Université Paris 13 Année 2021–2022

M2 Mathématiques des données

Codes correcteurs

Notes de cours (en construction)

Julien Lavauzelle
julien.lavauzelle@univ-paris8.fr

29 décembre 2021

Table des matières

Quelques références utiles

Notes de cours introductives à la théorie des codes

[Cou20] Alain Couvreur. Introduction to coding theory. `http://www.lix.polytechnique.fr/~alain.couvreur/doc_ens/lecture_notes.pdf`, 2020

Livres génériques sur la théorie des codes

[HP03] W. Cary Huffman and Vera Pless. *Fundamentals of Error-Correcting Codes*. Cambridge University Press, 2003

[vL99] Jacobus H. van Lint. *Introduction to Coding Theory, 3rd edition*. Springer, 1999

Codes géométriques (autre partie de cours)

[HvLP11] Tom Høholdt, Jacobus H. van Lint, and Ruud Pellikaan. Algebraic geometry codes. In *Handbook of Coding Theory*, volume 1, pages 871–961. 2011

[Wal] Judy L. Walker. Codes and curves. `https://cdn.preterhuman.net/texts/math/Codes%20and%20Curves.pdf`

Chapitre 1

Introduction

1.1 Contenu du cours

Ce document résume une partie[1] du contenu du cours de *Codes correcteurs* enseigné aux étudiants de M2 du *Master Mathématiques et applications* de l'Université Paris 13, en 2021–2022.

L'intention du cours est de faire découvrir des applications avancées et originales des codes correcteurs, qui pour certaines s'appuient sur des constructions algébriques ou géométriques. Le cours s'articule suivant trois axes :

1. la notion de localité en théorie des codes, et son application au stockage distribué (Chapitre 2) ;
2. l'utilisation des codes correcteurs en cryptographie, *via* le système de chiffrement de McEliece (Chapitre **??**) ;
3. le décodage en liste, qui permet de corriger davantage d'erreurs au prix d'une certaine incertitude dans le décodage (Chapitre **??**).

Bien qu'il soit présupposé que les étudiants aient suivi une introduction aux codes correcteurs, nous donnons ci-dessous un rappel de notions fondamentales utiles à la compréhension des chapitres suivants.

1.2 Rappels

En complément de ces rappels, nous invitons les étudiants à également lire les notes de cours suivantes : [Cou20].

1.2.1 Notations

On note $\mathbb{F}_q$ le corps fini à q éléments et $[1,n] \coloneqq \{1,\dots,n\}$. Les vecteurs $\boldsymbol{a} = (a_1,\dots,a_n) \in \mathbb{F}_q^n$ sont usuellement notés comme des vecteurs lignes. Les vecteurs $(0,\dots,0)$ et $(1,\dots,1)$ sont respectivement représentés par $\mathbf{0}$ et $\mathbf{1}$.

Le produit scalaire entre deux vecteurs $\boldsymbol{a},\boldsymbol{b} \in \mathbb{F}_q^n$ est noté $\langle \boldsymbol{a},\boldsymbol{b} \rangle \coloneqq \sum_{i=1}^n a_i b_i$.

Pour $\boldsymbol{a},\boldsymbol{b} \in \mathbb{F}_q^n$, on note $\mathrm{d_H}(\boldsymbol{a},\boldsymbol{b}) \coloneqq |\{i \in [1,n] \mid a_i \neq b_i\}|$ la distance de Hamming entre $\boldsymbol{a}$ et $\boldsymbol{b}$. Le poids de Hamming de $\boldsymbol{a}$ est alors $\mathrm{wt}(\boldsymbol{a}) \coloneqq \mathrm{d_H}(\boldsymbol{a},\mathbf{0}) \coloneqq |\{i \in [1,n] \mid a_i \neq 0\}|$.

Le support d'un vecteur $\boldsymbol{a} \in \mathbb{F}_q^n$ est $\mathrm{supp}(\boldsymbol{a}) \coloneqq \{i \in [1,n] \mid a_i \neq 0\}$. Son cardinal est donc $\mathrm{wt}(\boldsymbol{a})$.

Si $\boldsymbol{a} \in \mathbb{F}_q^n$ et $I \subset [1,n]$ est non-vide, alors $\boldsymbol{a}_{|I} \in \mathbb{F}_q^{|I|}$ est le vecteur constitué des symboles de $\boldsymbol{a}$ indexés par les éléments de I.

1. L'autre partie du cours est enseignée par P. Boyer, et traite de la notion de *codes géométriques*.

L'espace des matrices à k lignes et n colonnes sur $\mathbb{F}_q$ est noté $\mathbb{F}_q^{k\times n}$, et par convention, si $\boldsymbol{G} \in \mathbb{F}_q^{k\times n}$ et $I \subset [1,n]$, alors $\boldsymbol{G}_{|I} \in \mathbb{F}_q^{k\times |I|}$ est la sous-matrice de $\boldsymbol{G}$ constituée des colonnes indexées par I.

L'ensemble des polynômes de variable X, à coefficients dans $\mathbb{F}_q$, est noté $\mathbb{F}_q[X]$. On note également $\mathbb{F}_q[X]_{<k}$, ou $\mathbb{F}_q[X]_{\leq k-1}$, l'ensemble des polynômes de degré strictement plus petit que k.

1.2.2 Codes correcteurs

Dans ce cours, nous nous intéresserons uniquement au cas de codes correcteurs linéaires, que nous nommerons plus simplement *codes*.

