Introduction à la théorie des codes correcteurs d'erreurs

Codes linéaires

Odile PAPINI

POLYTECH
Université d'Aix-Marseille
odile.papini@univ-amu.fr
http://odile.papini.perso.esil.univmed.fr/sources/CODAGE.html

Plan du cours

1. poids des codes linéaires
2. description par des matrices génératrices
3. description par des matrices de contrôle
4. décodage d'un code linéaire
5. exemples de codes linéaires

Bibliographie I


F. J. Mac Willians & N. J. A. Sloane
The Theory of Error Correcting codes.
North Holland Publising, ed. 1978.


O. Papini & J. Wolfmann
Algèbre discrète et codes correcteurs d'erreurs.
Springer Verlag ed. 1995.


Support de cours
Claude Carlet Université Paris 13
http://www.math.univ-paris13.fr/ schartz/Mali/Mali07/ccc.pdf

introduction

On munit l'alphabet A de deux lois internes $+$ et $\star$ et la structure $(A, +, \star)$ a les propriétés suivantes :

A a une structure de corps fini

- $(A, +)$ est un groupe commutatif

$\forall x \in A,\ \forall y \in A,\ \forall z \in A,$

- $x \star (y \star z) = (x \star y) \star z$ **associativité**
- $x \star (y + z) = (x \star y) + (x \star z)$ **distributivité à gauche**
- $(x + y) \star z = (x \star z) + (y \star z)$ **distributivité à droite**
- $\exists\, 1 \in A$ tq $x \star 1 = 1 \star x = x$ **élément unité**
- $\forall x \in A \backslash \{0\}, \exists\, x' \in A$ tq $x \star x' = x' \star x = 1$ **élément symétrique**

rappel

loi interne $+$ dans un ensemble A :

$$\begin{array}{ccc} A \times A & \rightarrow & A \\ (x, y) & \rightarrow & x + y \end{array}$$

groupe

$(A, +)$: une structure telle que $\forall x \in A,\ \forall y \in A,\ \forall z \in A$

- $x + (y + z) = (x + y) + z)$ **associativité**
- $\exists e \in A,\ tq\ \forall x \in A,\ x + e = e + x = x$ **élément neutre**
- $\forall x \in A,\ \exists x' \in A,\ tq\ x + x' = x' + x = e$ **élément symétrique**

$(A, +)$ est un groupe **commutatif** si
$\forall x \in A, \forall y \in A, x + y = y + x$

rappel

L'alphabet A est un corps fini $\mathbb{K}$ alors $\mathbb{K}^n$ est un espace vectoriel loi externe $\times$:

$$\begin{array}{ccc} \mathbb{K} \times \mathbb{K}^n & \rightarrow & \mathbb{K}^n \\ (x, y) & \rightarrow & x \times y \end{array}$$

espace vectoriel

$(\mathbb{K}^n, +, \times)$ sur $\mathbb{K}$ corps commutatif est une structure telle que :

- $(\mathbb{K}^n, +)$ est un groupe commutatif
- $\forall \lambda \in \mathbb{K},\ \forall \mu \in \mathbb{K}\ , \forall x \in \mathbb{K}^n, \quad \lambda(\mu \times x) = (\lambda\mu) \times x$
- $e \in \mathbb{K}$ élément neutre $\quad e \times x = x$
- $\forall \lambda \in \mathbb{K},\ \forall \mu \in \mathbb{K},\ \forall x \in \mathbb{K}^n, \quad (\lambda + \mu) \times x = \lambda x + \mu x$
- $\forall \lambda \in \mathbb{K},\ \forall x \in \mathbb{K}^n,\ \forall y \in \mathbb{K}^n, \quad \lambda(x + y) = \lambda x + \lambda y$

poids d'un code

l'alphabet A est un corps fini $\mathbb{K}$

$\mathbb{K}^n$ est un espace vectoriel pour les lois habituelles

définition : poids

Soit $x = (x_1, x_2, ...x_n) \in \mathbb{K}^n$ le **poids** de x, noté $w(x)$, est le nombre de ses composantes non nulles.

$$w(x) = \sharp\{i \in \{1, 2, \ldots, n\},\ \text{tq } x_i \neq 0\}$$

poids d'un code

propriétés du poids

$\forall x, y \in \mathbb{K}^n$ et $\lambda \in \mathbb{K}$ on a :

i) $d(x, y) = w(x - y)$;

ii) $w(x) = d(x, 0)$;

iii) $w(x) = 0$ ssi $x = 0$;

iv) $w(\lambda x) = w(x)$ si $\lambda \neq 0$;

v) $w(x + y) \leq w(x) + w(y)$.

