

LIVRE : THÉORIE DES CODES : COMPRESSION, CRYPTAGE, CORRECTION

FICHE N° 15675

PRÉSERVER
SAUVEGARDER
VALORISER

Période de fabrication : 2000-2024
Fabricant : fabricant non renseigné
Domaines : Informatique et Communication
Sous-domaines : Ordinateurs
Organisme : ACONIT
Ville : Grenoble (Isère)
Modèle :
Matériaux : Papier

Description

Titre traduit : Error code correction ; foundation of coding

Ce document de 401 pages a pour titre Théorie des codes : compression, cryptage, correction. Il est une 3ème édition datée de 2018 (précédentes 2009, 2013). L'éditeur est Dunod. Une édition anglaise existe chez Wiley depuis 2015 sous le titre Foundations of Coding.

Parmi les domaines les plus importants couverts sont donc : les codes de corrections d'erreurs ; le codage des images en JPEG.

Les quatre auteurs sont des enseignants-chercheurs de l'ENSIMAG-ENSERG télécommunications à l'INPG de Grenoble, de l'INRIA Rhône-Alpes et de l'Université du Luxembourg.

L'ouvrage est structuré en quatre chapitres, (1-Théorie des codes, 2-Information et compression, 3-cryptologie, 4-détection et correction d'erreurs), et il est complété par une Bibliographie de 41 références et un Index de 12 pages.

De nombreux exercices sont proposés, dont les corrections sont présentées à la fin du livre ou accessibles par Internet.

Ce livre rend compte des débuts dans ce domaine :

- les codes de Hamming binaires datant de 1950, des codes correcteurs à redondance minimale (page 260) ; les codes LDPC (Low Density Parity Check) qui sont une classe de codes linéaires par blocs (p. 269), standardisés par les recommandations IEEE 802 ; par exemple le Minitel utilisait un code de Hamming par blocs de 15 octets, avec un 16ème octet de contrôle.

- les codes de Huffman, du type de codage statistique (page 111), codes de compression optimisés en longueur variable, avec leur arbre de représentation (page 76), un système de codes datant de 1952 ; un tel code est utilisé pour les images codées en JPEG (cf. <https://en.wikipedia.org/wiki/JPEG> et norme ISO/IEC 10918). En particulier les pages 139 à 145 détaillent le format JPEG qui compresse les images fixes avec perte d'information en calculant les fréquences spatiales par Transformée de Fourier discrète, leur « tatouage » (p. 142), le standard JPEG-2000 qui améliore la transformée en fréquence en remplaçant le standard DCT-JPEG de transformée en cosinus (norme datant de 1992), par une transformée en ondelettes. Il décrit les méthodes de protection avec un brouillage par ondelettes pour accès conditionnel (page 143). Est aussi décrit le format MPEG pour les images en séquence vidéo (M pour Motion picture) tenant compte de la corrélation entre images successives.

- les codes cycliques BCH (une extension du code de Hamming, et non de Huffman, codes très fameux nommés selon les initiales de leurs inventeurs Bose, Chaudhuri, Hocquenghem, ce dernier étant Alexis Hocquenghem un français du CNAM, qui fut mondialement renommé pour la publication de ces travaux en 1959, un renom qui lui permettait d'envoyer ses étudiants dans tout important laboratoire de par le monde) ;

Le livre commence par décrire ce qu'est un codage (page 8) en prenant l'exemple d'une image transmises par fax, avec une digitalisation de 1728 pixels.

Le livre développe les théories mathématiques à la base de ces codages et moyens de contrôle. De nombreuses tables et figures (ainsi par exemple le décodage itératif d'un turbo-code p. 310) synthétisent les algorithmes correspondants.

Une liste des algorithmes utilisés est donnée (page 382)

Utilisation

Les sujets traités dans cet ouvrage concernent de manière non limitative : les codes d'intégrité et d'authentification de la source (page 80) ; la cryptographie (chapitre 3) ; le standard de signature digitale (page 199) ou son modèle hybride (p. 222) ; les contrôles de parité sur les entiers comme le numéro de Sécurité Sociale, l'ISBN d'identification des

livres, ou la clef RIB d'un compte bancaire (page 248) ; les codes-barres comme le EAN-13 ou EN-128 (page 249), le codage des images en JPEG, ainsi que plusieurs autres sujets spécialisés.

Ce livre est basé sur des cours donnés à l'ENSIMAG (Grenoble) à partir de 2007.

En ce qui concerne le chapitre 4 intitulé Détection et correction d'erreurs, on y lit que les chapitres précédents dans le livre supposaient que toutes les communications étaient "sans bruit", c'est-à-dire qu'un message émis était systématiquement reçu tel quel, ou du moins que les seuls possibles altérations éventuelles seraient dues à un tiers mal intentionné qui savait les masquer. En réalité, il faut aussi tenir compte des altérations possibles du message dues au canal de transmission. La table 4.1 donne des ordres de grandeur du taux d'erreurs selon le type de canal utilisé. Les supports de stockage en mémoires contiennent eux aussi des erreurs.