Définition 1.1

Un code $\mathcal{C}$ *de* longueur n *est un $\mathbb{F}_q$-sous-espace vectoriel de $\mathbb{F}_q^n$. On note généralement k sa* dimension, *et d sa* distance minimale, *définie comme :*

$$d \coloneqq \min\{\mathrm{d_H}(\boldsymbol{c},\boldsymbol{c}') \mid \boldsymbol{c},\boldsymbol{c}' \in \mathcal{C},\, \boldsymbol{c} \neq \boldsymbol{c}'\} = \min\{\mathrm{wt}(\boldsymbol{c}) \mid \boldsymbol{c} \in \mathcal{C} \setminus \{\boldsymbol{0}\}\}\,.$$

On note souvent $[n,k,d]_q$, ou $[n,k,d]$, les paramètres d'un code. Par convention, le code de dimension 0 a distance minimale $n+1$.

Si $\mathcal{C}$ est un code $[n,k,d]_q$, alors toute matrice $\boldsymbol{G} \in \mathbb{F}_q^{k\times n}$ telle que

$$\mathcal{C} = \{\boldsymbol{m}\boldsymbol{G}, \boldsymbol{m} \in \mathbb{F}_q^k\}$$

est appelée *matrice génératrice* de $\mathcal{C}$. Les lignes $\boldsymbol{G}$ forment une base de de $\mathcal{C}$. Avec un autre point de vue, toute matrice $\boldsymbol{H} \in \mathbb{F}_q^{(n-k)\times n}$ telle que

$$\mathcal{C} = \{\boldsymbol{c} \in \mathbb{F}_q^n \mid \boldsymbol{H}\boldsymbol{c}^\top = \boldsymbol{0}^\top\}$$

est appelée *matrice de parité*, ou *matrice de contrôle*, de $\mathcal{C}$. On appelle *équation de parité* tout vecteur $\boldsymbol{h}$ tel que $\langle \boldsymbol{h}, \boldsymbol{c}\rangle = 0$ pour tout $\boldsymbol{c} \in \mathcal{C}$. Les lignes de $\boldsymbol{H}$ forment donc une base de l'espace orthogonal à $\mathcal{C}$.

Définition 1.2

Soit $\mathcal{C}$ un code $[n,k,d]_q$. On note $\mathcal{C}^\perp$ l'espace des vecteurs de $\mathbb{F}_q^n$ orthogonaux à ceux de $\mathcal{C}$. Il est appelé code dual *de $\mathcal{C}$. C'est un code de longueur n et de dimension $n-k$. Sa distance minimale est souvent notée $d^\perp$.*

Remarquons qu'une matrice génératrice de $\mathcal{C}^\perp$ est une matrice de parité $\mathcal{C}$, et réciproquement. D'ailleurs, on a $(\mathcal{C}^\perp)^\perp = \mathcal{C}$. En revanche, contrairement à $\mathbb{R}$ ou $\mathbb{C}$, l'intersection $\mathcal{C} \cap \mathcal{C}^\perp$ n'est pas toujours nulle, car il peut exister des vecteurs isotropes non-nuls dans $\mathbb{F}_q^n$, par exemple $(1,1) \in \mathbb{F}_2^2$.

Pour $J \subset [1,n]$ de cardinal $\ell \geq 1$, notons $\pi_J : \mathbb{F}_q^n \to \mathbb{F}_q^{|J|}$ l'application $\boldsymbol{x} \mapsto \boldsymbol{x}_{|J}$.

Définition 1.3

Soit $\mathcal{C}$ un code $[n,k,d]_q$ et $I \subset [1,n]$ de cardinal $1 \leq \ell \leq n-1$. Alors,

1. *le poinçonnement de $\mathcal{C}$ sur I est :*

$$\mathrm{Punct}_I(\mathcal{C}) \coloneqq \{\pi_{[1,n]\setminus I}(\boldsymbol{c}) \mid \boldsymbol{c} \in \mathcal{C}\} \subseteq \mathbb{F}_q^{n-\ell}\,,$$

2. *le raccourcissement de $\mathcal{C}$ sur I est :*

$$\mathrm{Short}_I(\mathcal{C}) \coloneqq \{\pi_{[1,n]\setminus I}(\boldsymbol{c}) \mid \boldsymbol{c} \in \mathcal{C}, \pi_I(\boldsymbol{c}) = \boldsymbol{0}\} \subseteq \mathbb{F}_q^{n-\ell}\,.$$

Proposition 1.4

Pour tout code $\mathcal{C}$ et tout sous-ensemble $I \subset [1,n]$ de cardinal $1 \leq |I| \leq n-1$, on a :

$$\mathrm{Punct}_I(\mathcal{C})^\perp = \mathrm{Short}_I(\mathcal{C}^\perp)\,.$$

Définition 1.5

Soit $\mathcal{C} \subseteq \mathbb{F}_q^n$ un code de dimension k. On appelle ensemble d'information de $\mathcal{C}$ un sous-ensemble $I \subset [1,n]$ de cardinal k, tel que $\pi_I(\mathcal{C})$ est de dimension k. Autrement dit, les coordonnées indexées par I contiennent toute l'information des mots du code.

1.2.3 Bornes

Les paramètres d'un code ne sont pas indépendants les uns des autres. Au-delà du fait que $0 \leq k \leq n$ et $1 \leq d \leq n+1$ (par définition), différentes bornes les régissent.

Proposition 1.6 (*Borne de Singleton*)

Soit $\mathcal{C}$ un code $[n,k,d]_q$. Alors :

$$k + d \leq n + 1\,.$$

Tout code dont les paramètres atteignent la borne de Singleton est appelé code MDS (pour *Maximum Distance Separable* en anglais). Les codes MDS ont d'autres propriétés remarquables (voir TD).