(démonstration laissée en exercice).

code linéaire

définition d'un code linéaire

Un **code linéaire** de longueur n sur $\mathbb{K}$ et de dimension k (noté (n,k)) est un **sous-espace vectoriel** de $\mathbb{K}^n$ de dimension k.

si $\sharp\mathbb{K} = p$ et si C est code linéaire (n, k) alors $\sharp C = p^k$

propriété :

si C est code linéaire **l'ensemble des distances** entre les mots de C est **l'ensemble des poids** de C

conséquence :

la distance minimale de C est le poids minimum de C

sous-espace vectoriel

C **sous-espace vectoriel** de $\mathbb{K}^n$ sur $\mathbb{K}$:

- C non vide
- stable pour $+$
- stable pour $\times$

caractérisation d'un sous-espace vectoriel

C est un **sous-espace vectoriel** de $\mathbb{K}^n$ sur $\mathbb{K}$ ssi

- C non vide
- $\forall x \in C,\ \forall y \in C \quad x - y \in C$
- $\forall x \in C,\ \forall \lambda \in \mathbb{K} \quad \lambda \times x \in C$

description des codes linéaires par les matrices génératrices

Un code linéaire est entièrement déterminé par une de ses bases

définition

Une **matrice gènèratrice** d'un code linèaire C sur le corps $\mathbb{K}$ est une matrice sur $\mathbb{K}$ dont les lignes forment une base de C.

propriétés

Soit C un code linéaire sur un corps $\mathbb{K}$.

i) Toute matrice génératrice est une matrice $k \times n$ sur $\mathbb{K}$, avec $k \leq n$, dont le rang est k;

ii) Inversement, toute matrice $k \times n$ sur $\mathbb{K}$ de rang k, est une matrice génératrice d'un code (n, k) sur $\mathbb{K}$;

description des codes linéaires par les matrices génératrices

matrices génératrices

- un code possède plusieurs matrices génératrices
- les mots de C sont toutes les combinaisons linéaires des lignes d'une matrice génératrice

exemple

Soit G la matrice génératrice d'un code C:

$$G = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 \end{pmatrix}$$

Quels sont les paramètres de C ?

propriétés des matrices génératrices(1)

Si G est une matrice génératrice de C, code linéaire (n, k) sur $\mathbb{K}$, alors :

propriétés

i) Les matrices génératrices de C sont de la forme $A \times G$, où A est **une matrice carrée inversible** $k \times k$ sur $\mathbb{K}$;

ii) Le code C est l'ensemble des mots de la forme

$$m_u = (u_1, u_2, ...u_k)G$$

avec $u = (u_1, u_2, ...u_k)$ dans $\mathbb{K}^k$, et l'application $u \to m_u$ est un isomorphisme vectoriel de $\mathbb{K}^k$ dans C;

propriétés des matrices génératrices (2)

Si G est une matrice génératrice de C, code linéaire (n, k) sur $\mathbb{K}$, alors :

propriétés (suite)

iii) Si $c_1, c_2, ...c_n$ sont les vecteurs colonnes de G, les mots du code C sont tous ceux de la forme

$$m_u = (< c_1, u >, < c_2, u >, \ldots, < c_n, u >)$$

avec $u \in \mathbb{K}^k$ et $< \cdot, \cdot >$ désignant le produit scalaire usuel de $\mathbb{K}^k$.

code linéaire systématique

définition

une matrice génératrice d'un code(n, k) est **normalisée** (ou **canonique**) si la matrice formée par les k premières colonnes est la matrice unité.

