28434 PADOVAN Dorian

Codes correcteurs d'erreurs : Une garantie pour les transferts d'information.

Les procédés utilisés pour garantir une transmission de l'information correcte et efficace m' intéressent depuis quelques années. Ce sujet, orienté sur l'algèbre des codes correcteurs d' erreurs, propose des méthodes de vérification de transferts effectués. Il m'a ainsi aussi pu renforcer mon intérêt pour l'algèbre tout en apportant des utilisations concrètes.

Pour garantir une transition correcte d'information entre deux interlocuteurs, il est essentiel de concevoir des algorithmes vérifiant qu'aucune corruption dans le transfert n'a eu lieu.

Positionnement thématique (ÉTAPE 1) :

- *INFORMATIQUE (Informatique Théorique)*
- *MATHEMATIQUES (Algèbre)*
- *INFORMATIQUE (Informatique pratique)*

Mots-clés (ÉTAPE 1) :

Mots-clés (en français)	**Mots-clés (en anglais)**
Codes correcteur d'erreurs	*Error-correcting code*
Codes linéaire	*linear code*
Codes de Hamming	*Hamming Code*
Codes de Reed-Solomon	*Reed-Solomon code*
théorie de l'information	*information theory*

Bibliographie commentée

Dans l'intention de rendre le transport d'information plus sécurisé Richard Hamming développa des codes correcteurs permettant de régler des problèmes sans la présence d'un ingénieur [1]. En parallèle, Claude Shannon proposa une théorie de l'information permettant d'étudier les limites des codes correcteurs [2].

Les codes correcteurs (n,k) ont pour but de faire parvenir un message avec la plus grande exactitude possible. Pour cela, il faut ajouter une certaine redondance dans le message pour pouvoir le reconstruire. Mathématiquement, cela correspond à une application avec un ensemble

de départ de dimension k représentant le message brut et celui d'arrivée de dimension n représentant le message codé . [3][4]

Naïvement, dans un canal qui altère peu un bit avec une certaine probabilité, on peut penser à mettre n bits à la place d'un seul puis prendre la majorité des valeurs lorsque l'on décode[5]. Cependant le rendement de ce code n'est pas bon. En effet, un message de longueur m est transformé en un message de taille nm. Cependant, en rajoutant 1 seul bit ayant pour rôle d' avoir un nombre pair de 1, on peut détecter une erreur en vérifiant la parité du nombre de 1 à l'arrivée avec un rendement de m/(m+1). Toutefois, on ne peut pas la corriger. Il s'agit donc d' avoir un code correcteur garantissant la correction de l'information avec un bon rendement.[3]

Dans les cas des codes de Hamming (n,k) on a n = 2 ^{m}-1 et k = n-m où m représente le nombre de bits de redondance utilisés pour garantir la correction. L'idée derrière ce code est d' utiliser ces m bits comme bits de parité mais sur des sections représentant chacune la moitié des bits du message. Avec une bonne répartition, cela permet de non seulement détecter une erreur mais aussi de la localiser. Avec cette méthode, le message est en mesure d'être restitué avec un rendement de k/m ce qui est bien meilleur que la méthode naïve. Cependant ce code ne permet de corriger le message seulement si il n'y a qu'une erreur.[1][3]

Les codes de Reed-Solomon utilisent la structure des corps finis et l'unicité des polynômes de Lagrange pour corriger les erreurs.En effet, si l'on découpe un message en n séquence de bits représentant chacune un entier, on peut trouver l'unique polynôme de Lagrange de degré n-1 tel que l'évaluation de l'indice d'une séquence par le polynôme correspond à l'entier représenté par la séquence. Par la suite, on obtient le message à transmettre en rajoutant au message initial k autres valeurs obtenues en évaluant le polynôme. Lorsque le message est reçu, si moins de k valeurs sont perdues, on peut les retrouver en retrouvant le polynôme puis en l'évaluant. [6][7]

Problématique retenue

Par quels outils et propriétés mathématiques les codes correcteurs d'erreurs permettent de garantir une transition correcte d'information ?

Objectifs du TIPE du candidat

Je cherche donc à travers mon TIPE à :

→étudier la théorie des codes correcteurs.

→me familiariser avec le fonctionnement et les limites des codes de Hamming et Red Solomon.

→comparer les codes correcteurs entre eux.

Références bibliographiques (ÉTAPE 1)

[1] RICHARD HAMMING : Error Detecting and Error Correcting Codes Théorie des codes *: https://zoo.cs.yale.edu/classes/cs323/doc/Hamming.pdf*

[2] CLAUDE ELWOOD SHANNON : A Mathematical Theory of Communication *: https://people.math.harvard.edu/~ctm/home/text/others/shannon/entropy/entropy.pdf*

[3] JEAN-GUILLAUME DUMAS, JEAN-LOUIS ROCH, ÉRIC TANNIER AND SÉBASTIEN VARRETTE : Théorie des codes *: Dunod 2013, ISBN 978-2-10-059911-0*

[4] MICHEL DEMAZURE : Cours d'algèbre *: Cassini 2008, ISBN 2-84225-000-1*

[5] PIERRE ABBRUGIATI : Introduction aux codes correcteurs d'erreurs *: https://www.lirmm.fr/~chaumont/download/cours/codescorrecteur/Cours_Pierre_Abbrugiati.pdf*

[6] ALEXEI PANTCHICHKINE : Mathématiques des codes correcteurs d'erreurs,"Cryptologie, Sécurité et Codage d'Information" *: https://www-fourier.ujf-grenoble.fr/~panchish/04cc*

[7] SATISH RAO : Discrete Mathematics and Probability Theory *: https://www.eecs70.org/assets/pdf/notes/n9.pdf*