Proposition 1.7 (*Borne de Hamming*)

Soit $\mathcal{C}$ un code $[n,k,d]_q$. Alors,

$$q^k \leq \frac{q^n}{\sum_{i=0}^{t} \binom{n}{i}(q-1)^i}\,, \qquad \text{où } t = \left\lfloor \frac{d-1}{2} \right\rfloor .$$

Tout code dont les paramètres atteignent la borne de Hamming est appelé *code parfait*. Notons qu'un code est parfait si l'ensemble des boules de rayon $t = \left\lfloor \frac{d-1}{2} \right\rfloor$ et dont les centres sont les mots de codes, forment une partition de $\mathbb{F}_q^n$.

Proposition 1.8 (*Borne de Plotkin*)

Soit $\mathcal{C}$ un code $[n,k,d]_q$ tel que $d > \frac{q-1}{q}n$. Alors,

$$q^k \leq \frac{d}{d - \frac{q-1}{q}n}\,.$$

On peut également de questionner sur l'existence de codes ayant certains paramètres.

Proposition 1.9 (*Borne de Gilbert–Varshamov*)

Il existe un code de paramètres $[n,k,d]_q$ tel que :

$$q^k \geq \frac{q^n}{\sum_{i=0}^{d-1} \binom{n}{i}(q-1)^i}.$$

Il peut être intéressant d'observer le comportement de ces bornes lorsque $n \to \infty$. On parle de *bornes asymptotiques*. Pour cela on note :

— $R = \frac{k}{n} \in [0,1]$ le *taux d'information*, ou *rendement*, du code
— $\delta = \frac{d}{n} \in [1/n, 1+1/n]$ la *distance relative* du code.

Asymptotiquement pour $n \to \infty$ (en notant R_∞ et $delta_\infty$ les taux asymptotiques), la borne de Singleton se réécrit $R_\infty + \delta_\infty \leq 1$. La borne de Hamming .....

On peut tracer le graphe de ces bornes :

Todo: tracer le graphe

1.2.4 Quelques constructions

Codes de répétition et de parité. Commençons par donner deux exemples de codes « triviaux » :

— Le *code de répétition* de longueur n sur $\mathbb{F}_q$ est le code de dimension 1 engendré par le vecteur $\mathbf{1} = (1, \dots, 1) \in \mathbb{F}_q^n$. C'est un code $[n, 1, n]_q$.
— Le *code de parité* de longueur n sur $\mathbb{F}_q$ est le code

$$\left\{ \boldsymbol{c} \in \mathbb{F}_q^n \;\middle|\; \sum_{i=1}^{n} c_i = 0 \right\}.$$

Notons qu'une matrice génératrice du code de parité est :

$$\boldsymbol{G} = \begin{pmatrix} 1 & 0 & \dots & \dots & 0 & -1 \\ 0 & 1 & 0 & \dots & 0 & -1 \\ \vdots & \ddots & \ddots & \ddots & \vdots & \vdots \\ \vdots & & \ddots & \ddots & 0 & \vdots \\ 0 & \dots & \dots & 0 & 1 & -1 \end{pmatrix}.$$

Ces deux codes sont MDS, et sont les duaux l'un de l'autre.

Codes de Hamming binaires. Un *code de Hamming* sur $\mathbb{F}_2$ peut être construit de la manière suivante. Pour un entier $r \geq 2$ fixé, on définit la matrice de parité $\boldsymbol{H} \in \mathbb{F}_2^{r \times n}$ du code comme la matrice dont chacune des $n = 2^r - 1$ colonnes est formée des coordonnées d'un vecteur non-nul de $\mathbb{F}_2^r$ (on ordonne les colonnes arbitrairement). Par exemple, pour $r = 2$ et $r = 3$, on obtient respectivement les matrices :

$$\boldsymbol{H}^{(r=2)} = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix} \qquad \text{et} \qquad \boldsymbol{H}^{(r=3)} = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}.$$

On a alors les résultats suivants.

Proposition 1.10

Pour tout $r \geq 2$, le code de Hamming de paramètre r est un code de longueur $n = 2^r - 1$, de dimension $2^r - 1 - r$ et de distance minimale 3. Sa distance duale est $d^\perp = 2^{r-1}$.

Notons que les codes de Hamming sont parfaits, mais n'atteignent la borne de Singleton que pour $r = 2$ (c'est alors le code de parité de longueur 3).

Codes de Reed–Solomon. Les codes de Reed–Solomon forment une famille importantes de codes. Ils sont construits de la manière suivante.

Définition 1.11

Soit $\boldsymbol{x} = (x_1, \dots, x_n) \in \mathbb{F}_q^n$ tel que les x_i sont deux à deux distincts. Le code de Reed–Solomon de dimension k et points d'évaluation $\boldsymbol{x}$ est :

$$\mathrm{RS}_k(\boldsymbol{x}) \coloneqq \{(f(x_1), \dots, f(x_n)) \mid f \in \mathbb{F}_q[X]_{<k}\} \subseteq \mathbb{F}_q^n.$$

On note souvent $\mathrm{ev}_{\boldsymbol{x}}(f) \coloneqq (f(x_1), \dots, f(x_n)) \in \mathbb{F}_q^n$ le *vecteur d'évaluation* du polynôme f sur $\boldsymbol{x}$.

Proposition 1.12

Les codes de Reed–Solomon sont des codes MDS.

