T. D. Codes correcteurs d'erreurs.
POLYTECH. 4ième année
AIX MARSEILLE UNIVERSITÉ
Année universitaire 2020/2021

Enseignants : Alexis Bonnecaze
Odile Papini

Feuille de T. D. 2 : Codes linéaires

Exercice 1 : code linéaire

Soit le code C sur $\mathbb{F}_2$, $C = \{x_1 = (1,1,0,0),\ x_2 = (1,1,1,0),\ x_3 = (1,0,1,0)\}$.

1) Ce code n'est pas linéaire car il manque le mot nul $(0,0,0,0)$.
2) Comment transformer ce code en un code linéaire ?
   En rajoutant en plus du mot nul $(0,0,0,0)$, les mots :
   $x_4 = x_1 + x_2 = (0,0,1,0)$,
   $x_5 = x_1 + x_3 = (0,1,1,0)$,
   $x_6 = x_2 + x_3 = (0,1,0,0)$.
   $x_7 = x_1 + x_2 + x_3 = (1,0,0,0)$.

   $C_{lin} = \{x_1 = (1,1,0,0),\ x_2 = (1,1,1,0),\ x_3 = (1,0,1,0),\ x_4 = (0,0,1,0),$
   $x_5 = (0,1,1,0),\ x_6 = (0,1,0,0),\ x_7 = (1,0,0,0),\ x_8 = (0,0,0,0)\}$.

3) Question supplémentaire : quelle est la dimension de C ? donner une base de C.

Exercice 2 : code linéaire description par une matrice génératrice

Soit un code linéaire sur $\mathbb{F}_2$ dont la matrice génératrice est :

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

1) Mettre la matrice G sous forme normalisée.

$$G = \begin{matrix} l_1 \\ l_2 \\ l_3 \end{matrix} \begin{pmatrix} 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 & 1 \end{pmatrix} \quad G' = \begin{matrix} l_1 + l_2 \\ l_1 + l_3 \\ l_1 + l_2 + l_3 \end{matrix} \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 \end{pmatrix}$$

   Remarque : on n'a pas utilisé de permutation de colonnes, donc G' est une autre matrice génératrice du code.

1) la longueur est $n = 6$ et la dimension est $k = 3$.
2) le nombre de mots du code est 2^k, $2^3 = 8$ mots.
3) Les mots du code C sont toutes les combinaisons linéaires des lignes de la matrice G' :
   $(0,0,0,0,0,0) : 0$ [1]
   $(1,0,0,1,1,1) : l'_1$
   $(0,1,0,0,1,1) : l'_2$
   $(0,0,1,1,1,0) : l'_3$
   $(1,1,0,1,0,0) : l'_1 + l'_2$
   $(1,0,1,0,0,1) : l'_1 + l'_3$
   $(0,1,1,1,0,1) : l'_2 + l'_3$
   $(1,1,1,0,1,0) : l'_1 + l'_2 + l'_3$.
4) La capacité de correction du code est $e = \lfloor (d-1)/2 \rfloor = 1$ car $d = 3$.
5) La matrice de contrôle du code C est

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

Exercice 3 : code linéaire description par une matrice de contrôle

Soit le code de Hamming étendu dont la matrice de contrôle est

$$H = \begin{matrix} l_1 \\ l_2 \\ l_3 \\ l_4 \end{matrix} \begin{pmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}$$

1) Mettre la matrice H sous forme normalisée.

$$H' = \begin{matrix} l_1 \\ l_2 \\ l_3 \\ l_1 + l_2 + l_3 + l_4 \end{matrix} \begin{pmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

2) La longueur est $n = 8$ et la dimension est $k = 4$.
3) La distance minimale du code est $d = 4$ car
   Il n'y a pas de mot de poids 1 car aucune colonne de H est nulle.
   Il n'y a pas de mot de poids 2 car il n'y a pas deux colonnes de H qui

1. Par abus de langage on note 0 lemot nul.

sont identiques
Il n'y a pas de mot de poids 3 car il n'existe pas de combinaisons linéaire de 3 colonnes de H nulle. En revanche, il existe une combinaison linéaire de 4 colonnes de H nulle donc $d = 4$.