Si un code possède une matrice génératrice normalisée, on dit que ce code est **systématique**.

code linéaire systématique

propriétés

iv) Tout code **linéaire** est **équivalent** à un **code linéaire systématique**

v) Si le code C, linéaire (n, k), est systématique, alors, pour chaque $u = (u_1, u_2, ...u_k)$ de $\mathbb{K}^k$, il existe un mot et un seul de C de la forme :

$$m_u = \underbrace{(u_1, u_2, ...u_k,}_{\text{information}} \quad \underbrace{x_{k+1}, x_{k+2}, \ldots, x_n)}_{\text{redondance}}$$

codage avec un code linéaire

G matrice génératrice d'un code C

premier codage : numérisation

$$\text{message} \rightarrow u = (u_1, u_2, ...u_k) \rightarrow m_u = (u_1, u_2, ...u_k, x_{k+1}, x_{k+2}, \ldots, x_n)$$

$$\text{message} \rightarrow u = (u_1, u_2, ...u_k)$$

second codage : codage avec code correcteur

$$u = (u_1, u_2, ...u_k) \rightarrow m_u = (u_1, u_2, ...u_k)G = (u_1, u_2, ...u_k, x_{k+1}, x_{k+2}, \ldots, x_n)$$

Borne de SINGLETON

proposition

Si d est la distance minimale d'un code linéaire $C(n,k)$, alors $d \leq n - k + 1$.

Cette borne est appelée **borne de Singleton**.

définition

un code linéaire $C(n,k)$ est **Maximum Distance Separable** (M. D. S.)
si sa distance minimale d atteint la borne de singleton, i.e.

$$d = n - k + 1$$

description par des matrices de contrôle

sous-espace vectoriel considéré comme **noyau** d'une application linéaire.

définition

Soit C un code (n, k) sur $\mathbb{K}$.
Le **code orthogonal** de C est l'espace vectoriel orthogonal de C pour le produit scalaire usuel de $\mathbb{K}^n$.

propriété

le code orthogonal de C, noté $C^{\perp}$, est un code linéaire $(n, n-k)$

description des codes linéaires par les matrices de contrôle

définition

On appelle **matrice de contrôle** de C, toute matrice **génératrice de son orthogonal**

propriété (fondamentale)

Soit H une matrice de contrôle d'un code C et $x = (x_1, x_2, ...x_n)$

$x \in C$ ssi ${}^tH(x_1, x_2, ...x_n) = (0, 0, \ldots, 0)$

description des codes linéaires par les matrices de contrôle

conséquences

G une matrice génératrice de C.

a) Si H une matrice de contrôle de C, alors $G({}^tH) = 0$

b) Réciproquement, si H est une matrice vérifiant $G({}^tH) = 0$, et qui de plus est de rang maximum,
alors H est une matrice de contrôle de C

construction d'une matrice de contrôle

construction d'une matrice de contrôle

Soit C un code linéaire systématique

G une matrice génératrice normalisée de C : $G = ([I_k][M])$

M : matrice formée par les $n-k$ dernières colonnes, I_k : matrice unité d'ordre k.

$H = ([^tM][-I_{n-k}])$ est une **matrice de contrôle** de C.

construction d'une matrice de contrôle

matrice génératrice de C

$$G = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 \end{pmatrix}$$

$$M = \begin{pmatrix} 1 & 0 \\ 1 & 0 \\ 0 & 1 \\ 0 & 1 \end{pmatrix}$$

matrice de contrôle de C

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

conséquences

conséquences

- $c_1, \cdots, c_n$: colonnes de H, alors :
  ${}^tH(x_1, x_2, ..., x_n) = x_1c_1 + x_2c_2 + \ldots + x_nc_n$

- $(x_1, x_2, ..., x_n) \in C$ ssi $x_1c_1 + x_2c_2 + \ldots + x_nc_n = 0$

- donc **il existe un mot de C de poids r** ssi il existe une **combinaison linéaire à coefficients non-nuls, de r colonnes de H**, qui est elle-même nulle.