En TD, on observera que le dual d'un code de Reed–Solomon est « presque » un code de Reed–Solomon, dans le sens où il suffit de multiplier chaque coordonnée par un coefficient non-nul (indépendant du mot de code) pour obtenir un code de Reed–Solomon.

Chapitre 2

Notions de localité pour le stockage distribué

2.1 Contexte et motivations

Le développement du stockage en ligne soulève la question de la gestion durable des données à stocker : par exemple, en cas de panne ponctuelle, on veut être certain de pouvoir retrouver les données déposées sur les serveurs.

L'utilisation d'un seul serveur se stockage paraît donc prohibée : si le serveur est en échec, il devient impossible d'accéder à l'information qui y était déposée. On s'intéresse donc au problème du **stockage distribué**, c'est-à-dire à la répartition idéale de données à stocker sur différents serveurs.

Dans notre modèle, les données dont stockées sur plusieurs serveurs qui communiquent entre eux. Ces données sont distribuées sur plusieurs serveurs pour plusieurs raisons :

— la capacité de stockage d'un serveur peut être inférieure à la quantité de données à stocker

— comme expliqué précédemment, on souhaite également réparer des serveurs défaillants ; il ne faut donc pas placer toutes les données au même endroit.

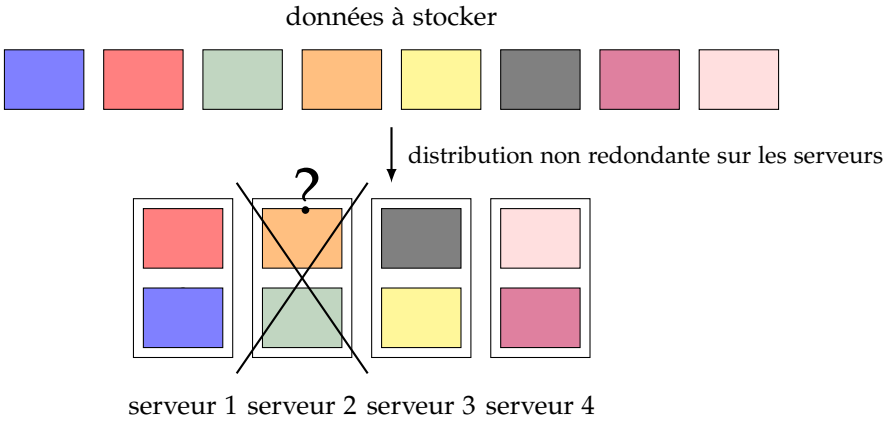


FIGURE 2.1 – Illustration d'un stockage distribué mais non-redondant. Les serveurs ont une capacité de deux fichiers (représentés par les rectangles colorés), on doit donc utiliser plusieurs serveurs. Dans cet exemple, en cas de panne du second serveur, les fichiers représentés en orange et en vert sont inaccessibles.

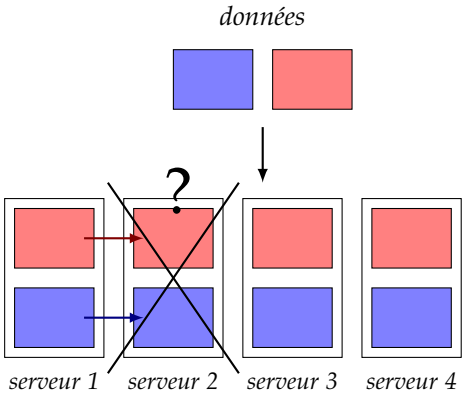
Dans la Figure 2.1, on donne un exemple de stockage distibué non-redondant : les fichiers à stocker sont simplement déposés sur les différents serveurs. On remarque que cette distribution n'est pas

satisfaisante en cas de panne. Avant de formaliser plus précisément le problème, commençons donc par donner deux exemple de stockage distribué redondant

Exemple 2.1

Dans cet exemple, on effectue des copies des données sur n serveurs. Si l'un des serveurs échoue, on pourra ainsi récupérer l'information en faisant une copie su serveur défaillant. Si les fichiers à stocker sont de taille M, les performances de ce système de stockage sont :

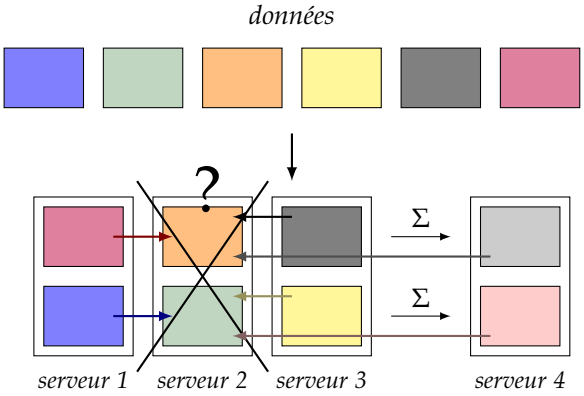
- *la complexité de stockage est nM,*
- *le nombre de serveurs à contacter pour la reconstruction est* 1.



