

Transmission d'images : Code de Golay - Code de Reed-Solomon

Les codes correcteurs nous semblaient être un sujet intéressant et, au cours de nos recherches, nous avons découvert plus précisément le thème de la transmission d'image, qui nous a paru pertinent. De plus, l'usage aussi bien des codes de Golay que de Reed-Solomon nous a permis d'enrichir notre travail.

La communication est un des enjeux principaux de notre société. Or, des erreurs peuvent survenir, nécessitant des corrections. C'est notamment le cas dans la transmission d'images, comme dans le programme Voyager (1977). Les codes de Golay et de Reed-Solomon, que nous avons étudiés, ont permis la transmission correcte de ces images.

Ce TIPE fait l'objet d'un travail de groupe.

Liste des membres du groupe :

- CHARVIN *Eléonore*

Positionnement thématique (ETAPE 1)

INFORMATIQUE (Informatique Théorique), MATHÉMATIQUES (Algèbre).

Mots-clés (ETAPE 1)

Mots-Clés (en français)	Mots-Clés (en anglais)
<i>Codes correcteurs d'erreurs</i>	<i>Error-correcting codes (ECC)</i>
<i>Code de Reed-Solomon</i>	<i>Reed-Solomon code</i>
<i>Code de Golay</i>	<i>Golay code</i>
<i>Polynôme générateur</i>	<i>Generator polynomial</i>
<i>Transmission d'image</i>	<i>Picture transmission</i>

Bibliographie commentée

Lors de sa transmission d'un émetteur vers un récepteur, par exemple lors de missions spatiales, l'information passe par un canal de communication. Ces canaux n'étant pas totalement fiables, l'information peut être altérée. L'information reçue est alors différente de celle émise. Bien que semblant superflue, cette différence peut avoir de multiples conséquences. Il est donc intéressant de pouvoir trouver ces erreurs et les corriger. C'est le but des **codes correcteurs d'erreurs**. Le principe de la majorité de ces codes repose sur l'introduction d'une redondance dans le message initial. Cette redondance est obtenue à l'aide d'opérations, plus ou moins nombreuses et complexes en fonction des types de codes, effectuées sur les composantes du message envoyé.

Un alphabet est un ensemble, dont les éléments sont appelés lettres (ou symboles), à partir duquel les mots du message sont engendrés comme suites de lettres. On choisit généralement pour alphabet un corps fini F_q à q éléments. **[1]**

Un **polynôme générateur** est un polynôme unitaire de $F_q[X]$ diviseur de $X^n - 1$. On appelle matrice génératrice d'un code la matrice de taille $n \times k$ dans les bases canoniques d'une application linéaire g injective de F_q^k dans F_q^n qui à un mot de k lettres à communiquer associe un mot codé de n lettres, où $k < n$. Cette matrice contient la redondance qui permettra de détecter une erreur et de corriger le message reçu en cas d'erreur de transmission. L'ensemble $g(F_q^k)$ est appelé code. [2]

Pour repérer les erreurs introduites lors de la transmission et retrouver le message envoyé à partir du message reçu, on utilise la distance de Hamming entre deux éléments de F_q^n . Cette distance est égale au nombre de symboles de l'alphabet dont diffèrent ces deux éléments. [3] On définit alors la distance minimale, notée d , comme étant la plus petite distance entre deux éléments distincts du code.

Un code est ainsi décrit par le triplet (n, k, d) où n est la longueur du code (dimension de l'espace d'arrivée de g), k la dimension du code (dimension de l'espace de départ de g) et d la distance minimale entre deux mots du code. Ce triplet permet d'estimer les capacités de détection et de correction qui sont les plus grands nombres d'erreurs que l'on peut respectivement détecter et corriger. Un code de capacité de correction e est dit e -correcteur.

Il existe plusieurs types de codes linéaires (n, k, d) sur un corps fini F_q . Ce sont des sous-espaces vectoriels de dimension k de F_q^n . En particulier, les codes cycliques sont des codes linéaires notés C tels que si (x_1, \dots, x_n) est dans C alors $(x_n, x_1, \dots, x_{n-1})$ est dans C . Les codes de correction de **Reed-Solomon** [4] et de **Golay** [5] ont été utilisés pour la **transmission d'images** dans le cadre des missions Voyager de la NASA.

Il est intéressant de chercher à comparer le taux de transmission k/n , la probabilité d'erreurs résiduelles après correction et la pertinence de ces deux codes pour la **transmission d'images**. [6][7]

Problématique retenue

La **transmission d'images** en couleur nécessite la transmission de données, sujette à des erreurs éventuelles. L'enjeu consiste donc à détecter et corriger ces erreurs, en ayant les plus grands taux de transmission et capacité de correction possibles tout en conservant une probabilité d'erreurs résiduelles la plus petite possible.

Objectifs du TIPE

- Comprendre des notions d'algèbre relative à la théorie des corps finis
- Implémenter le **code de Reed-Solomon**
- L'appliquer à une image entachée d'erreurs

- Comparer les résultats avec le **code de Golay** (probabilité d'erreurs résiduelles, capacité de correction et taux de transmission)

Références bibliographiques (ETAPE 1)

- [1] ODILE PAPINI, JACQUES WOLFMANN : Algèbre discrète et codes correcteurs : *Springer-Verlag*. (1994)
- [2] PIERRE WASSEF : Cours d'arithmétique à l'université Pierre et Marie Curie : <https://perso.univ-rennes1.fr/christophe.mourougane/enseignements/2007-8/arithmetique.pdf>
- [3] PIERRE MEUNIER : Algèbre : Cryptologie - Codes linéaires correcteurs d'erreurs : *Cépaduès Edition*. (2016)
- [4] R. J. MCELIECE : The Decoding of Reed-Solomon Codes : *California Institute of Technology*. (1988) <https://ntrs.nasa.gov/citations/19890010973>
- [5] T. K. TRUONG, J. K. HOLMES, I. S. REED, X. YIN : A simplified procedure for decoding the (23,12) and (24,12) Golay codes : *University of Southern California*. (1989) <https://ntrs.nasa.gov/citations/19890010085>
- [6] ABBAS DANDACHE, THIERRY VALLINO, FABRICE MONTEIRO, JEAN-PIERRE DELAHAYE : Code Reed-Solomon (127, k, d) avec effacements : simulation et conception sur réseaux de circuits programmables (FPGA) : <http://documents.irevues.inist.fr/bitstream/handle/2042/2118/005.PDF%20TEXTE.pdf?sequence=1> (1998)
- [7] FRANÇOIS DUBOIS : Codes et Automates finis au CNAM : <https://www.imo.universite-paris-saclay.fr/~fdubois/cours/codes-automates/codauto-cours-06-18mars2020.pdf> (2020)

DOT

- [1] [Septembre 2020 - Découverte du sujet des codes correcteurs d'erreurs et compréhension de notions algébriques et informatiques à l'aide du livre [1]]
- [2] [Novembre 2020 - Décision d'étudier le code de Reed-Solomon à l'aide du livre [3]]
- [3] [Décembre 2020 - En recherchant les applications du code de Reed-Solomon, découverte du code de Golay et décision d'étudier individuellement ces deux codes]
- [4] [Février 2021 - Choix de l'application à la transmission d'image, avec l'exemple des missions Voyager, ayant utilisé ces codes]
- [5] [Mai 2021 - Résolution des difficultés rencontrées lors de l'étude et l'implémentation des racines primitives des corps finis]