Par rapport à une information analogique, un intérêt fondamental d'une information numérique (donc sous forme de symboles discrets comme des bits) est qu'il existe des formats de représentation des données qui permettent de retrouver l'information initiale lorsque le taux d'erreurs est borné. Développée à partir d'un article fondateur de Shannon, au milieu XX^e siècle, la théorie du codage de canal, souvent dénommée théorie des codes, a pour objet l'étude et la construction de telles représentations - les codes correcteurs - qui soient les plus performantes possibles.

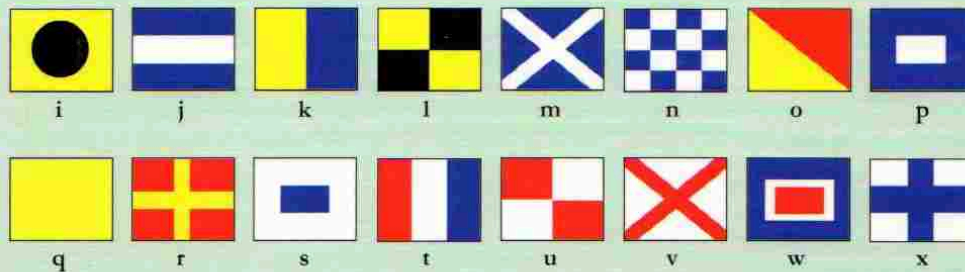
Ce chapitre introduit les principaux types de codes : codage par blocs, détection de parité, de parité longitudinale et transversale, second théorème de Shannon, multiplication matrice-vecteur, les algorithmes de propagation, les codes cycliques, l'entrelacement, et en particulier les codes détecteurs et correcteurs d'erreurs : CRC, LDPC (et sa représentation par graphe de Tanner), Reed-Solomon, l'algorithme de Viterbi, les turbo-codes, LUHN, distance de Hamming, code de Golay, de Berlekamp-Welch, BCH, CIRC.

Les turbo-codes (page 311) ont été intégrés dans de nombreux standards et en particulier pour les communications spatiales. L'European Space Agency a été la première à les utiliser pour la sonde lunaire Smart-1 lancée en 2003. La NASA les utilise depuis 2003 pour toutes ses sondes spatiales. Les turbo-codes sont utilisés dans les téléphones portables UMTS, l'ADSL (version 2, 3G, 4G), la télévision haute définition (HDTV) normalisée en 2005.

Le livre traite aussi les codes-barres bidimensionnels QR (page 293)

Théorie des codes

Compression, cryptage, correction



Jean-Guillaume Dumas
Jean-Louis Roch
Éric Tannier
Sébastien Varrette

3^e édition

DUNOD

Ligne	Taux d'erreurs
Disquette	10^{-9} : à 5 Mo/s, 3 bits erronés par minute
CD-ROM optique	10^{-5} : 7ko erronés sur un CD de 700 Mo
DAT audio	10^{-5} : à 48 kHz, deux erreurs par seconde
Disques Blu-ray	$< 2 \cdot 10^{-4}$: environ 1.6Mo erronés pour 32Go
Hard Disk Drives (HDD)	$> 10^{-4}$: environ 10^6 erreurs pour 10Go
Technologie Flash	10^{-5}
Solid State Drives (SSD)	$< 10^{-5}$
Mémoires à semi-conducteurs	$< 10^{-9}$
Liaison téléphonique	entre 10^{-4} et 10^{-7}
Télécommande infrarouge	10^{-12}
Communication par fibre optique	10^{-9}
Satellite	10^{-6} (Voyager), 10^{-11} (TDMA)
ADSL	10^{-3} à 10^{-9}
Réseau informatique	10^{-12}

Table 4.1 – Ordre de grandeur du taux d'erreurs.

$$H = \begin{bmatrix} 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}$$

$$w_c = 2, w_r = 4.$$

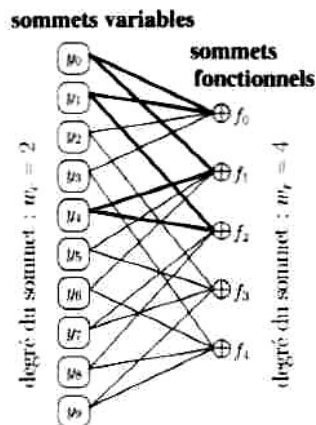


Figure 4.2 – Exemple d'un code LDPC régulier (10,5) et de sa représentation par un graphe de Tanner. Les six arêtes en gras illustrent un cycle de longueur 6.

Pour nous citer :

Base de la Mission nationale de sauvegarde et de valorisation du patrimoine scientifique et technique contemporain, PATSTEC, Livre : Théorie des codes : compression, cryptage, correction (fabricant non renseigné), <https://www.patstec.fr/ressources/objets/detail?id=29598>, consulté le 2026-07-18