Exemple 2.2

Dans cet exemple, si l'on dispose de n serveurs, alors les données sont partitionnées en $n-1$ sous-ensembles. On stocke les données brutes en les disposant sur les $n-1$ premiers serveurs suivant la partition choisie, puis le dernier serveur a le rôle de « contrôle de parité » : on y stocke la somme (`xor`) des fichiers déposés sur les autres serveurs.
Si l'un des serveurs échoue, alors on est capable de récupérer l'information disparue en efectuant la somme (`xor`) des données stockées sur les autres serveurs. D'un point de vue performance, si la taille ds fichiers est M, alors :

- *la complexité de stockage est $\frac{n}{n-1}M$,*
- *le nombre de serveurs à contacter pour la reconstruction est $n-1$.*



Remarque 2.3

Dans l'Exemple 2.2, il peut être gênant qu'un unique *serveur ait le rôle de contrôle de parité : il n'est jamais contacté pour de la lecture, et toujours contacté pour de la reconstruction. On peut alors équilibrer le rôle des serveurs en découpant l'information (*file striping*), pour que chaque serveur ait un rôle de contrôle de parité pour un sous-ensemble des données à stocker.*

Dans les deux exemples précédents, on observe un compromis en terme de performances, entre la complexité de stockage (autrement dit, la redondance) et la complexité de reconstruction, en nombre de serveurs à contacter.

On peut dès lors se poser les questions suivantes :

— existe-t-il d'autres compromis, moins extrêmes que la copie sur n serveurs (coûteux) en stockage, et le serveur de parité (coûteux pour la reconstruction) ?
— si oui, quelles sont les limites théoriques ?
— en accord avec ces limites théoriques, peut-on obtenir des constructions optimales ?

L'objectif de ce chapitre est de donner un aperçu des réponses possibles à ces questions.

2.2 Définitions et résultats généraux

2.2.1 Un formalisme de codes pour les systèmes de stockage distribués

Commençons par adopter un **formalisme issue de la théorie des codes** pour représenter le système de stockage.

On suppose que les données à stocker peuvent être partionnées en k sous-ensembles de même taille, de sorte qu'on les assimile à des vecteurs $\boldsymbol{m}$ de $\mathbb{F}_q^k$. Étant donné n serveurs et un code $\mathcal{C} \subseteq \mathbb{F}_q^n$ de dimension k, le système de stockage fondé sur $\mathcal{C}$ est le suivant. Pour chaque vecteur d'entrée $\boldsymbol{m}$ à stocker :

— on encode $\boldsymbol{m}$ en un mot de code $\boldsymbol{c} \in \mathcal{C}$,
— pour tout $i \in [1, n]$, on stocke le symbole $c_i \in \mathbb{F}_q$ sur le i-ème serveur.

Todo: faire un exemple

Définition 2.4

Soit $\mathcal{C} \subseteq \mathbb{F}_q^n$ un code.

1. *Une coordonnée $i \in \{1, \dots, n\}$ a* **localité** $r \geq 1$ *s'il existe*
   - *un ensemble $S \subseteq [1, n] \setminus \{i\}$ de cardinal r, et*
   - *une application linéaire $\phi_i : \mathbb{F}_q^r \to \mathbb{F}_q$*

   tels que pour tout $\boldsymbol{c} \in \mathcal{C}$, on a $c_i = \phi_i(\boldsymbol{c}_{|S})$. On dit alors que S est un **ensemble de recontruction** *pour i.*
2. *Le code $\mathcal{C}$ est* **localement recouvrable** *avec localité r si toutes les coordonnées $i \in [1, n]$ ont localité r. On écrit que $\mathcal{C}$ est un LRC (*locally recoverable code*) de localité r, ou un code r-LR.*

Exemple 2.5

Soit $\mathcal{C} \subseteq \mathbb{F}_q^{12}$ le code ayant pour matrice de contrôle

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

Alors, $i = 1$ a pour ensemble de reconstruction $\{2, 3, 4\}$. En effet, on a :

$$c_1 = -c_2 - c_3 - c_4\,, \quad \forall \boldsymbol{c} \in \mathcal{C}\,.$$

Similairement, on observe ensuite que tous les indices $i \in [1, 12]$ ont un ensemble de reconstruction de taille 3. Le code $\mathcal{C}$ est donc localement recouvrable avec une localité $r = 3$.
Remarquons ici que le code $\mathcal{C}$ est ici la juxtaposition de 3 codes de parité de longueur 4.

Lemme 2.6

Si $\mathcal{C}$ est un code r-LR, alors une système de stockage fondé sur $\mathcal{C}$ permet de reconstruire n'importe quel serveur défaillant en contactant au plus r autres serveurs.

Démonstration : Si le i-ème serveur est défaillant, notons S un ensmeble de reconstruction associé à i. Alors, on peut recalculer c_i grâce à l'application ϕ_i, qui n'a besoin que de r valeurs $\boldsymbol{c}_{|S}$ stockées sur r serveurs distincts du i-ème. ■

Remarque 2.7

La définition d'un code localement recouvrable est équivalente à la suivante :
Définition équivalente. *Un code est r-LR si et seulement si la condition suivante est vérifiée. Pour tout $i \in [1, n]$, il existe $S \subseteq [1, n] \setminus \{i\}$ de cardinal r tel que*

$$\dim \mathcal{C}_{|S} = \dim \mathcal{C}_{|S \cup \{i\}} .$$

Nous avons donné un cadre formel aux systèmes de stockage permettant de reconstruire un serveur défaillant. Notons que, si le système est fondé sur un code $\mathcal{C}$ de longueur n, de dimension k et de localité r, alors :

1. la complexité de stockage est $\frac{n}{k}M$, si les données originelle ont taille M,
2. le nombre de serveurs à contacter pour la reconstruction est r.

On en vient donc à de nouvelles problématiques, induites par le paramètre de localité r : quelles sont les bornes liants n, k, d et r ? existe-t-il des constructions optimales pour ces bornes ?

2.2.2 Localité de codes communs

Avant de chercher à répondre aux questions précédents, donnons la localité de codes communs (voir Chapitre 1 pour la définition de ces codes).