4) Donner la matrice génératrice du code équivalent.

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

5) Soit les mots reçus $y_1 = (1, 1, 1, 0, 0, 0, 0, 1)$ et $y_2 = (0, 1, 1, 1, 1, 1, 0, 0)$, sous l'hypothèse d'une seule erreur commise au plus , décoder $y_1$et y_2.
$H.y_1^t = (0, 0, 0, 0)$ le syndrome est nul il n'y a pas d'erreur. Donc le mot reçu est le mot transmis $x = y$.
$H.y_2^t = (1, 0, 0, 1)$ le syndrome n'est pas nul donc il y a erreur et $x_2 = y_2 + \epsilon_2$ avec $w(\epsilon_2) \neq 0$ et $H.y_2^t = H.\epsilon_2^t$. Pour déterminer l'erreur on peut construire la tableau de déchiffrement et utiliser la méthode de décodage par tableau de déchiffrement (voir le cours 2). Cependant, dans cet exercice c'est inutile, en effet sous l'hypothèse d'une seule erreur commise au plus , $w(\epsilon_2) = 1$, comme $H.y_2^t = H.\epsilon_2^t$ et ϵ_2 est un vecteur qui a toutes ses composantes nulles sauf une, en regardant la matrice H on voit que la 5 ième colonne est de H correspond au syndrome donc $\epsilon_2 = (0, 0, 0, 0, 1, 0, 0, 0)$ et le mot transmis est $x_2 = (0, 1, 1, 1, 0, 1, 0, 0)$.

6) Les paramètres de l'orthogonal du code $C^\perp$: longueur $n = 8$, dimension $k = 4$. et la matrice génératrice de l'orthogonal du code.

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

Exercice 4 : Codes Simplexes

Un code Simplexe sur $\mathbb{F}_2$ est un code de longueur $2^m - 1$ admettant pour matrice génératrice une matrice $(m \times 2^m - 1)$ dont les colonnes sont tous les m-uplets non nuls de $\mathbb{F}_2$.

Pour $m = 3$:

1) une matrice génératrice :

$$G = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix} \begin{matrix} l_1 \\ l_2 \\ l_3 \end{matrix}$$

La dimension du code est $k = 3$ car il existe une sous-matrice de G de rang 3.

2) Les mots du code sont les combinaisons linéaires des lignes de G :
$(0,0,0,0,0,0,0) : 0$
$(1,0,0,1,0,1,1) : l_1$
$(0,1,0,1,0,1,1) : l_2$
$(0,0,1,0,1,1,1) : l_3$
$(1,1,0,0,1,1,0) : l_1 + l_2$
$(1,0,1,1,0,1,0) : l_1 + l_3$
$(0,1,1,1,1,0,0) : l_2 + l_3$
$(1,1,1,0,0,0,1) : l_1 + l_2 + l_3$.
On remarque que tous les mots sont de poids 4.

3) La distance minimale est donc $d = 4$ et la capacité de correction du code est donc $e = \lfloor (d-1)/2 \rfloor = 1$.

4) Quels sont les paramètres du code dual du code Simplexe ?
longueur $= 2^m - 1 = 7$ et dimension$= n - k = 4$

5) Exhiber tous les mots du code dual du code Simplexe.

$$G = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix} \quad \text{donc} \quad H = \begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}$$

Le code dual du code Simplexe est de dimension 4 donc il comporte 16 mots.

$$G^{\perp} = H = \begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 \end{pmatrix} \begin{matrix} l_1 \\ l_2 \\ l_3 \\ l_4 \end{matrix}$$

$(0,0,0,0,0,0,0) : 0$
$(1,1,0,1,0,0,0) : l_1$
$(1,0,1,0,1,0,0) : l_2$
$(0,1,1,0,0,1,0) : l_3$
$(1,1,1,0,0,0,1) : l_4$

