger les transmissions numériques, sont présentés dans la première moitié du livre (chapitres 1 à 6). Dans cette première partie, un chapitre est également dédié aux différentes techniques de modulation, sans lesquelles les signaux codés ne pourraient être véhiculés dans les milieux réels de transmission. La deuxième partie (chapitres 7 à 11) est consacrée aux turbocodes, inventés plus récemment (1990-93), et dont le pouvoir de correction, qui avoisine les limites théoriques prédites par Shannon, en fait un standard de codage dans des applications de plus en plus nombreuses. Différentes versions de turbocodes, ainsi que la famille des codes LDPC, sont présentées. Enfin, certaines techniques utilisant les principes du turbo-décodage, telles que la turbo-égalisation et la turbo-détection multi-utilisateurs, sont introduites en fin d'ouvrage.

Une caractéristique particulière de ce livre, par comparaison avec la manière dont peut être ailleurs abordé le problème du codage, est le souci de l'application. Les aspects mathématiques n'y sont traités que par nécessité et certains résultats, qui reposent sur des développements complexes, devront être admis. En revanche, les considérations pratiques, en particulier sur les algorithmes et les circuits de traitement, y sont largement détaillées et commentées. De nombreux exemples de performance sont fournis, pour différents schémas de codage et de modulations codées.

Les auteurs du livre sont des enseignants-chercheurs reconnus pour leur expertise dans le domaine des algorithmes et des circuits associés pour les communications. Ils sont notamment à l'origine des turbocodes et de la généralisation de « l'effet turbo » aux différentes fonctions de traitement de l'information dans les récepteurs. Un soin particulier a été apporté dans la rédaction de cet ouvrage collectif, vis-à-vis de l'unité de vue et de la cohérence des notations. Certains concepts, identiques ou similaires, peuvent toutefois y être introduits

à plusieurs reprises et de différentes manières, ce qui – espérons-le – n'enlève rien à la pédagogie de l'ouvrage car celle-ci est l'art de la répétition. *Codes et turbocodes* a été pensé pour être à la fois un livre de découverte du codage et du décodage correcteur d'erreurs, une source précieuse d'informations sur les nombreuses techniques imaginées depuis le milieu du vingtième siècle, et une ouverture vers des problèmes non encore complètement résolus.

Brest, Octobre 2006
Claude Berrou

[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.

Nota Bene : tout commentaire sur le contenu de cet ouvrage peut être envoyé à l'adresse électronique suivante : `turbocode@mlistes.enst-bretagne.fr`

Sommaire