Code de répétition. Le code de répétition, de paramètres $[n, 1, n]_q$, a localité $r = 1$. En effet, tout symbole c_i est la copie exacte d'un symbole c_j avec $j \neq i$. Remarquons que ce code correspond à l'Exemple 2.1 ave $n = 4$

Code de parité. Le code de parité de paramètres $[n, n-1, 2]_q$, a localité est $r = n - 1$. En effet, par définition on peut recalculer c_i en effectuant la somme suivante :

$$c_i = -\sum_{j \neq i} c_j .$$

Ce code correspond à l'Exemple 2.2 avec $n = 4$.

Codes de Reed–Solomon. Soit $\mathcal{C} = \mathrm{RS}_k(\boldsymbol{x}, \boldsymbol{y})$. Rappelons que le code $\mathcal{C}$ a pour paramètres $[n, k, n - k + 1]$. Sa localité est $r = k$. En effet, soit $\boldsymbol{c}$ un mot de code, et supposons que l'on veuille retrouver un symbole $c_i = f(x_i)$, où $f \in \mathbb{F}_q[X]_{<k}$. Alors, on choisit pour ensemble de reconstruction S n'importe quel autre sous-ensemble de $[1, n] \setminus \{i\}$ de cardinal k. Les valeurs de $\boldsymbol{c}$ indexées par S permettent de reconstruire le polynôme f par interpolation (il y a k valeurs d'interpolation pour un polynôme de degré $\leq k - 1$). Puis, on obtient $c_i = f(x_i)$.

2.2.3 Bornes

Lemme 2.8

Soit $\mathcal{C} \subseteq \mathbb{F}_q^n$ un code de dimension k et de distance duale $d^\perp \geq 2$. Alors, $\mathcal{C}$ a localité r, avec :

$$d^\perp - 1 \leq r \leq k .$$

Démonstration : Soit $\boldsymbol{G}$ une matrice génératrice de $\mathcal{C}$.
Soit $i \in [1, n]$. Comme le code a dimension k, il existe un ensemble de k colonnes indépendantes $\{G_j\}_{j \in S}$ de $\boldsymbol{G}$. Par ailleurs, comme $d^\perp \neq 1$, on peut supposer que $i \notin S$ (en effet, la i-ème colonne de $\boldsymbol{G}$ est non-nulle donc peut être complétée de $k-1$ colonnes de $\boldsymbol{G}$ pour former une famille libre). Alors, S est un ensemble de reconstruction pour i de taille k. On en déduit que $r \leq k$.
Si S est un ensemble de reconstruction pour $i \in [1, n]$, alors il existe une relation linéaire entre c_i et les c_j, $j \in S$ (*via* l'application ϕ_i, voir Définition 2.4). Cette relation linéaire peut s'écrire $c_i + \sum_{j \in S} \lambda_j c_j$, avec $\lambda_j \in \mathbb{F}_q$ non tous nuls. Il existe un mot $\boldsymbol{h} \in \mathcal{C}^\perp$ qui est supporté par $S \cup \{i\}$: c'est le mot qui vaut 1 en position i, λ_j en position j et 0 partout ailleurs. Par conséquent, $d^\perp \leq \mathrm{wt}(\boldsymbol{h}) \leq 1 + |S| = 1 + r$. ■

La proposition suivante généralise le cas des codes de Reed–Solomon vu dans la section précédente.

Proposition 2.9

Un code MDS de dimension k a localité $r = k$.

Démonstration : Exercice. ■

Donc, la localité d'un code MDS est maximale comparée à sa dimension. Ce sont donc les codes avec les coûts de reconstruction locale les plus lourds.

Proposition 2.10

Soit $\mathcal{C} \subseteq \mathbb{F}_q^n$ un code de dimension k et de localité r. Alors, on a :

$$k \leq \frac{nr}{r+1}\,.$$

Démonstration : Donnons une borne inférieure sur la dimension de $\mathcal{C}^\perp$. Commençons par choisir un indice $i_1 \in [1, n]$. Alors il existe un mot $\boldsymbol{h}^{(1)} \in \mathcal{C}^\perp$ tel que

$$i_1 \in I_1 = \mathrm{supp}(\boldsymbol{h}_1) \quad \text{et} \quad \mathrm{wt}(\boldsymbol{h}_1) \leq r+1\,.$$

Pour $j \geq 2$, on choisit ensuite, itérativement, un indice $i_j \notin I_1 \cup \cdots \cup I_{j-1}$, et un mot $\boldsymbol{h}_j \in \mathcal{C}^\perp$ tel que $i_j \in I_j := \mathrm{supp}(\boldsymbol{h}_j)$ et $\mathrm{wt}(\boldsymbol{h}_j) \leq r+1$.
Alors, il est clair que le code engendré par les mots $\{\boldsymbol{h}_1, \ldots, \boldsymbol{h}_j\}$ est un sous-code de $\mathcal{C}^\perp$. Par ailleurs, on démontre par induction que ce code a dimension j car $\boldsymbol{h}^{(j)}$ est le sul mot (parmi $\boldsymbol{h}_1, \ldots, \boldsymbol{h}_j$) dont la coordonnée indexée par i_j est non-nulle.
Le procédé décrit ci-dessus peut être effectué tant que $\cup_{\ell=1}^{j} I_j \neq [1, n]$. On a :

$$\left| \bigcup_{\ell=1}^{j} I_j \right| \leq \sum_{\ell=1}^{j} |I_j| \leq j(r+1)$$

donc on peut aller (au moins) jusque $j_{\max} := \lceil \frac{n}{r+1} \rceil \geq \frac{n}{r+1}$. Donc, on obtient