$(0,1,1,1,1,0,0) : l_1 + l_2$
$(1,0,1,1,0,1,0) : l_1 + l_3$
$(0,0,1,1,0,0,1) : l_1 + l_4$
$(1,1,0,0,1,1,0) : l_2 + l_3$
$(0,1,0,0,1,0,1) : l_2 + l_4$
$(1,0,0,0,0,1,1) : l_3 + l_4$
$(0,0,0,1,1,1,0) : l_1 + l_2 + l_3$
$(1,0,0,1,1,0,1) : l_1 + l_2 + l_4$
$(0,1,0,1,0,1,1) : l_1 + l_3 + l_4$
$(0,0,1,0,1,1,1) : l_2 + l_3 + l_4$
$(1,1,1,1,1,1,1) : l_1 + l_2 + l_3 + l_4.$

6) Pour $m \in \mathbb{N}$ quelconque, montrer que le dual d'un code Simplexe est un code de Hamming.

Par définition, les colonnes de la matrice génératrice du code Simplexe, noté $G_{simplexe}$ sont tous les m-uplets non nuls de $\mathbb{F}_2$.

La matrice de contrôle du code Simplexe est la matrice génératrice de l'orthogonal du code Simplexe, $H_{simplexe} = G^{\perp}_{simplexe}$.

Donc $G_{simplexe}.H^t_{simplexe} = G_{simplexe}.G^{\perp^t}_{simplexe} = 0$.

par conséquent $G_{simplexe}$ est la matrice de contrôle du code dual du code Simplexe : $G_{simplexe} = H^{\perp}_{simplexe}$.

Les colonnes de la matrice de contrôle du dual du code Simplexe sont tous les m-uplets non nuls de $\mathbb{F}_2$, le code dual d'un code Simplexe est donc un code de Hamming.

Pour $m \in \mathbb{N}$ quelconque :

1) Montrer que la dimension du code est m.
Par définition, puisque la matrice G est constituée de tous les $m-$uplets non nuls de $\mathbb{F}_2$, il y en a m parmi eux qui constituent une base.

2) Montrer que chaque mot non nul est de poids 2^{m-1}.
Le poids d'un mot c'est la différence entre le nombre total de composantes (ici $2^m - 1$) et le nombre de composantes nulles.
On se ramène au problème de trouver le nombre de composantes nulles.
Or, tout mot d'un code linéaire s'écrit $m_u = (< c_1.u >, < c_2.u > , \cdots < c_i.u >, \cdots < c_n.u >)$ où u est $k-$uplet non nul, les c_i pour $1 \leq i \leq n$ sont les colonnes de G et $< ., . >$ représente le produit scalaire entre deux vecteurs.
Donc, il s'agit de compter les c_i tels que $< c_i.u >= 0$, $1 \leq i \leq n$. Cela revient à compter le nombre de vecteurs orthogonaux aux $m-$uplet u.
Soit u fixé, on regroupe les composantes non nulles sur les j premières positions $u_1, \cdots, u_j$ et les composantes nulles sur les $m - j$ dernières $u_{j+1}, \cdots, u_m$.
Dans le produit $< c_i.u >= 0$, $c_i = (c_{i_1}, \cdots, c_{i_j}, c_{i_{j+1}}, \cdots, c_{i_m})$.
On compte les c_i pour lesquels les $c_{i_1}, \cdots, c_{i_j}$ sont nuls dans $< c_i.u >= 0$. Comme les $u_{j+1}, \cdots, u_m$ sont nuls, on a pour chaque c_{i_k} , $1 \leq k \leq m$,

