Feuille TD 4 - Codes correcteurs - Codes linéaires

1 Code de Hamming

On considère le code de Hamming (15,11) de distance 3.

1. Quel est son rendement ?
2. Expliciter une matrice génératrice, sous forme canonique.
3. Donner l'algorithme de codage.
4. Donner un algorithme qui détecte jusqu'à 2 erreurs.
5. Donner un algorithme qui corrige 1 erreur. Que se passe-t-il en cas de 2 erreurs?

2 Codage et décodage des codes linéaires

Soit C un code linéaire (n, k) sur un vocabulaire V de cardinal $q = p^m$ où p est un nombre premier. On pose $r = n - k$.

Soit $G = \left[\begin{array}{c|c} & \\ L & R \\ & \end{array}\right]$ une matrice génératrice de C, où L est une matrice carrée $k \times k$ et R est une matrice $k \times r$. On rappelle que $C = \mathrm{Im}(G) = \{x^t.G \ / \ x \in V^k\}$.
Dans toute la suite, on supposera que L **est inversible** (cette hypothèse est sans restriction moyennant une permutation éventuelle des chiffres des mots de C).

1. Soit M une matrice $k \times k$ inversible. Montrer que $M.G$ est une matrice génératrice de C.

2. Montrer que C admet une **unique** matrice génératrice G' **normalisée** (ou *canonique*) de la forme

$$G' = \left[\begin{array}{c|c} & \\ I_k & T \\ & \end{array}\right]$$

où I_k est la matrice identité $k \times k$. Expliciter T en fonction de L et R.
En déduire qu'un code linéaire est *systématique*.

3. En déduire une méthode pour calculer le codage du mot source $[u_1, \ldots, u_k] \in V^k$.

4⋆. La *matrice de contrôle* H de C est une matrice $r \times n$ définie par : $H = \left[\begin{array}{c|c} & \\ T^t & -I_r \\ & \end{array}\right]$.

Montrer que $x = [x_1, \ldots x_n] \in C$ si et seulement si $H.\begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} = O$ (i.e. le vecteur nul de V^r).

N.B. Le code engendré par H est appelé *code orthogonal* de C.

5. En déduire une méthode simple pour détecter une erreur lorsqu'on utilise le code C.

6. On suppose maintenant que C est t-correcteur.
Soit $x = [x_1, \ldots, x_n] \in C$ le mot de code envoyé et $y \in V^n$ le mot reçu. On suppose que la distance de Hamming $d_H(x, y)$ entre x et y vérifie : $d_H(x, y) \leq t$.
La correction consiste à calculer x à partir de y.

a. Quel est le cardinal de $\mathrm{Im}(H)$?

b. Soit $e = y - x$ le vecteur d'erreurs. Montrer que e est l'unique elément de V^n de poids de Hamming $w_H(e)$ **minimal** tel que $He = Hy$. (**NB** Le vecteur Hy est appelé *syndrome d'erreur*).

c. En déduire une méthode de correction permettant de calculer x à partir de y.

3 Codes de Golay

On considère le code de Golay $\mathcal{G}_{12}$ ternaire (i.e. sur $V = \mathbb{F}_3$) de matrice génératrice $G = [I_6|R]$ avec

$$R = \begin{bmatrix} 0 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 2 & 2 & 1 \\ 1 & 1 & 0 & 1 & 2 & 2 \\ 1 & 2 & 1 & 0 & 1 & 2 \\ 1 & 2 & 2 & 1 & 0 & 1 \\ 1 & 1 & 2 & 2 & 1 & 0 \end{bmatrix}$$

1. En admettant que $\mathcal{G}_{12}$ est de distance 6, donner ses caractéristiques et sa matrice de contrôle.

2. On vérifie facilement que si r et s sont deux lignes quelconques de G, alors $r.s = 0$ (non demandé). En déduire que $\mathcal{G}_{12}$ est auto-dual, i.e. $\mathcal{G}_{12} = \mathcal{G}_{12}^{\perp}$.

3. Montrer que $\mathcal{G}_{12}$ n'est pas parfait.

4. Soit $\mathcal{G}_{11}$ le code obtenu à partir de $\mathcal{G}_{12}$ en supprimant sa dernière composante; expliciter la matrice de contrôle associée à $\mathcal{G}_{11}$. Quelle est sa distance ?

5. Montrer que $\mathcal{G}_{11}$ est un code parfait.

Complément: un code binaire parfait

On peut construire un code binaire parfait (23, 12, 7) à partir du code de Golay binaire $\mathcal{G}_{24}$.

Le code (24, 12, 8) $\mathcal{G}_{24}$ a les propritétés suivantes:

- $\mathcal{G}_{24}$ est auto-dual (i.e. $\mathcal{G}_{24}^{\perp} = \mathcal{G}_{24}$).
- $\mathcal{G}_{24}$ admet aussi $[A|I_{12}]$ comme matrice génératrice.
- Le poids de tout mot de $\mathcal{G}_{24}$ est divisible par 4 (en effet, toute ligne a un poids multiple de 4 et les lignes étant toutes orthogonales 2 à 2, toute combinaison de lignes a un poids aussi multiple de 4).
- $\mathcal{G}_{24}$ est de distance 8 (il n'y a pas de mot de poids 4).
- Soit $\mathcal{G}_{23}$ le code (23, 12, 7) obtenu à partir de $\mathcal{G}_{24}$ en supprimant sa dernière composante; $\mathcal{G}_{23}$ est un code parfait.

$\mathcal{G}_{24}$ a pour matrice génératrice $G = [I_{12}|A]$ avec (NB '0' est noté '.')

$$A = \begin{bmatrix} . & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & . & 1 & 1 & 1 & . & . & . & 1 & . \\ 1 & 1 & . & 1 & 1 & 1 & . & . & . & 1 & . & 1 \\ 1 & . & 1 & 1 & 1 & . & . & . & 1 & . & 1 & 1 \\ 1 & 1 & 1 & 1 & . & . & . & 1 & . & 1 & 1 & . \\ 1 & 1 & 1 & . & . & . & 1 & . & 1 & 1 & . & 1 \\ 1 & 1 & . & . & . & 1 & . & 1 & 1 & . & 1 & 1 \\ 1 & . & . & . & 1 & . & 1 & 1 & . & 1 & 1 & 1 \\ 1 & . & . & 1 & . & 1 & 1 & . & 1 & 1 & 1 & . \\ 1 & . & 1 & . & 1 & 1 & . & 1 & 1 & 1 & . & . \\ 1 & 1 & . & 1 & 1 & . & 1 & 1 & 1 & . & . & . \\ 1 & . & 1 & 1 & . & 1 & 1 & 1 & . & . & . & 1 \end{bmatrix}$$