$$n - k = \dim \mathcal{C}^\perp \geq j_{\max} \geq \frac{n}{r+1}\,,$$

ce qui implique que $k \leq \frac{nr}{r+1}$. ■

Proposition 2.11

Soit $\mathcal{C}$ un code $[n, k, d]$ de localité r. On suppose que $n > (r+1)(\lceil k/r \rceil - 1)$ et que $\mathcal{C}$ est non-dégénéré. Alors, on a :

$$d \leq n - k + 2 - \left\lceil \frac{k}{r} \right\rceil\,.$$

Démonstration : Todo: à terminer ■

Remarque 2.12

Cette borne généralise la borne de Singleton « classique », donnée en Proposition 1.6. En effet, on a vu que $r \leq k$, ce qui donne $d \leq n - k + 2 - 1 = n - k + 1$.

Remarque 2.13

Les codes MDS atteignent cette borne, mais avec une localité maximale $r = k$.

Exemple 2.14

On définit un code par sa matrice de contrôle :

$$\boldsymbol{H} = \begin{bmatrix} 11\dots1 & 00\dots0 & & & 00\dots0 \\ 00\dots0 & 11\dots1 & 00\dots0 & & \\ & & & & \\ & & 00\dots0 & 1\dots11 & 00\dots0 \\ 00\dots0 & & & 00\dots0 & 11\dots1 \end{bmatrix} \in \mathbb{F}_q^{s\times(r+1)s}.$$

Ce code a longueur $n = (r+1)s$, dimension $k = n - s = rs$ et localité r. Sa distance minimale est égale à 2 (les deux premières colonnes de $\boldsymbol{H}$ sont liées). Dans ce contexte, la borne de la Proposition 2.11 est :

$$d \leq n - k + 2 - \left\lceil \frac{k}{r} \right\rceil = s + 2 - s = 2.$$

Le code est donc optimal.

2.3 Une construction optimale : les codes de Tamo–Barg

Dans cette partie, nous allons construire une famille de codes qui atteint la borne de la Proposition 2.11. Ces codes seront conçus sur le modèle des codes de Reed–Solomon, en choisissant plus particulièrement les points d'évaluation et l'espace de polynômes à évaluer.

Commençons par un exemple pour nous donner une idée de la construction.

Exemple 2.15

Sur $\mathbb{F}_q$ où $q = 13$, on choisit les points d'évaluation

$$\boldsymbol{x} = (1, 3, 9, 2, 6, 5, 4, 12, 10)$$

que l'on partitionne en trois ensembles $\mathcal{A}_1 = \{1, 3, 9\}$, $\mathcal{A}_2 = \{2, 6, 5\}$, $\mathcal{A}_3 = \{4, 12, 10\}$.
Remarquons que $\mathcal{A}_1$, $\mathcal{A}_2$ et $\mathcal{A}_3$ ont été choisis de sorte que

$$\begin{cases} \forall a \in \mathcal{A}_1, & a^3 = 1, \\ \forall a \in \mathcal{A}_2, & a^3 = 8, \\ \forall a \in \mathcal{A}_3, & a^3 = -1, \end{cases}$$

Puis, on considère l'espace de fonctions polynomiales suivant :

$$\mathcal{F} \coloneqq \mathrm{Vect}_{\mathbb{F}_q}\{1, x, x^3, x^4, x^6, x^7\}.$$

Finalement, on construit le code

$$\mathcal{C} \coloneqq \{\mathrm{ev}_{\boldsymbol{x}}(f), f \in \mathcal{F}\} \subseteq \mathbb{F}_q^9.$$

Soit maintenant $\boldsymbol{c} = \mathrm{ev}_{\boldsymbol{x}}(f)$ un mot de $\mathcal{C}$, et supposons que l'on souhaite retrouver c_i. On note x_i le point d'évaluation tel que $c_i = f(x_i)$, et on suppose, par exemple, que $x_i \in \mathcal{A}_2$ (on pourrait très bien prendre l'exemple de $\mathcal{A}_1$ ou $\mathcal{A}_3$).
Alors, en notant $f(x) = \sum_i \lambda_i x^i \in \mathcal{F}$, on obtient que pour tout $a \in \mathcal{A}_2$:

$$\begin{aligned} f(a) &= (\lambda_0 + a^3\lambda_3 + a^6\lambda_6) + a(\lambda_1 + a^3\lambda_4 + a^6\lambda_7) \\ &= (\lambda_0 + 8\lambda_3 + 8^2\lambda_6) \times 1 + (\lambda_1 + 8\lambda_4 + 8^2\lambda_7) \times a \end{aligned}$$

Autrement dit, observée sur $\mathcal{A}_2$, la fonction polynomiale f est de degré 1. Comme on a deux points d'évaluations autres que x_i dans $\mathcal{A}_2$, on peut interpoler $f_{|\mathcal{A}_2}$ sur ces deux points puis retrouver $c_i = f_{|\mathcal{A}_2}(x_i)$.
Plus formellement, on peut simplement remarquer que $\mathcal{C}_{|\mathcal{A}_2}$ est le code de Reed-Solomon de dimension 2 évalué sur $\mathcal{A}_2$.
Concernant les paramètres du code :

1. *la longueur est $n = 9$,*
2. *la dimension est $k = 6$ (dimension de $\mathcal{F}$),*
3. *la distance minimale est ≥ 2, car $\mathcal{C}$ est inclus dans le code de Reed–Solomon $\mathrm{RS}_8(\boldsymbol{x})$, qui est un code $[9, 8, 2]_{13}$,*
4. *la localité est $r = 2$ au vu de ce qui précède.*

On obtient donc

$$n - k + 2 - \left\lceil \frac{k}{r} \right\rceil = 9 - 6 + 2 - 3 = 2$$

ce qui implique (vue la Proposition 2.11) que $d = 2$ et que $\mathcal{C}$ est optimal.