2 choix donc au total on a 2^{m-j} choix pour les c_i.
On compte les c_i pour lesquels les $c_{i_1}, \cdots, c_{i_j}$ sont non nuls dans $< c_i.u >= 0$. Comme les $u_1, \cdots, u_j$ sont non nuls, on compte le nombre de c_i qui ont un nombre pair de composantes égales à 1 parmi les j composantes. Ce nombre est égal à $C_j^0 + C_j^2 + C_j^4 + \cdots$.
Or on sait que $2^j = \Sigma_{i=0}^{j-1} C_j^i$ donc $C_j^0 + C_j^2 + C_j^4 + \cdots = 2^{j-1}$.
Au final le nombre c_i tels que $< c_i.u >= 0$, $1 \leq i \leq n$. est
$2^{j-1} \times 2^{m-j} - 1$.
(On enlève 1 car on a compté le vecteur nul 2 fois.)
donc le nombre de composantes nulles c'est $2^{j-1} \times 2^{m-j} - 1$ et le poids est donc $2^m - 1 - (2^{j-1} \times 2^{m-j} - 1) = 2^{m-1}$.

3) Montrer que la capacité de correction est $2^{m-2} - 1$.
comme $d = 2^{m-1}$, on a $e = \lfloor (2^{m-1} - 1)/2 \rfloor = 2^{m-2} - 1$

Exercice 5 : Codes de Hamming

Un code de Hamming sur $\mathbb{F}_2$ est un code de longueur $2^m - 1$ admettant pour matrice de contrôle une matrice dont les $2^m - 1$ colonnes sont tous les m-uplets non nuls de $\mathbb{F}_2$

1) La dimension du code est $2^m - 1 - m$.
Par définition la matrice de contrôle est formée par les $2^m - 1$ colonnes qui sont tous les m-uplets non nuls de $\mathbb{F}_2$. Il existe des sous matrices de H de rang m. Donc la dimension du code orthogonal engendré par H est m donc la dimension du code de Hamming est $2^m - 1 - m$.

3) La capacité de correction est 1.
La distance minimale de tout code de Hamming est $d = 3$ car il n'existe pas de mot de poids 1 ni de mot de poids 2.
S'il existait un mot de poids 1, il existerait une colonne de H nulle, ce qui n'est pas le cas d'après la définition de H. S'il existait un mot de poids 2, il existerait deux colonnes de H égales, ce qui n'est pas le cas d'après la définition de H. En revanche, on trouve des mots de poids 3 car il existe des colonnes de H combinaisons linéaires d'au moins 2 colonnes de H.

Exercice 6 **(facultatif) : poids**

Soit K un corps fini, Demontrer que le poids vérifie les propriétés suivantes :

$\forall x, y \in K^n$ et $\forall \lambda \in K$

i) $d(x,y) = w(x-y)$;
par définition $d(x,y) =\mid \{i \in \{1, \cdots n\}, x_i \neq y_i\} \mid$.les composantes non-nulles de $x-y$ sont celles pour lesquelles x et y diffèrent.

ii) $w(x) = d(x,0)$ [2] ;
Immédiat en remplaçant y par 0 dans i).

iii) $w(x) = 0$ si et seulement si $x = (0)$;
$w(x) = d(x,0)$ donc $w(x) = d(x,0) = 0$ si et seulement si $x = 0$.

iv) $w(\lambda\, x) = w(x)$ si $\lambda \neq 0$;
$w(\lambda\, x)$ est le nombre de composantes non nulles de $\lambda\, x$, comme $\lambda \neq 0$, c'est le nombre de composantes de x.

v) $w(x+y) \leq w(x) + w(y)$.
$w(x+y) = w(x-(-y)) = d(x,(-y))$

par la propriété iv) de la distance de Hamming (voir TD1)

$d(x,y) \leq d(x,z) + d(z,y)$.
on a $d(x,(-y)) \leq d(x,0) + d(0,(-y))$

donc $d(x,(-y)) \leq w(x)) + w((-y))$
par la propriété iv) $w(\lambda\, x) = w(x)$ si $\lambda \neq 0$, on a $w(-y) = w(y)$ donc $w(x+y) \leq w(x) + w(y)$.

2. Par abus de langage on note O lemot nul.