- le **poids minimum de C est le plus petit entier non-nul r** tel qu'il existe une **combinaison linéaire à coefficients non-nuls, de r colonnes de H**, qui est elle-même nulle.

décodage d'un code linéaire

H une matrice de contrôle du code C linéaire (n, k) sur $\mathbb{K}$, matrice de l'application linéaire h :

$$\begin{array}{ccc} \mathbb{K}^n & \to & \mathbb{K}^{n-k} \\ x & \to & h(x) \quad \textbf{syndrome} \end{array}$$

$x \in C$ ssi $h(x) = 0$ C est le **noyau** de h

Si x : mot envoyé y : mot reçu, ε : **mot erreur**

$y = x + \varepsilon$

donc

$$h(y) = h(x) + h(\varepsilon)$$

or $x \in C$ donc

$$h(y) = h(\varepsilon)$$

décodage d'un code linéaire

propriété

$h(x) = h(y)$ ssi $x - y \in Kerh$: **partition de K^n en classes d'équivalences**

classes latérales

$u \in K^n$, **classe latérale :** $u + C = \{u + x,\ x \in C\}$
Il y q^{n-k} classes latérale et chacune d'elles contient p^k vecteurs.

propriété

2 classes latérales sont **disjointes** ou **confondues**

décodage d'un code linéaire

principe du décodage

- corriger y c'est trouver ε
- y et ε ont même syndrome : ils sont dans la même classe latérale
- si pour chaque classe latérale on connaît le syndrome correspondant, on calcule le syndrome de y et ε est dans la classe latérale associée
- si le code est e-correcteur et $w(\varepsilon) \leq e$ alors il existe un seul mot ε, $w(\varepsilon) \leq e$ dans la classe latérale
- il suffit de chercher dans la classe latérale associée au syndrome de y le seul mot de poids $\leq e$, c'est ε

décodage d'un code linéaire

algorithme de décodage

- **calcul du syndrome de y**
- **détermination de la classe latérale associée**
- **recherche dans cette classe du mot ε, $(w(\varepsilon) \leq e)$**
- **calcul de $x = y - \varepsilon$**

construction du tableau de déchiffrement

i) On écrit sur une ligne tous les mots du code C en commençant à gauche par le mot nul : $0, c_1, c_2, c_3, \ldots$

ii) On écrit, en dessous du mot nul, un mot u de $\mathbb{K}^n$ qui n'a pas été écrit sur la ligne précédente, et de plus petit poids possible, puis les autres mots de la classe de u : $u, u + c_1, u + c_2, \ldots$

iii) On recommence avec un mot v non écrit dans les lignes précédentes, ainsi de suite jusqu'à épuisement des mots de $\mathbb{K}^n$.

iv) On écrit enfin à droite de chaque ligne, le syndrome associé à la classe correspondante ($h(0) = 0$ pour la première ligne, $h(u)$ pour la deuxième, $h(v)$ pour la troisième, $\cdots$

construction du tableau de déchiffrement

tableau de déchiffrement

0	c_1	c_2	$\dots$	c_n	$h(0)$
u	$u+c_1$	$u+c_2$	$\dots$	$u+c_n$	$h(u)$
v	$v+c_1$	$v+c_2$	$\dots$	$v+c_n$	$h(v)$
.	.	.	.	.	.
.	.	.	.	.	.

tableau de déchiffrement réduit

0	$h(0)$
u	$h(u)$
v	$h(v)$
.	.
.	.

codes simplexes (binaires)

code simplexe

un **code simplexe** (binaire) de longueur $2^k - 1$, un code admettant comme **matrice génératrice** une matrice $(k \times (2^k - 1))$ dont les colonnes sont tous les vecteurs de $\mathbb{F}_2^k \setminus \{0\}$, écrits une fois et une seule.

propriété

Un code simplexe (binaire) a pour longueur $2^k - 1$, pour dimension k, et chaque mot non-nul a pour poids 2^{k-1}. Sa capacité de correction e vaut $2^{k-2} - 1$.

preuve laissée en exercice.

codes de Hamming

code de Hamming

un **code de Hamming** (binaire) de longueur $2^k - 1$, est un code admettant comme **matrice de contrôle** H, une matrice dont les $2^k - 1$ colonnes sont tous les vecteurs de $\mathbb{F}_2^k \setminus \{0\}$.

code simplexe

propriété
Un code de Hamming a pour longueur $2^k - 1$, pour dimension $2^k - 1 - k$, et pour capacité de correction $e = 1$.

preuve laissée en exercice.