En nous inspirant de l'exemple précédent, nous allons maintenant construire un code localement recouvrable de localité $r \geq 2$ quelconque atteignant la borne de la Proposition 2.11.

Pour cela, on considère un polynôme $g \in \mathbb{F}_q[x]$ tel que $\deg g = r + 1$. On considère également des éléments $y_1, \ldots, y_s \in \mathbb{F}_q$ tels que pour tout $j \in [1, s]$, l'équation $g(x) = y_j$ admet exactement $r + 1$ solutions $\mathcal{A}_j = \{a_{j,1}, \ldots, a_{j,r+1}\} \subseteq \mathbb{F}_q$.

Pour $1 \leq \ell \leq s$, on construit l'espace de fonctions polynomiales :

$$\mathcal{F}_\ell \coloneqq \mathrm{Vect}\{x^i g(x)^j \mid 0 \leq i \leq r - 1, 0 \leq j \leq \ell - 1\}$$

et le vecteur d'évaluation

$$\boldsymbol{a} = (a_{1,1}, \ldots, a_{1,r+1}, a_{2,1}, \ldots, \ldots, a_{s,1}, \ldots, a_{s,r+1})$$

Définition 2.16

Avec les notations ci-dessus, le code de Tamo-Barg est défini comme :

$$\mathrm{TB}_\ell(\boldsymbol{a}, g) \coloneqq \{\mathrm{ev}_{\boldsymbol{a}}(f) \mid f \in \mathcal{F}_\ell\} \subseteq \mathbb{F}_q^{s(r+1)}.$$

Proposition 2.17

Soient $\ell \geq 1$, $g \in \mathbb{F}_q[X]$ et $\boldsymbol{a} \in \mathbb{F}_q^{s(r+1)}$ construits comme ci-dessus, avec $\deg g = r + 1$. Aors, le code de Tamo–Barg $\mathrm{TB}_\ell(\boldsymbol{a}, g)$ a pour longueur $n = (r + 1)s$, pour dimension $k = r\ell$, et pour distance minimale $d = (r + 1)(s - \ell) + 2$. Il est également localement recouvrable de localité r. Il atteint donc la borne de la Proposition 2.11.

Démonstration : Notons $\mathcal{C} = \mathrm{TB}_\ell(\boldsymbol{a}, g)$. Il est clair que la longueur du code est $n = (r + 1)s$. Concernant la dimension, on a $k \leq r\ell$ car $\mathcal{F}_\ell$ est de dimesnion $r\ell$. Par ailleurs, les polynômes à évaluer sont de degré $\leq (r + 1)(s - 1) + r - 1 = (r + 1)s - 2$, et sont évalués sur les $(r + 1)s$ points distincts de $\boldsymbol{a}$. Par conséquent l'application d'évaluation est injective donc $\dim \mathcal{C} = r\ell$.
La localité du code est r, par construction. Pour montrer cela, choisissons un un mot $\boldsymbol{c} = \mathrm{ev}(f) \in \mathcal{C}$. Alors, pour tout $j \in [1, s]$ et tout $a_{j,i} \in \mathcal{A}_j$, on a

$$f(a_{j,i}) = \sum_{u=0}^{r-1} \sum_{v=0}^{\ell-1} \lambda_{u,v}\, a_{j,i}^u\, g(a_{j,i})^v = \sum_{u=0}^{r-1} \left(\sum_{v=0}^{\ell-1} y_j^v\, \lambda_{u,v} \right) a_{j,i}^u$$

Par conséquent, le code $\mathcal{C}_{|\mathcal{A}_j}$ peut s'écrire comme $\mathrm{RS}_r(\boldsymbol{a}_{|\mathcal{A}_j})$, qui est un code $[r + 1, r, 2]$. Donc en particulier on a $\dim \mathcal{C}_{|\mathcal{A}_j} = r = \dim \mathcal{C}_{|\mathcal{A}_j \setminus \{a_{j,i}\}}$.
Enfin, la distance minimale du code est $d = (r + 1)(s - \ell) + 2$. En effet, on voit que $\mathcal{C}$ est un sous-code de $\mathrm{RS}_{k'}(\boldsymbol{a})$, avec $k' = (r + 1)(\ell - 1) + r$. Donc

$$d \geq n - k' + 1 = (r + 1)(s - \ell) + 2$$

Comme le code est sujet à la borne de la Proposition 2.11, il y a égalité dans la dernière inéquation. ∎

Bibliographie

[Cou20] Alain Couvreur. Introduction to coding theory. `http://www.lix.polytechnique.fr/~alain.couvreur/doc_ens/lecture_notes.pdf`, 2020.

[HP03] W. Cary Huffman and Vera Pless. *Fundamentals of Error-Correcting Codes*. Cambridge University Press, 2003.

[HvLP11] Tom Høholdt, Jacobus H. van Lint, and Ruud Pellikaan. Algebraic geometry codes. In *Handbook of Coding Theory*, volume 1, pages 871–961. 2011.

[vL99] Jacobus H. van Lint. *Introduction to Coding Theory, 3rd edition*. Springer, 1999.

[Wal] Judy L. Walker. Codes and curves. `https://cdn.preterhuman.net/texts/math/Codes%20and%20Curves.pdf`.